Dipartimento Impresa e Management

Corso di Laurea Magistrale in Marketing
indirizzo in Analisi e Misure di Marketing

Cattedra di Analisi e Misurazione delle Performance di Marketing - Marketing Metrics

ANALISI DEI FATTORI CRITICI SULL'ADOZIONE DEI SERVIZI IOT IN AMBITO MEDICO E SANITARIO: TRATTAMENTO DEI DATI PERSONALI, PRIVACY PARADOX ED ESTERNALITÀ DI RETE

Relatore:
Prof. Costabile Michele

Candidato
Sergenti Pietro

Correlatore:
Prof. Tedeschi Piermario

Anno Accademico 2018/2019

Un ringraziamento speciale va a mia madre Elsa e mio padre Italo che mi hanno accompagnato costantemente durante tutta la mia vita.

Un ringraziamento a mio padrino Fabio per la fiducia avuta nei miei confronti.

Dedico questa tesi alla mia madrina Paola e mia zia Angiolina.

INDICE

Introduzione

Sempre più frequentemente interagiamo nel quotidiano con dispositivi elettronici, dai semplici elettrodomestici alle apparecchiature digitali di ultima generazione. Soprattutto verso questi ultimi si rivolge l'attenzione del mercato. Da molti anni a questa parte il *trend* di utilizzo di nuove tecnologie è in forte crescita e questo fenomeno risulta essere presente in diversi settori e contesti. Il più affascinante di tutti riguarda sicuramente l'ambito applicativo dell'*Internet of Things*, che tradotto significa banalmente Internet delle cose. L'*Internet of Things*, da cui l'acronimo IoT, fa riferimento alla capacità di oggetti o dispositivi, di interagire con il mondo esterno. I dispositivi IoT quindi, non si limitano più a registrare in maniera passiva i dati, ma bensì ad immagazzinarli, rielaborarli e trasmetterli ad altri dispositivi. Questa è pertanto la loro principale peculiarità, la capacità di interfacciarsi in maniera semplice con l'utilizzatore e di comunicare tra loro. Una tale duttilità di applicazione ha permesso a tutti i dispositivi IoT, meglio noti come *smart device*, di fare facilmente breccia nel mercato, e di riflesso, nella vita degli utilizzatori. Grazie a questi dispositivi di più vario genere (si pensi dagli orologi, ai telefoni, ai visori a realtà aumentata) si sono modificate, in un lasso di tempo relativamente breve, le abitudini dei consumatori. Questo cambiamento comportamentale, denotabile come un crescente utilizzo e disposizione di dispositivi *smart*, ha portato ad un aumento esponenziale dei dati generati, in particolar modo quelli di natura privata/personale. Proprio sulla raccolta dei dati personali sono nate, e tutt'oggi presenti, molte discussioni riguardanti la tutela della privacy degli utilizzatori spesso ignari o inconsapevoli della grande mole di dati generati e raccolti sulla loro persona. Inoltre, trattandosi di tipologie di dati etichettabili come *big data*, a causa della mole generata, sono soggetti a molti rischi, uno dei quali riguarda l'anonimizzazione che può essere facilmente aggirata. Nonostante si sia denotata una forte preoccupazione verso la tutela dei dati personali e della propria privacy, l'atteggiamento reale tenuto dai consumatori non sempre rispecchia l'atteggiamento teorico da loro stessi indicato. Questo perché malgrado la privacy sia risultata essere una preoccupazione primaria nell'era digitale, i consumatori sono disposti a concedervici accesso in cambio di *reward*, anche di bassa valenza. L'osservazione di questa incoerenza comportamentale ha portato molti studiosi a domandarsi il perché questo avvenga ma soprattutto ad interrogarsi sul "cosa" fosse necessario per far sì che si "attivasse" questa inversione comportamentale. Proprio in risposta a questi quesiti è stato definito il paradosso della privacy (*privacy paradox*).

In questo studio, pertanto, si cercherà di comprendere se una determinata tipologia di *reward* possa essere in grado di innescare l'inversione comportamentale del consumatore circa la disponibilità alla raccolta, elaborazione e condivisione dei propri dati personali. Nello specifico la *reward* utilizzata sarà una ricompensa di servizio e non monetaria. Lo studio verterà sui sistemi IoT a carattere medico sanitario, fenomeno di business che dimostra avere un grande seguito in termini di crescita per gli anni futuri. Specialmente negli ultimi anni il settore sanitario ha concentrato gli sforzi sull'ottimizzazione delle procedure di gestione dell'inventario attraverso l'integrazione della tecnologia di informazione e comunicazione, ma soprattutto sulla ristrutturazione dell'assistenza sanitaria utilizzante tecnologie IoT nella gestione ed ottimizzazione delle

risorse mediche, monitoraggio delle situazioni sanitarie ed aumento dell'uso dell'assistenza medica domiciliare. L'IoT *healthcare* è un promettente scenario di applicazione B2C, in cui i consumatori (pazienti) vengono tenuti sotto osservazione da remoto, grazie l'ausilio di *smart devices* e la generazione/raccolta di bio-dati.

Vale la pena chiedersi quindi, come possano coesistere dispositivi IoT *healthcare* e problematiche di privacy dovute alla raccolta dei dati. L'obbiettivo di questo studio è proprio quello di comprendere come poter rendere questo possibile, utilizzando come moderatore una ricompensa di servizio a carattere medico-sanitario. Integrare quindi ad un dispositivo IoT di carattere generale una competenza medica e vedere se questa è ritenuta sufficientemente importante da innescare il paradosso della privacy facendo così adottare il servizio IoT al consumatore. Inoltre, il modello di riferimento utilizzato può dirci molto su altri elementi cruciali ai fini dell'adozione, quali le esternalità di rete indirette, i benefici percepiti e l'atteggiamento.

Nel primo capitolo verrà esposta la revisione della letteratura in merito agli *hot topic* della ricerca, ossia la nascita e definizione dell'*Internet of Things*, con identificazione della *market size, forecast* di mercato ed applicazione all'area medico/sanitaria; definizione ed inquadramento del concetto di privacy, *privacy paradox* e domanda di ricerca. Il secondo capitolo invece presenterà il modello da cui ha origine lo studio, con formulazione delle ipotesi ed introduzione della variabile aggiuntiva (*service reward).* L'ultimo capitolo, il terzo, esporrà le analisi condotte sul campione di riferimento ottenuto tramite la raccolta di dati grazie a questionari condivisi sulle principali piattaforme social. Grazie ad esse la parte conclusiva esporrà alcune implicazioni manageriali derivanti dai risultati ottenuti, nonché limiti della ricerca e spunti per eventuali lavori futuri.

CAPITOLO 1
La privacy nell'era dell'Internet of Things

In questo capitolo verranno affrontate, dal punto di vista della letteratura, le tematiche principali affrontate durante l'intero studio. L'intenzione è quella di creare una solida base di conoscenza, tale da permettere al lettore di muoversi liberamente nel testo, nonché comprendere in maniera chiara le argomentazioni trattate.

1.1 – Internet of Things

Oggi l'utilizzo di Internet e delle sue applicazioni è diventato un elemento perfettamente integrato nella vita di tutti i giorni. Il concetto di IoT nasce già molti anni addietro ma lo si può ancora considerare in una fase iniziale del suo sviluppo commerciale. Le sue caratteristiche di versatilità e massima flessibilità di applicazione gli consentono di collocarsi su più *industry*: dal settore *automotive* a quello logistico, da quello prettamente informatico a quello medico-sanitario. Tutto ciò avviene con una velocità di crescita tale da portare ad un aumento esponenziale degli *smart device*: dispositivi capaci di comunicare tra di loro in pochissimo tempo.

1.1.1 – Nascita del concetto di Internet of Things

La locuzione "Internet of Things", conosciuta anche con l'acronimo di IoT, si compone di due termini chiave: "Internet" e "Things". Con il termine "Internet" si intende il sistema globale di interconnessione fra reti di computer che utilizzano la suite di protocolli Internet standard (TCP/IP) per raggiungere miliardi di utenti nel mondo (Somayya Madakam, R. Ramaswamy, Siddharth Tripathi, 2015). È un insieme di reti che si compone di network privati, pubblici, accademici, aziendali, governativi di portata locale e globale collegati da un'ampia gamma di dispositivi e tecnologie di rete wireless, elettroniche e ottiche (Nunberg, G., 2012). Al giorno d'oggi più di 100 paesi nel mondo si impegnano quotidianamente nello scambio di dati, informazioni e opinioni attraverso Internet. In base a quanto riportato dall'Internet World Statistics, al 31 Dicembre 2011 veniva stimato un traffico di utenti su Internet pari a 2,5 miliardi equivalente al 32,7% della popolazione mondiale (Somayya Madakam, R. Ramaswamy, Siddharth Tripathi, 2015).

Per quel che riguarda il termine "things", "cose" in italiano, fa effettivamente riferimento ad un qualsiasi oggetto o persona che possa essere distinguibile nel mondo reale. Quando si parla di "things" in questo contesto possiamo ormai non limitarci esclusivamente ai dispositivi elettronici in senso stretto, poiché questo termine include qualsiasi "cosa" che sia anche scollegata dall'ambito elettronico. Proprio grazie a questa considerazione verso categorie molto distanti dall'ambito tecnologico si rivela l'importanza dell'IoT (Kosmatos, E.A., Tselikas, N.D. and Boucouvalas, A.C. 2011): l'innovazione derivante dalla capacità di includere ed armonizzare servizi su categorie di prodotti completamente differenti lo consacra come un vero punto di svolta nella storia dell'informatica.

Nonostante il chiarimento delle parole che lo compongono, risulta quasi impossibile trovare una definizione di IoT in grado di accontentare tutti, dai semplici utilizzatori ai ricercatori. Il primo ad avergli attribuito una

definizione risulterebbe essere Kevin Ashton, un esperto di innovazione digitale. Ciò che però tutte le definizioni risultano avere in comune è l'idea che la prima versione di Internet riguardasse principalmente i dati creati dalle persone, mentre la versione successiva riguarderebbe i dati creati dalle cose. La miglior definizione che si possa dare all'IoT è la seguente:

"An open and comprehensive network of intelligent objects that have the capacity to auto-organize, share information, data and resources, reacting and acting in face of situations and changes in the environment"
(Kosmatos, E.A., Tselikas, N.D. and Boucouvalas, A.C. 2011)

"Una rete aperta e completa di oggetti intelligenti che hanno la capacità di auto-organizzarsi, condividere informazioni, dati e risorse, reagire e agire di fronte a situazioni e cambiamenti nell'ambiente"

L'Internet of Things è un fenomeno in continua crescita che ad oggi si configura come uno dei trend più innovativi del mondo IT. Molta è l'attenzione che gli è stata dedicata negli ultimi anni, questo a causa della sua potenzialità che ha proiettato la visione di un'infrastruttura globale di oggetti fisici collegati in rete, ed in grado di consentire in un qualsiasi momento e luogo la connettività per qualsiasi cosa o persona (Kosmatos, E.A., Tselikas, N.D. and Boucouvalas, A.C. 2011). L'IoT può essere considerato come un network globale capace di garantire la comunicazione "*human-to-human*", "*human-to-things*" e "*things-to-things*". In sintesi, permette la comunicazione tra qualsiasi cosa al mondo fornendo un'identità unica ad ogni soggetto (Aggrarwal, R. and Lal Das, M, 2012). In questo modo ci proiettiamo un contesto in cui ogni singolo elemento può essere connesso alla rete ed è in grado di comunicare con essa in maniera intelligente. Viene completamente ribaltata l'idea per cui "essere connessi" riguardava esclusivamente l'utilizzo di dispositivi elettronici, server, computer o altro. Nell'*Internet of Things* sensori ed attuatori integrati negli oggetti fisici sono collegati tramite reti cablate e *wireless* e sono in grado di generare enormi quantità di dati che passano ai computer per le analisi (Aggrarwal, R. and Lal Das, M, 2012). Gli oggetti possono quindi percepire l'ambiente e comunicare, diventando strumenti utili alla comprensione dei fenomeni che ci circondano e alla risoluzione immediata degli stessi. Un'altra particolarità è che tutto ciò sta avvenendo tramite un processo di distribuzione su ampia scala. Questo è possibile grazie al livello di efficienza raggiunta da questi sistemi, tale da permettere loro di erogare un servizio senza più bisogno dell'intervento umano. L'IoT si riferisce alla codifica e alla messa in rete di oggetti e cose di uso quotidiano per renderli individualmente leggibili e tracciabili su Internet (Biddlecombe, E. 2009). La rivoluzione tecnologica che è in grado di garantire l'IoT è lo specchio di ciò che saranno in grado di fornirci in futuro l'informatica e le telecomunicazioni. Il suo sviluppo dipende dall'innovazione tecnica dinamica in settori riguardanti sensori *wireless* e nanotecnologie.
La prima applicazione di Internet su un oggetto non computerizzato in senso stretto si ha nei primi anni '80. In questo caso venne utilizzato un distributore per la Coca-Cola per il quale i programmatori scrissero un algoritmo che consentiva di verificare da remoto se un determinato scompartimento del distributore fosse

pieno o meno. Questo si traduceva direttamente nella possibilità di sapere se nella macchinetta una determinata bevanda era disponibile ancor prima di andare al distributore. Anche se la definizione di IoT nasce negli anni '80, come detto in precedenza, fu Kevin Auston, direttore esecutivo di Auto-ID Labs al MIT a coniarne la terminologia nel 1999. Proprio grazie al centro Auto-ID il termine IoT è divenuto sempre più popolare in particolar modo nel 2003 quando il termine aveva iniziato a comparire anche nelle pubblicazioni relative agli analisti di mercato.

1.1.2 – Definizione odierna di IoT

Dopo aver tracciato un breve *escursus* storico sulla nascita dell'IoT ed una sua primaria definizione, è giunto il momento di esaminare quanto di più recente c'è da sapere a riguardo. Inutile dire come dai primi anni '90 ad oggi la definizione dell'IoT abbia subito molti cambiamenti. L'aumento degli *smart device* ha definitivamente consacrato l'avvento di quest'ultimo arricchendone sia il palinsesto applicativo che quello letterario. Come già rimarcato in precedenza l'*Internet of Things* prometteva sin dall'inizio un nuovo paradigma tecnologico in grado di connettere tutto e tutti in un qualsiasi momento ed in un qualsiasi posto utilizzando qualunque percorso/rete o servizio (Baldini et al., 2016; Guillemin and Friess, 2009; Man et al., 2015; UK Research Council, 2013). La visione dell'IoT è quella di uno "*smart world*" attrezzato di tecnologie di rilevamento e componenti intelligenti. L'*Internet of Things* si colloca in quello che viene definito Web 3.0; un web che a differenza del suo predecessore, il Web 2.0, coinvolge in maniera molto più profonda i suoi utenti. Ciò è dovuto al fatto che questi si relazionano con un ambiente fisico e non più prettamente informatico e che va ben oltre la semplice creazione e condivisione di contenuti (Kreps and Kimppa, 2015). Non stupisce che una visione così audace abbia destato l'interesse di accademici e professionisti. È opportuno ritenere che l'IoT impatterà significativamente individui, aziende e politiche mettendo in discussione modelli aziendali, societari ed erogazione di servizi per come oggi sono conosciuti (Shin, 2014; Stankovic, 2014). Per contro la natura pervasiva dell'IoT e la continua generazione di dati potrebbero seriamente suscitare importanti preoccupazioni sull'invasione della privacy in un mondo completamente connesso. Proprio in virtù di quanto sopra citato, la mole di pubblicazioni correlate all'IoT è aumentata esponenzialmente negli ultimi anni (Olson et al.,2010). Un paper molto importante e di grande contributo alla letteratura risulta essere quello di Atzori et al. (2010), che contiene i concetti riguardanti la classificazione e l'introduzione delle tecnologie compatibili con l'IoT ed una struttura di applicazioni pertinenti ad esso in grado di suggerire nuove strade per ulteriori ricerche (Atzori et al., 2010). Seguendo un simile approccio, anche lo studio di Li et al. (2014) si preoccupa di dare una visione integrata dell'IoT, affrontandone l'architettura, le tecnologie e le applicazioni in termini prettamente tecnici. Inoltre, vengono affrontati i problemi collegati alla standardizzazione dei processi, sicurezza dei dati e privacy degli utenti (Li et al., 2014). Le tecnologie abilitanti e i problemi di sicurezza dell'IoT sono state le tematiche che hanno coperto per l'80% la letteratura esistente in merito sino al 2014 (Yan et al., 2015).

A seguito di quanto detto emerge un problema evidenziato nello studio di Li et al., ovvero la grande lacuna nella letteratura IoT legata al business. Nessuna delle review svolte sino a quel momento aveva mai fornito un'analisi delle pubblicazioni dell'IoT dal punto di vista del business. Proprio per questo motivo la terza parte di questo capitolo viene interamente dedicata all'applicazione dell'IoT nel mondo del business, a dimostrazione dell'importanza della tematica e attualità della stessa.

Come precedentemente detto esistono molte definizioni in grado di identificare l'Internet of Things, ma quelle maggiormente apprezzate dall'opinione pubblica sono tre. La prima è attribuibile ad Atzori et al. (2010) secondo cui l'IoT è il risultato della convergenza di tre visioni: una visione "orientata alle cose", una "orientata verso Internet" ed una "semantica". L'IoT è stato definito semanticamente come "una rete mondiale di oggetti interconnessi" in grado di esercitare una "presenza pervasiva" nei confronti degli utenti che a loro volta interagiscono con altri oggetti ma anche nei confronti dell'ambiente fisico che li circonda e raggiungere così obbiettivi comuni (Atzori et al., 2010).

La seconda definizione invece è stata presentata da ITU (ITU Strategy and Policy Unit, 2005; ITU-T, Y. 2060, 2012), che ha posto l'accento su come l'IoT sia ogni oggetto del mondo fisico o virtuale "in grado di essere identificato nelle reti di comunicazione".

Infine, quella che può essere considerata una delle definizioni più rappresentative è stata proposta dalla Commissione Europea, secondo cui l'IoT è un'infrastruttura di rete globale dinamica integrata in Internet in cui varie "*things*" hanno identità unica, attributi fisici, personalità virtuale e interfacce intelligenti (Guillemin e Friess, 2009). In altre parole, "l'*Internet of Things* consentirà a persone e cose di essere connessi in qualsiasi momento, in qualsiasi luogo, con qualsiasi cosa e chiunque, idealmente utilizzando qualsiasi percorso/rete o servizio" (Guillemin e Friess, 2009). Il termine "cose" agisce come una nuova dimensione dell'estensione dell'attuale interazione umana e applicativa esistente, consentendo di collegare persone e oggetti, scambiando informazioni in tempo reale attraverso qualsiasi percorso (Baldini et al., 2016; Guillemin e Friess, 2009 ; Man et al., 2015; UK Research Council, 2013).

Per quanto differenti, le definizioni sopra citate hanno vari punti di contatto. Ad esempio, condividono tutte e tre il concetto di rete dinamica, di infrastruttura globale, interconnessione ma soprattutto l'interazione tra esseri umani e cose. Lo scopo dell'IoT è rendere possibile la condivisione efficiente di informazioni in tempo reale tra attori autonomi nella rete (Yang et al., 2013). L'IoT si riferisce alla presenza pervasiva di miliardi di oggetti in grado di comunicare in maniera intelligente, connessi in una struttura simile ad Internet. L'idea finale dell'IoT è quella di considerarlo come l'estensione futura di Internet, ma anche delle città e del mondo stesso, proprio grazie alla sua capacità di comprendere oggetti smart in grado di percepire e reagire a ciò che li circonda (Ng et al., 2015; Rau et al., 2015; Shin , 2014; Stankovic, 2014).

L'architettura globale IoT facilita lo scambio di beni e servizi e l'interazione tra oggetti intelligenti, così da creare delle vere e proprie opportunità di innovazione di servizio. Quello che sostanzialmente l'IoT è in grado di garantire è un'innovazione dei processi standard come oggi li conosciamo. Grazie alle sue caratteristiche ed alla sua architettura, è uno strumento completamente nuovo e con caratteristiche di versatilità ed

applicazione uniche (Baldini et al., 2016; Dlodlo et al., 2012; Winter, 2014). Con i *social system* sempre più orientati verso una piena connettività, l'IoT è stato considerato come una vera e propria rivoluzione tecnologica ed un processo di cambiamento sociale (Elmaghraby e Losavio, 2014; Quigley and Burke, 2013; Speed, 2010; Xu, 2012). Bisogna tuttavia tener conto che il mondo sta diventando ricco di dati e ci stiamo avviando verso uno scenario in cui la condivisione e l'esposizione di dati sensibili aumenterà sempre di più, portandoci a ragionare su tematiche quali la tutela della privacy e sulla sicurezza delle informazioni (Brill, 2014; Weinberg et al., 2015).

L'ultima tematica affrontata è uno dei punti chiave su cui verterà la ricerca: la disciplina in merito alla tutela della privacy e la percezione che l'utente ha di questa. Prima di passare ad analizzare questa parte bisogna però soffermarci sulla letteratura relativa alle attività commerciali e le prospettive organizzative. Il motivo per cui affrontiamo questo argomento è che la letteratura che la riguarda questo argomento è una delle meno presenti ma più attuali. Basti considerare che è solo dal 2015 che vengono fatte ricerche di spessore sulle potenziali applicazioni di business dell'IoT (Y. Lu et al., 2018). Per questo motivo risulta opportuno darne spazio attraverso un approfondimento delle sezioni successive.

1.1.3 – IoT e Applicazioni di business

L'applicazione dei servizi IoT al mondo del business è un fenomeno in rapida espansione e il continuo aumento della letteratura a riguardo rappresenta una valida dimostrazione. È però da pochi anni che ricercatori ed accademici hanno rivolto il loro sguardo in questa direzione. Sino a pochi anni addietro si preoccupavano maggiormente della definizione di architettura dell'IoT e delle sue caratteristiche anziché i possibili utilizzi nelle varie *industry*. Per questo motivo in questa parte del capitolo analizzeremo l'applicazione dei sistemi IoT e la potenzialità del loro impatto su organizzazioni ed aziende. Successivamente alle sue applicazioni verrà trattata la questione di creazione del valore, innovazione, strategia design e sicurezza.

Riconsiderando quanto esplorato nelle sezioni precedenti possiamo certamente affermare che la gran parte dei primi prodotti IoT era stata sviluppata equipaggiando prodotti già esistenti con sensori o tag in grado di facilitare la raccolta, l'elaborazione e la gestione delle informazioni. Sempre nel 2014 alcuni dei maggiori studi di riferimento (Atzori et al., 2010 e Shin, 2014) si preoccupavano di come fosse difficile prevedere il potenziale impatto nella realtà dell'IoT, questo a causa della sua natura pervasiva e del rapido miglioramento delle tecnologie abilitanti (Atzori et al., 2010; Shin, 2014). Come è possibile vedere dalla Tabella 1 le applicazioni dell'IoT vengono riassunte in 14 domini di servizio, a loro volta classificati su quattro tipologie, a seconda della destinazione dell'obiettivo e dell'ambito. Inoltre, la classificazione si avvale di un modello di gerarchia analitica (AHP) utile valutare e confrontare la redditività e la prospettiva delle applicazioni IoT orientate al cliente, alle imprese e al pubblico (Kim e Kim, 2016). *L'analytic hierarchy process* (AHP) è una tecnica di supporto per le decisioni multicriterio sviluppata negli anni '70 dal matematico iracheno naturalizzato statunitense Thomas L. Saaty. Quello che questa tecnica ci permette di fare è confrontare più variabili intese come alternative di scelta in relazione ad una moltitudine di criteri. Questi possono essere di

tipo qualitativo o quantitativo ed il processo è in grado di ricavare una valutazione globale per ogni alternativa. Questo nel concreto garantisce l'ordinamento delle alternative a seconda della preferenza espressa e la selezione di quella che massimizza il risultato richiesto. I punti di forza principali sono: il confronto a coppie delle alternative decisionali e la separazione fra importanza del criterio e impatto sulla decisione.
Proprio per via di queste sue caratteristiche l'AHP risulta essere un ottimo strumento di misurazione per carpire quanto le applicazioni dell'IoT impattino in maniera positiva o meno l'utente finale.

Tabella 1

Application level	Service domains	Descriptions and functions
Infrastructural level	Smart environment	Concentrates on environment monitoring and protection. Wireless sensors measure environmental indicators (e.g. pollution, water quality, temperature, humidity) and proceed to the information platform, which triggers alerts and actions (Chen et al., 2014; Dlodlo et al., 2012).
	Smart city	City equipped with various IoT devices and systems, aimed at monitoring, analysing and sharing information and coordination within a city system (Chen et al., 2014; Shin, 2014). Helps governments and other stakeholders to improve city planning (Atzori et al., 2010; Chen et al., 2014).
	Smart energy	Enhances users' awareness of usage control by services such as smart power grid, smart meter, and remote meter reading (Chen et al., 2014; Dlodlo et al., 2012; Shin, 2014).
	Smart tourism	A networked system of tourism destination including industries, services, and visitors in emerging forms of technological infrastructure that facilitates data transformation into value propositions, supports cooperation, knowledge sharing, and open innovation (Del Chiappa and Baggio, 2015; Gretzel et al., 2015). The tourism supply chain management can be enhanced with geospatial data enabled by IoT technologies, thus improving sustainability in tourism destinations (Babu and Subramoniam, 2016).
Organisational level	Smart logistics and supply chain management	Contributes to shortening process and reaction period by obtaining real-time information monitoring for enterprises (Atzori et al., 2010; Chen et al., 2014). It also facilitates resource utilisation, quality management, safety and traceability (Dlodlo et al., 2012).
	Smart agriculture	Conservation status monitoring and transportation management, facilitating inventory control, distribution management, and logistics of perishable agricultural products (Atzori et al., 2010; Chen et al., 2014; Dlodlo et al., 2012; Shin, 2014).
	Industrial plants and manufacturing	Optimising the production process in digitalised industrial plants by deployment of identification tags and interaction with the intelligent network (Atzori et al., 2010; Dlodlo et al., 2012). This enhances process controlling and tracking, industrial environment monitoring, product lifecycle monitoring (PLM), safety and security, energy saving, and pollution control in production processes (Chen et al., 2014).
Individual level	Smart home	Enabled by connecting items and devices at home which form a wireless sensor network to enhance applications in security, intelligent indoor environment control, household appliance control, smart metering and energy saving, thus creating a smart and comfortable private space (Atzori et al., 2010; Chen et al., 2014; Dlodlo et al., 2012; Risteska Stojkoska and Trivodaliev, 2017). The devices, data processing hubs, the cloud, and third party applications constitute a general smart home management system/platform that clarifies the specific tasks and requirements for smart homes (Kiesling, 2016; Risteska Stojkoska and Trivodaliev, 2017).
	Entertainment and gaming	Intelligent system that can adjust the game activity and difficulty level with the excitement and energy levels of the gamer by sensing the parameters of the players (Atzori et al., 2010).
	Social networking	Smart devices automatically update information about the users' real-time location, mutual friends' meeting, and attendance at events or social web pages, which reduces effort (Atzori et al., 2010; Dlodlo et al., 2012).
	Smart safety	Protects personal and community property by reading identification tags to alert owners or security guards when an item is moved without authorisation and recording location information of the movement to help users track items (Atzori et al., 2010; Dlodlo et al., 2012). Ensures safety in both public and private spaces by controlling the accessibility of critical information which requires personal identification, monitoring dangerous cargo, food and water safety, alerting and responding to emergencies in communal facilities (Chen et al., 2014; Dlodlo et al., 2012).
All-Inclusive level	Smart transportation	Auto-control and intelligent regulation of connected vehicles effectively reduces time spent on commuting and energy consumption. Provides real-time road status, navigation, and assisted driving to the users and improves road safety and transportation efficiency (Atzori et al., 2010; Chen et al., 2014; Dlodlo et al., 2012; Shin, 2014).
	Medical and healthcare	Devices provide opportunities for remote and participatory medical services by monitoring personal health conditions and alerting for potential disease (Amendola et al., 2014; Chen et al., 2014; Dlodlo et al., 2012; Shin, 2014). Patient and medical resource management systems in hospitals and pharmacies, contribute to more efficient and effective treatments (Atzori et al., 2010; Chen et al., 2014; Dlodlo et al., 2012; Shin, 2014).
	Education	Applications facilitate learning by controlling the class environment (measuring physical environment parameters), and by embedding knowledge within objects and automatically adjusting local conditions to improve the effectiveness of study (Adorni et al., 2012; Atzori et al., 2010; Dlodlo et al., 2012; Uzelac et al., 2015).

Il modello si compone di 3 criteri principali a loro volta segmentati in 11 sottocriteri ed ordinati gerarchicamente: prospettive tecnologiche (praticità tecnica, affidabilità tecnica, efficienza dei costi e standardizzazione); potenziale di mercato (domanda di mercato, accettazione degli utenti, modello di business e costruzione degli ecosistemi); ambiente normativo (regolamentazione industriale, protezione del consumatore e supporto governativo).
Tra i criteri appena elencati, il più importante è sicuramente il potenziale di mercato. Applicando il modello AHP i ricercatori hanno scoperto che l'applicazione più promettente dei sistemi IoT riguarda la logistica IoT, seguita rispettivamente da IoT *healthcare* e IoT *energy management* (Kim e Kim, 2016). In seguito, ci andremo a soffermare proprio sull'IoT *healtchare*. Le tecnologie IoT, come quelle descritte sino ad ora, hanno

le potenzialità per poter spostare il mercato da un esperimento di innovazione tecnologica ad una strategia aziendale convincente. Questo è possibile poiché l'IoT ha le caratteristiche per poter:

- Sbloccare l'eccesso di capacità delle risorse fisiche.
- Creare un mercato liquido e trasparente.
- Consentire una rivalutazione radicale del credito e del rischio.
- Migliorare l'efficienza operativa.
- Integrare il digital nelle catene del valore.

(Brody e Pureswaran, 2015).

Per le prospettive future legate al business, risulta fondamentale saper riconoscere l'importanza delle opportunità e adeguare di conseguenza le strategie in base al mercato ed alle preferenze espresse dagli utenti. Tutto ciò sarà in grado di migliorare le prestazioni dei servizi erogati dalle organizzazioni, questo grazie ad una trasformazione che avverrà all'interno delle aziende, attraverso la digitalizzazione e connessione di risorse fisiche all'IoT (Brody e Pureswaran, 2015).

1.1.3.1 – Innovazione dei servizi: benefici e opportunità

L'IoT sembrerebbe quindi essere la chiave di volta in grado di modificare i processi industriali e commerciali esistenti e creare nuovi valori economici e di mercato (Dutton, 2014; Kim e Kim, 2016; Santoro et al., 2017). Nell'economia del futuro, guidata dalla conoscenza, le innovazioni rese possibili da prodotti e processi rivitalizzati dall'IoT potrebbero essere uno dei fattori trainanti in grado di rafforzare i vantaggi finanziari e competitivi (Del Giudice, 2016). È proprio il valore che i sistemi IoT sono in grado di creare a determinarne l'adozione o meno, aprendo una serie di opportunità capaci di collegare attività, risorse e attori nelle reti aziendali (Andersson e Mattsson, 2015).

L'integrazione dell'IoT nelle organizzazioni accelera la creazione di valore e migliora i servizi verso i clienti, in particolare applicando il framework CSLC (*Customer Life Cycle*), potenziato dai flussi di dati digitali formatisi dall'adozione di massa di dispositivi IoT (Ives et al., 2016). L'utilizzo della struttura CSLC nei sistemi informativi aiuta le aziende a comprendere e migliorare i servizi per i clienti sfruttando le innovazioni IoT nelle diverse fasi. Dal punto di vista della rete aziendale, tutti gli attori, le attività e le risorse possono essere considerati intermediari utili nel processo di *networking* della trasformazione. L'evoluzione delle tecnologie IoT tende a dare sempre maggiore spazio agli *smart device* nella vita delle persone e nelle attività organizzative (Andersson and Mattsson, 2015). Per quanto riguarda l'innovazione del servizio, risulta avere importanza cruciale il modello di business. Quest'ultimo è un fattore rappresentativo della mediazione tra tecnologia e valore economico in senso stretto. È fondamentale che questo sia in armonia con gli altri attori del processo (Andersson and Mattsson, 2015). Assume primaria rilevanza per un'impresa definire, od eventualmente ridefinire, il proprio modello di business, applicandosi in specifici settori al fine di allinearsi con le diverse tendenze, in rapida crescit,a della tecnologia. Tutto ciò per creare valore aggiunto ed ottenere

un vantaggio competitivo nei confronti dei suoi *competitor* (Chui et al., 2010; Dutton, 2014; Gretzel et al., 2015; Pisano et al., 2015). In questo senso l'IoT è in grado di impattare i modelli di business, innovando quelli vecchi ed agevolandone di nuovi (Gerpott and May, 2016).

1.1.3.2 – Strategia e logistica

La visione del prodotto del futuro è quella incentrata sul cliente: la *customer experience* sarà l'offerta più importante che l'IoT dovrà garantire (Brody e Pureswaran, 2015). La moltitudine di *devices* connessi ad Internet permetterà alle aziende di condurre ricerche di mercato sempre più precise e accurate. Tutto ciò garantirà una conoscenza dei propri clienti sempre più dettagliata basata sul loro comportamento (Ng et al., 2015). Questo offre l'opportunità di personalizzare le strategie e offrire prodotti customizzati per i clienti attraverso un'efficiente *supply chain*. Quelle che emergono come migliori strategie di gestione della *supply chain* risultano essere il "*tailoring*" ed il "*platform*" (Ng et al., 2015). Queste due tipologie strategiche di personalizzazione sono quelle che vengono maggiormente raccomandate a chi fornisce prodotti nell'era IoT. La strategia di "tailoring" fa leva sulla capacità del fornitore di produrre un crescente numero di prodotti su misura per soddisfare la domanda dei clienti. La strategia di "*platform*", invece pone l'accento sulla capacità da parte del fornitore di produrre un prodotto/*platform* standardizzato, contenente dati personali, che consenta ai clienti di acquistare ulteriori prodotti personalizzati realizzati da altri fornitori ma compatibili con il prodotto/*platform* d'origine. Questo consentirebbe una personalizzazione continua dell'esperienza percepita dal cliente (Ng et al., 2015).

Entrambe le strategie sono da considerarsi redditizie grazie alla massimizzazione della customer experience e quindi del valore ad essa associato. L'unico vantaggio che la strategia "*platform*" risulterebbe avere su quella "*tailoring*" è che la prima è in grado di soddisfare puntualmente la domanda qual ora si verificasse un aumento di questa in termini di varietà contestuale (Ng et al., 2015).

In merito all'ambito logistico, l'IoT può essere utilizzato per garantire "il trasporto autonomo e controllato di oggetti dal mittente al destinatario" (Bremer, 2015), migliorandone il servizio e la competitività. Il meccanismo di creazione del valore della tecnologia IoT è strettamente collegato alla capacità di generare informazioni in grado di facilitare l'ottimizzazione dei flussi dei processi aziendali, i processi industriali, la manutenzione predittiva, fornendo soluzioni di servizio efficienti (Del Giudice, 2016).

1.1.3.3 – Sicurezza, responsabilità e design etico

In ultima istanza tratteremo la parte riguardante la sicurezza, le responsabilità e la componente etica. È una tappa fondamentale del percorso condotto sino ad ora perché va a porre la lente d'ingrandimento sulla relazione esistente tra la generazione dei dati che l'IoT provoca e come questi impattino la *customer experience*. Perché se è vero che le tecnologie IoT registrano dati di rilevamento ambientale, gran parte di questi si compone di dati sensibili dell'utente ed è necessario vedere come la raccolta dei dati venga percepita

dall'opinione dell'utilizzatore e regolata dal quadro legislativo in cui questa si colloca. In questa sezione la tematica verrà affrontata in maniera rapida e meramente espositiva, questo perché la tutela della privacy ed il trattamento dei dati sensibili saranno argomento centrale del prossimo capitolo.

Come accennato poche righe sopra è importante affrontare le problematiche sottostanti in materia di privacy e sicurezza al fine di ottimizzare la distribuzione dei benefici e del valore dei prodotti IoT verso gli utenti. Per come è strutturato l'IoT, la sicurezza è fondamentale sia a livello di prodotto fisico che a livello di servizio/applicazione: ciascuno degli strati componenti l'architettura dei servizi IoT (rilevamento, servizio e interfaccia) si rivolge a potenziali minacce, perciò è necessario adottare contromisure appropriate (Li et al., 2016). Per quanto esista una legislazione per garantire le informazioni in termini di privacy, riservatezza, integrità, autenticità e disponibilità di utilizzo, la protezione in senso stretto può essere garantita solo dal sistema e dai processi di progettazione etica in unità di business (Elmaghraby e Losavio, 2014). La criminalità organizzata e il terrorismo cybernetico sono delle realtà che generano grande preoccupazione nei confronti della società, dal momento che gli impianti di produzione, le infrastrutture critiche (rete elettrica, oleodotti, ecc.), le case intelligenti e la proprietà intellettuale sono tutti collegati ed integrati nel mondo IoT (Bradley et al., 2014).

Data la natura dell'IoT, è ovvio pensare che la mole di dati, informazioni e conoscenze generate che vengono raccolte e trasferite tra mondo virtuale e fisico sia di ampia scala. Emerge quindi, in maniera piuttosto evidente, il problema collegato alla sicurezza (Baldini et al., 2016; Popescul e Georgescu, 2013). Le minacce alla sicurezza derivano da ogni strato nell'architettura IoT, causando non pochi problemi in termini di analisi dei rischi di sicurezza a causa delle ampie dimensioni dell'IoT (Bradley et al., 2014). "La sicurezza include ... [protezione da] ... accesso illegale alle informazioni e attacchi che causano interruzioni fisiche nella disponibilità del servizio" (Elmaghraby and Losavio, 2014).

Le questioni etiche più comuni relative all'IoT sono sintetizzate in quattro aspetti (Caron et al., 2016; Popescul and Georgescu, 2013) chiave:

- La privacy: intesa come il diritto di far valere il diritto ad una vita privata limitandone la rivelazione di informazioni.
- L'accuratezza: garantire l'autenticità, l'integrità e responsabilità delle informazioni.
- La proprietà: far valere il diritto di possesso delle informazioni.
- L'accesibilità: assicurare il diritto di ottenere specifiche informazioni.

Una delle sfide etiche vitali riguardanti il diritto di proprietà dei dati personali e delle informazioni interessa l'identificazione. Lo sviluppo di oggetti dotati di sensori consente loro di raccogliere e inviare dati in grandi quantità e in diversi modi i attraverso Internet senza l'intervento umano (Popescul e Georgescu, 2013). Dal lato economico, le sfide etiche provengono dalle "scelte consapevoli derivanti da incentivi malriposti", grazie ai quali gli incentivi economici delle organizzazioni imprenditoriali dipendono dalla creazione di applicazioni

o dispositivi che raccolgono i dati degli utenti invece di proteggerli, soprattutto nel *trading* dei dati tra utenti ed imprese (Baldini et al., 2016).

Un prodotto IoT basato sul design etico dovrebbe avere quattro caratteristiche:

- Capacità di fornire controllo e consapevolezza nella raccolta e distribuzione dei dati agli utenti.
- Capacità di attuare normative diverse nel tempo e nello spazio.
- Capacità di supportare contesti dinamici.
- Capacità di percepire e supportare scelte etiche

(Baldini et al., 2016)

Il processo di sviluppo dei prodotti IoT può essere riassunto in quattro fasi principali:

- Comprendere ed includere la fiducia che gli utenti hanno verso le applicazioni, i prodotti e i servizi; questo vale sia a livello pubblico che privato.
- Il coinvolgimento degli utenti nel processo di progettazione aiuta a tradurre e includere le loro esigenze e i loro valori nel prodotto/servizio.
- La semplicità e la trasparenza della raccolta, dell'utilizzo, della conservazione e dell'accessibilità dei dati dovrebbero essere dimostrate e comprese dagli utenti.
- Stabilire un quadro legale e la responsabilità della privacy e della fiducia degli utenti per migliorare maggiormente l'ambiente IoT.

1.1.4 – Numeri e forecast del mercato IoT

Dopo aver ampiamente parlato nelle sezioni precedenti dell'Internet of Things sia in termini tecnici che in termini applicativi è giunto il momento di fare un quadro della situazione odierna. Questa volta però non cureremo la parte descrittiva del fenomeno, bensì quella numerica. Andremo a misurare il livello a cui è arrivata la diffusione della tecnologia IoT sul mercato ed anche quali sono le previsioni per il futuro.

Abbiamo quindi visto come sicurezza, integrazione con la tecnologia esistente e i ritorni sugli investimenti siano i tre maggiori ostacoli con cui, ad oggi, l'IoT ha a che fare. Bain ha rilevato che le imprese sarebbero più propense ad acquistare dispositivi IoT, pagandoli sino al 22% in più, se venissero affrontati in maniera più massiccia i problemi collegati alla sicurezza (Figura 1). Il processo integrativo dei sistemi IoT continua ad essere un ostacolo; questo è dovuto al fatto che i fornitori non hanno semplificato questo elemento per le soluzioni IoT nei sistemi aziendali quanto le imprese si aspettavano. La soluzione consisterebbe nell'aumento degli investimenti da parte dei venditori per la semplificazione del processo d'integrazione dei sistemi IoT, cosa che permetterebbe alle imprese di garantire soluzioni strategiche end-to-end migliori.

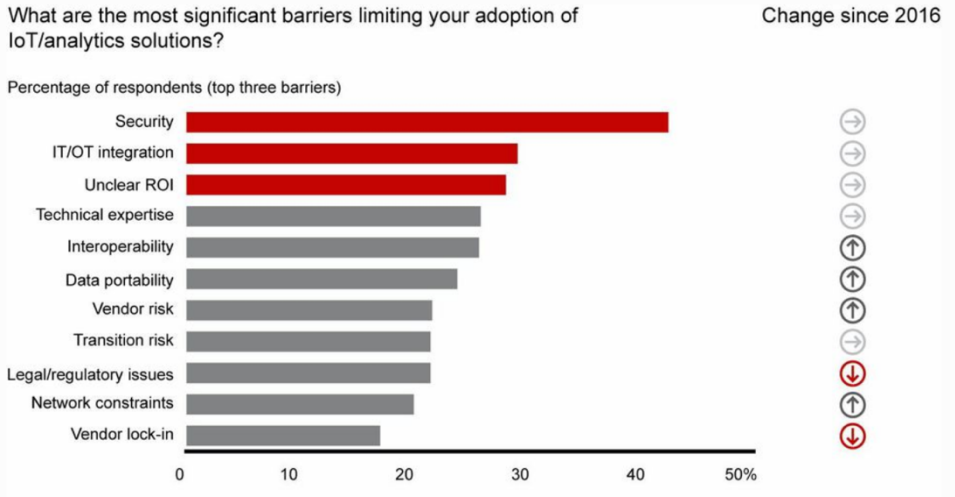


Figura 1 – Sources: Bain IoT customer survey, 2016, Bain IoT customer survey 2018; market partecipant interview

Le previsioni di crescita del mercato aggregato per *l'Internet of Things* stimano un aumento del volume di spesa nel mercato sino a 520 milioni di dollari entro il 2021, quasi il doppio rispetto ai 235 milioni di dollari del 2017. I segmenti per i quali è prevista una crescita maggiore saranno il *data center* e l'analisi, raggiungendo un tasso di crescita annuale composto (CAGR) del 50% dal 2017 al 2021. Integrazione dei sistemi, *data center&analytics*, rete, dispositivi *consumer*, connettori e sistemi *embedded legacy* saranno invece le sei aree principali di applicazione dei sistemi IoT. In Figura 2 è possibile vedere un confronto fra i CAGR di ciascuna area e le entrate mondiali per categoria.

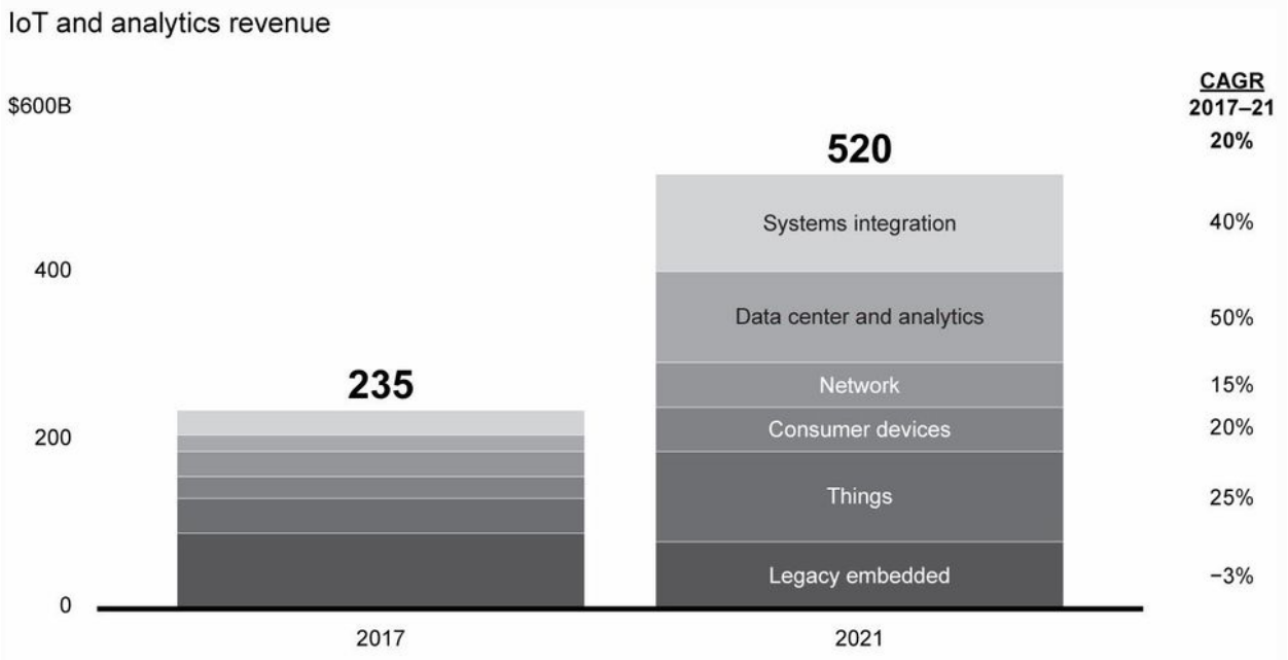


Figura 2 – Sources: Gartner; IDC; Harbor; Cisco, Ericsson;Machina Research; Ovum; Bain analysis; market participant interviews

Viste le previsioni stimate per il futuro, il mercato rimane ancora ottimista sul valore di business dell'IoT e sulla possibilità di fornire un ROI positivo. Tuttavia, molti pianificano implementazioni IoT meno estese entro il 2020. Bain ritiene che le imprese stiano ancora eseguendo molte prove di concetto, in quantità maggiore

rispetto a due anni fa. È emerso inoltre, che più clienti stanno valutando di provare nuovi casi applicativi; trend in netta crescita dal 2016 ad oggi (Figura 3).

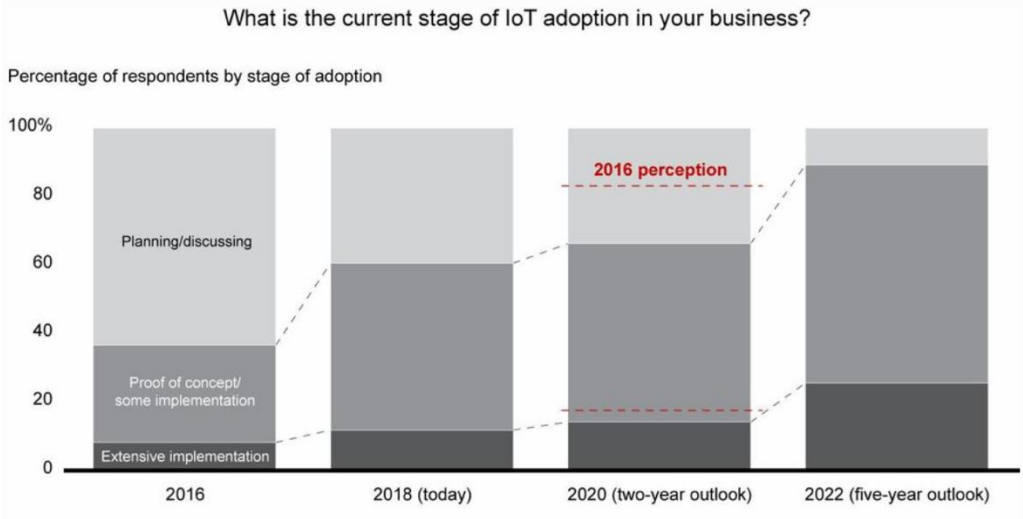


Figura 3 – Sources: Bain IoT customer survey, 2016, Bain IoT customer survey 2018

I fornitori si stanno concentrando su due o tre settori al fine di scalare velocemente la profondità della loro esperienza. Oltre l'80% devi venditori punta ancora su 4-6 settori (Figura 4), rendendo difficile il raggiungimento di una scala di competenze e conoscenze tali da conquistare nuovi clienti. Ciò che emerge dalle ricerche condotte da Bain è che la concentrazione su due o tre domini permette di acquisire una maggiore padronanza nei mercati specifici. Tradotto, questo significa poter fornire informazioni più dettagliate e precise in maniera più veloce ed efficiente alle imprese. Acquisire esperienza in due o tre settori chiave è anche un'eccellente strategia di differenziazione per competere nel mercato dei fornitori.

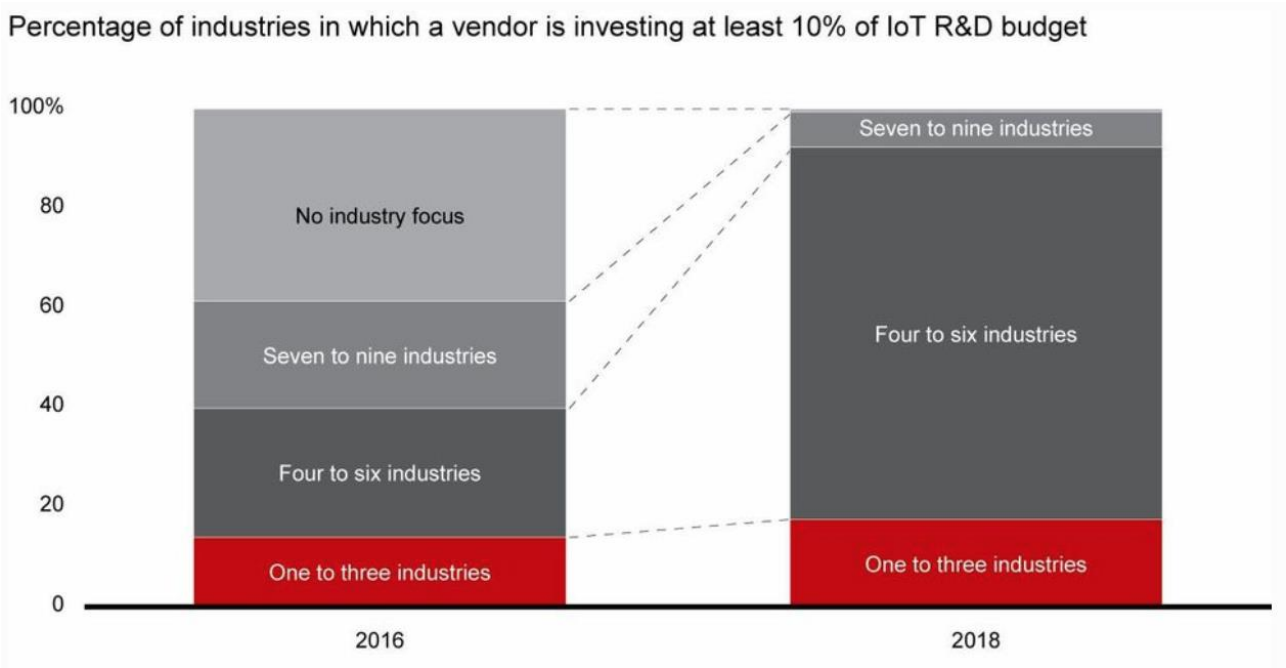


Figura 4– Sources: Bain IoT vendor survey, 2016, Bain IoT vendor survey 2018

1.1.5 – IoT Healthcare: focus

In questa sezione trattiamo, infine, il tema principale dello studio: l'applicazione dei sistemi IoT all'ambito medico/sanitario. Arrivati a questo punto abbiamo acquisito una confidenza tale da poter parlare di questo fenomeno di business come uno dei quali avrà maggiore seguito, in termini di crescita, negli anni futuri.

Negli ultimi anni il settore sanitario ha concentrato gli sforzi sull'ottimizzazione delle procedure di gestione dell'inventario attraverso l'integrazione della tecnologia di informazione e comunicazione grazie all'introduzione di dispositivi di localizzazione e data mining, in grado di definire dei veri e propri modelli di inventario ideali.

Con l'adozione della metodologia di roadmapping è stata sviluppata una tabella di marcia degli sviluppi nella gestione dell'assistenza sanitaria con tecnologie IoT, per il periodo 2010-2020 (Figura 5) (Cheng et al., 2014). Molti ricercatori sono stati attivi sulla ristrutturazione dell'assistenza sanitaria che utilizza le tecnologie IoT nella gestione ed ottimizzazione delle risorse mediche (Lee & Paladan, 2014; Ng et al., 2014), (Jara , 2014; Xu et al., 2014a; Jara et al., 2010) monitoraggio delle situazioni sanitarie (Shahamabadi et al., 2014; Sung & Chang, 2013; Castellani et al., 2012; Istepanaian & Zhang, 2012; Luo et al., 2012; Sung & Chiang, 2012; Istepanian et al., 2011), ed aumento dell'uso dell'assistenza domiciliare (Monares et al., 2014; Sebestyen et al., 2014; Yang et al., 2014; Yang et al., 2014a; Pang et al., 2013; Tarouco et al., 2012).

L'IoT Healthcare è un promettente scenario di applicazioni IoT B2C, in cui i consumatori (pazienti) sono tenuti sotto osservazione da remoto. Usando dispositivi e dispositivi di largo consumo, i bio-dati dei propri utenti (ad es. percentuale di grasso corporeo, pressione sanguigna o livello di glucosio) vengono raccolti in modo persistente e costante attraverso sensori, immagazzinati e quindi trasmessi ai fornitori di servizi medico/sanitari (es. medici o aziende). Gli erogatori del servizio sanitario sono quindi in grado di diagnosticare da remoto i propri clienti, dare consigli o prescrizioni, settare i dispositivi medici di proprietà degli utenti e persino trasmettere documenti dei pazienti agli ospedali locali (Chen, 2012; Jung e Chung, 2013; Miorandi et al., 2012). Il servizio che l'assistenza sanitaria IoT può garantire varia a seconda del monitoraggio dell'attività dell'utente. Questo significa che il potenziale dell'IoT è illimitato al fine di innovare i servizi medici e sanitari.

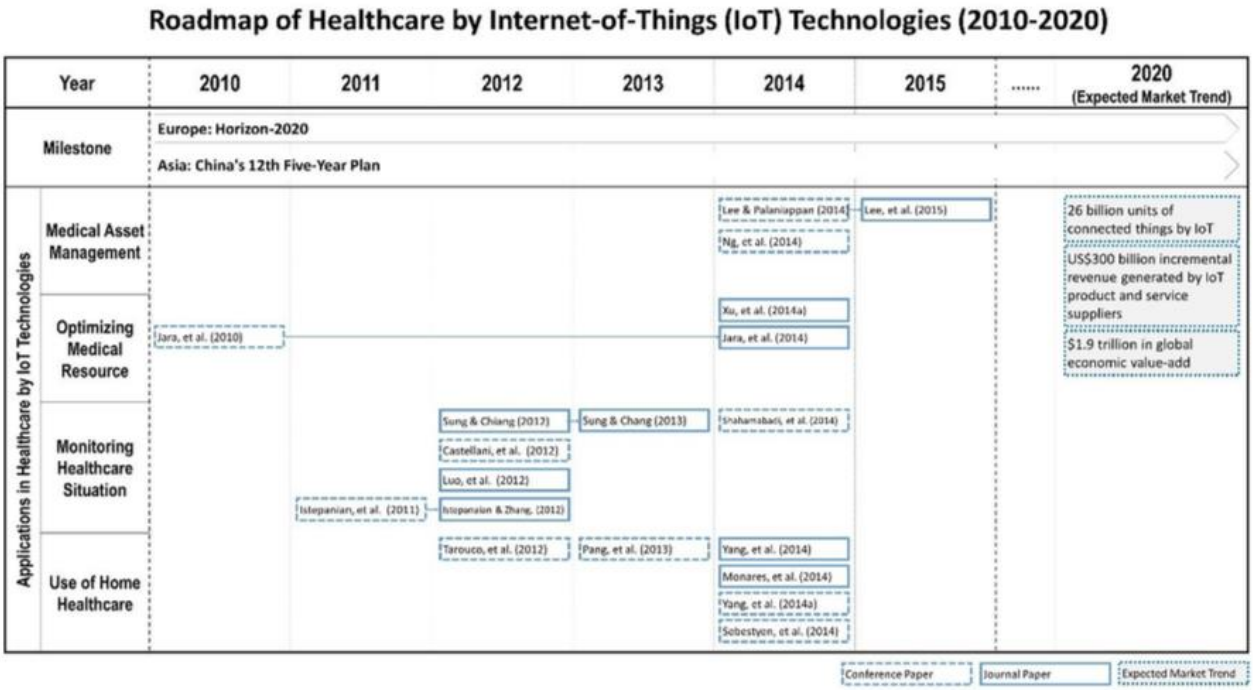


Figura 5 – Sources: Roadmap of Healthcare Industry by Internet-of-Things (IoT) Technologies (2010–2020)

Con l'aspettativa che la sanità IoT migliorerà i servizi in termini di praticità e accessibilità, dando vita a servizi avanzati dimostra di avere un grande potenziale commerciale. Al contempo anche l'IoT *Healthcare* presenta le criticità comuni a tutti gli altri business di cui trattato sopra. Le critiche mosse in questo senso riguardano l'accettazione da parte degli utenti e nella regolamentazione a livello legislativo. Inoltre, in questo specifico caso si pone il problema dell'"invasione" dell'autorità degli esperti medici che potrebbero resistere ad una eventuale migrazione dei pazienti verso relazioni remote e virtuali tra pazienti e medici.

1.2 – Il concetto di privacy: nascita ed evoluzione della disciplina

Dopo la revisione dedicata all'IoT nel capitolo precedente risulta doveroso, se non necessario, approfondire il concetto di privacy ed il suo legame con il mondo dell'Internet of Things. L'unione che l'IoT genera tra mondo reale e mondo virtuale comporta la creazione di moltissimi dati, nella maggior parte dei casi dati personali. Ecco perché adesso ci occuperemo di analizzare come la disciplina della privacy intende regolare questo fenomeno e come tutelare il consumatore.

Il termine "privacy", traducibile in italiano con "riservatezza", indica il diritto della riservatezza delle informazioni personali e della propria vita privata. "*The right to be let alone*" ("il diritto di essere lasciati in pace"), secondo il giurista statunitense Louis Brandeis che fu probabilmente il primo in assoluto a formulare una legge sulla riservatezza ("Storia della Privacy"; Michele Iaselli, Stefano Gorla –ed. Lex et Ars-2015). Comunemente per privacy si intende il diritto della persona di impedire che le informazioni che la riguardo vengano trattate da altri senza il proprio consenso ("Storia della Privacy"; Michele Iaselli, Stefano Gorla –ed. Lex et Ars-2015). Con l'introduzione dei primi mezzi tecnologici gli studiosi si sono posti il problema del rapporto "riservatezza-computer", in quanto l'impiego di elaboratori elettronici di fatto consente di impadronirsi ed archiviare dati riguardanti la persona compresi quelli della sua vita privata. Il "*right to*

privacy" ha di conseguenza acquisito un significato più ampio che non aveva in passato: al cittadino è riconosciuto il diritto di esercitare anche un controllo sull'uso dei propri dati personali inseriti in un archivio elettronico. Il diritto alla riservatezza diventa affermazione della libertà e dignità delle persone nonché capacità di limitare il potere informatico controllandone mezzi e fini ("Storia della Privacy"; Michele Iaselli, Stefano Gorla –ed. Lex et Ars-2015). L'evoluzione che ha portato alla nuova concezione di privacy si è ottenuta lentamente attraverso i secoli, pertanto andremo a ripercorrere, seppur sinteticamente, la sua storia.

1.2.1 – Nascita del concetto di privacy

Le origini moderne della privacy vengono attribuite a due giuristi statunitensi Samuel Warren e Louis Brandeis, autori nel 1890 di un saggio intitolato "*The right to privacy. The implicit mode explicit*". I due avvocati preparavano una causa contro la "Evening Gazzette" di Boston, uno dei primi giornali ad utilizzare la stampa a rotativa, per aver pubblicato indiscrezioni sulla vita matrimoniale dello stesso Warren. I due si ritrovarono quindi a riflettere su quali informazioni riguardanti la vita personale di un individuo dovessero essere di dominio pubblico e quali, invece, meritassero tutela dalla curiosa invadenza altrui.

In Europa un primo accenno storico-giuridico alla privacy è riscontrabile in area germanica, dove, tra la fine del XVIII secolo e l'inizio del XIX si iniziò a discutere sull'esistenza di una categoria di diritti conosciuta come Persönlichkeitsrechte o Individualrechte. Solo nel 1954, con una sentenza del Bundesgerichtshof, venne sancita l'appartenenza di un generale diritto della personalità alla nozione di ulteriore diritto. Il dibattito sul pieno riconoscimento giuridico ai diritti della personalità si estese oltre i confini germanici e soprattutto in Francia, dove nel 1909 venne legittimata la categoria dei diritti della personalità grazie all'opera di Perreau, che contribuì in maniera determinante al successo della categoria. Contemporaneamente in Italia si sviluppava un percorso portato avanti da Adolfo Ravà, docente di filosofia del diritto. Partendo da un'analisi del "Tractatus de potestate in seipsum" di Baldassare Gomez de Amescua giurista spagnolo del XVI secolo, Ravà coniugava filosofia e diritto per individuare la personalità giuridica come "diritto sulla propria persona". Molti anni più tardi lo stesso Ravà individuò tra i diritti della personalità un diritto che emerse dal rapporto per analogia legis di diverse norme: il c.d. diritto alla riservatezza. Le prime pronunce di violazione, risalenti agli anni '50, furono generate da opere cinematografiche e pubblicazioni relative a vicende personali di personaggi noti, che portarono gli interessati ad chiedere il diritto alla riservatezza di fronte ai giudici. Tra i provvedimenti di maggiore importanza si ricorda la sentenza emessa nel 1963 dalla Cassazione, riguardante una serie di articoli pubblicati dal settimanale "Tempo", sulla vita intima di Claretta Petacci, amante del Duce, e ritenuti offensivi dai congiunti della stessa che fecero causa al settimanale. La Corte, in questo caso, emise una sentenza decisiva, che mutò la rigida posizione iniziale su questo tema. Il cambiamento decisivo avvenne nel 1975, anno in cui il Supremo Collegio affermò l'esistenza alla riservatezza. La causa era relativa alle controversie tra Soraya Esfendiari e alcuni giornalisti che avevano pubblicato foto ritraenti l'ex imperatrice in atteggiamenti intimi nella sua casa. Anche a livello europeo il dibattito faceva progressi e così dopo la convenzione di Strasburgo e le varie interpretazioni degli Stati nazionali, la tutela della riservatezza come

protezione dei dati personali veniva ribadita in una serie di provvedimenti comunitari: la direttiva 95/46/CE (relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati), la 97/66/CE (sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni) e la 2002/58/CE (relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche. In Italia la direttiva 95/46/CE determinò l'adozione della 1.n.675 del 31Dicembre 1996, che istituisce la figura del Garante per la protezione degli stessi dati. L'adozione della 1.675 fu un obbligo: l'Europa avrebbe permesso di godere dei benefici dell'Accordo di Schengen solo se il paese membro avesse adeguato la normativa sul trattamento dei dati personali. Il successo del diritto al rispetto della vita privata è stato consacrato dall' art.8 (art.8, 1°comma della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali; CEDU ai sensi del quale "ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza") della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

1.2.2 – La privacy nell'era digital

Oggi la digitalizzazione ha un ruolo principale in tutto il mondo. Infatti, lo scambio di mail, messaggi, foto e video è ormai di ordinaria amministrazione, soprattutto con l'importante avvento dei social network, in cui ogni giorno aumentano gli utenti. Diventa quindi fondamentale prestare attenzione alla tutela della privacy. Nell'ambito dei social media il codice della privacy garantisce a chiunque il diritto di verificare la correttezza del trattamento dei dati; intervenire per revocare il proprio consenso al trattamento ("Storia della Privacy"; Michele Iaselli, Stefano Gorla –ed. Lex et Ars-2015). Nel Novembre 2013 l'ONU ha approvato la risoluzione sul "Diritto della privacy nell'era digitale", il primo documento che stabilisce che i diritti umani "dovrebbero prevalere indipendentemente dal medium e dovrebbero quindi essere protetti sia offline che online" come fatto notare, in apertura di sessione dal rappresentante del Brasile. La risoluzione approvata senza votazione, richiama gli Stati membri a rivedere le loro "procedure, prassi e legislazioni in materia di sorveglianza delle comunicazioni, intercettazioni e raccolta dati personali, compresa la sorveglianza di massa al fine di rafforzare il diritto alla privacy, garantendo la piena ed effettiva attuazione di tutti gli obblighi rilevanti ai fini delle norme internazionali sui diritti umani" così si legge nel documento pubblicato dall'ONU. Per rafforzare il tema della tutela della privacy, la Commissione europea ha emanato un nuovo regolamento. Anche nelle aziende, l'argomento sulla tutela dei dati è sempre più al centro dell'attenzione, soprattutto nel momento della programmazione di nuovi software. In particolare, l'archiviazione sostitutiva ha condizionato le nuove tutele sulla privacy, in modo da garantire la protezione delle informazioni durante il trasferimento dati. Sono stati, infatti, istituiti nuovi protocolli di protezione, molto importanti per chi sviluppa software ed eroga servizi ICT per le aziende. Oggi si parla di "privacy be design" e "privacy be default". La prospettiva e lo scopo è quello di fare in modo che anche la privacy possa essere digitale e quindi fare in modo che tutti i dati raccolti all'interno del software possano eliminare il rischio di violazioni della privacy. Oggi il web rappresenta la principale applicazione di quello che può essere definito l'Internet "tradizionale" nel quale l'intervento umano

è ancora predominante, ad es. cercare informazioni tramite un motore di ricerca, fare acquisti, interagire sui social media. Nel mondo IoT, invece, i sensori sono in grado di operare quasi totalmente in autonomia. L'uso di sensori (di varia natura, dimensione, complessità e costo) permette di raccogliere, analizzare e trasmettere enormi quantità di dati, inclusi quelli relativi al comportamento delle persone. Quindi sebbene la prospettiva dell'adozione dei sistemi IoT sia interessante e promettente i rischi legati all'uso e allo sfruttamento dei Big data sollevano molta preoccupazione riguardo a come e da chi queste enormi quantità di dati siano utilizzati. La preoccupazione più ricorrente riguarda proprio la tutela della privacy delle persone, visto che, nel caso dei Big data, l'anonimizzazione dei dati può essere aggirata abbastanza facilmente, incrociando opportunamente i tanti e vari dati raccolti sulle persone e analizzandoli con tecniche sofisticate di *big data analysis.* Da ciò deriva che possano essere aperti varchi nei confronti della privacy e della libertà delle persone.

1.3– Regolamentazione

In quest'ultima sezione di revisione della letteratura, prima di passare alla domanda di ricerca, tratteremo la relazione tra servizi IoT e regolamentazione del mercato. Verrà poi posta particolare attenzione sulla tutela della privacy. Parleremo quindi di quali siano gli effettivi rischi cui l'utente si espone durante la fruizione del servizio e come l'utente stesso percepisca tali rischi.

1.3.1 – Principali rischi e studio del fenomeno

La regolamentazione è un "mezzo per il controllo sociale della tecnologia" (Braun e Wield, 1994). Le tecnologie IoT presentano intrinsecamente una dipendenza maggiore o totale sulle macchine. L'utilizzo di dispositivi IoT può essere accompagnato da problemi etici e tecnici, come la sicurezza pubblica, l'affidabilità la responsabilità legale e la privacy. Se un'applicazione IoT non riesce ad ottenere una giustificazione per tali problemi da parte delle autorità di regolamentazione, la sua commercializzazione sarà limitata o non inizierà nemmeno la fruizione. Affinché un'applicazione IoT possa avere esito nel mercato e nella società, deve superare anticipatamente l'incertezza normativa (Dutton, 2014). Inoltre, il supporto politico e finanziario del governo può rendere un'applicazione IoT più promettente tramite l'utilizzo di questa. L'ambiente normativo attorno ad un'applicazione IoT deve essere esplorato e considerato un fattore critico capace di influire sulla sua possibilità di realizzazione.

La regolamentazione industriale si pone come primo obbiettivo la promozione di una concorrenza leale sul mercato, in grado di incoraggiare l'innovazione e l'aumento del benessere sociale. La politica industriale influisce sul vantaggio comparativo di un'azienda nel tempo influenzando lavoro, capitale, tecnologia ed innovazioni (Sabonienė, 2010). Le applicazioni IoT porteranno un'enorme trasformazione della composizione competitiva nel mercato esistente, concorrendo e cooperando con i *player* attuali. Ancora più importante, la visione IoT spinge per una convergenza di settori industriali eterogenei (Bradley et al., 2013), come ad esempio le telecomunicazioni mediche, la sicurezza pubblica dei veicoli e tutte le possibili combinazioni. Per garantire un sano sviluppo del panorama industriale dettato dall'IoT è necessario un quadro normativo

altamente responsabile, sul quale le aziende possano fare affidamento in modo da poter prevedere la risposta legale (Weber, 2011). Tuttavia, l'attuale quadro normativo deve ancora essere aggiornato prima di poter riflettere la convergenza nei settori della comunicazione e dei media. Considerando che la risposta normativa è difficilmente responsabile, per le imprese un dominio di applicazioni IoT con minori rischi normativi sarà preferito per investimenti e sviluppo primari. In futuro il governo potrebbe essere una fonte finanziaria affidabile per le applicazioni IoT pubbliche che dovrebbero essere in grado di migliorare il benessere sociale.

I dispositivi IoT sono definiti come dispositivi con capacità di elaborazione e comunicazione, comprese apparecchiature ed elettrodomestici con diversi domini applicativi (ITU-T, Y. 2060, 2012; Uzelac et al., 2015). La letteratura precedente suggerisce che il 70% dei sistemi IoT comunemente utilizzati sono vulnerabili per via della mancanza di crittografia dei trasporti, di protezione inadeguata del software, di mancanza della sicurezza dell'interfaccia Web e di autorizzazioni insufficienti (Lee e Lee, 2015). Tuttavia, la definizione della responsabilità nell'IoT necessita di un quadro legale stabile per le imprese (Weber, 2011). La responsabilità può essere definita come l'obbligo di una persona (responsabile) di spiegare e giustificare le proprie azioni o decisioni a un'altra persona (l'a*ccountee*) (Weber, 2011). Questo deve essere sviluppato in un approccio multi-stakeholder, dal momento che l'IoT dovrebbe far fronte a diversi segmenti della società (Weber, 2011). Poiché le transazioni commerciali e gli scambi di informazioni vengono effettuati attraverso l'architettura dell'informazione globale in un contesto IoT, è essenziale chiarire chi è responsabile una volta verificatosi l'errore di sistema.

1.3.2 – Consapevolezza ed atteggiamento dei consumatori verso il fenomeno

Uno dei pilastri fondamentali su cui si basa la regolamentazione dell'IoT è la protezione dei consumatori, garantendone il benessere contro possibili effetti negativi causati dal mercato. Per natura, le tecnologie IoT tendono a generare un maggiore flusso di dati, implicando una maggiore esposizione ai rischi collegati al trattamento dei dati personali. Proprio per via della pervasività tipica dell'IoT l'utente si confronta direttamente con il tema della violazione della privacy (Bailey, 2012).

Per quanto l'IoT fornisca vantaggi significativi, la gestione delle aspettative degli utenti verso la privacy contribuirà significativamente a costruire in loro fiducia ed accettazione nei confronti dei servizi IoT, permettendo così il raggiungimento del loro pieno potenziale (Brill, 2014; Lee e Lee, 2015; Ng, 2014b). A livello individuale la privacy viene considerata come un'arma a doppio taglio: gli utenti considerano i controlli della privacy come una protezione delle loro informazioni personali, ma il rischio di una sua violazione della privacy potrebbe costituire un ostacolo all'accettazione dell IoT (Zhou e Piramuthu, 2015).

Parlando di preoccupazioni dell'utente sulla tutela dei dati sensibili ad esso associati, Caron et al. (2016) evidenzia quattro principali tipologie di preoccupazione (Caron et al., 2016):

- Sorveglianza senza il consenso del singolo: sensori ed applicazioni potrebbero essere utilizzati per monitorare le mosse delle persone ed il loro comportamento.
- Generazione ed utilizzo incontrollati di dati: in una rete interconnessa di applicazioni e sensori, il processo di diffusione dei dati raccolti è quasi impossibile da gestire.
- Autenticità inadeguata e conservazione dell'anonimato: l'attuale autenticazione centralizzata dei servizi non fornisce sicurezza nel controllo dell'accesso e l'identificazione automatica tra i servizi comporta nuovi rischi.
- Rischi di sicurezza delle informazioni raccolte: l'IoT potenzialmente è in grado di raccogliere e trasferire un grande volume di informazioni utilizzando più dispositivi collaborativi, diventando così un potenziale rischio per la sicurezza.

Queste preoccupazioni rivelano due sfide principali nella protezione della privacy nell'IoT: il controllo della generazione di dati e la sicurezza delle informazioni.

La prima sfida si rapporta direttamente con la natura pervasiva dell'IoT ed il cambiamento dinamico dei contesti. Uno degli aspetti chiave dello sviluppo del servizio IoT è il miglioramento della qualità dell'esperienza dei consumatori, che deve ottimizzare la connettività nelle relazioni tra uomo e cose (Ortiz et al., 2014). Inoltre, i cambiamenti nel tempo, nello spazio, nella cultura e nella necessità di interazione tra i vari sistemi guidano contesti dinamici con diverse politiche sulla privacy, determinando sfide per le offerte IoT nell'adattamento dei requisiti dinamici (Stankovic, 2014). Quindi, lo sviluppo della privacy deve essere esaminato in contesti specifici (Inverno, 2014). Questa problematica potrebbe essere risolta dalla legislazione. Un principio importante nella privacy informatica è l'applicazione della protezione di questa basata sul contesto in cui ci si colloca. Ad esempio, le persone si aspettano un diverso livello di privacy a seconda che le attività siano svolte a casa o in pubblico (Elmaghraby e Losavio, 2014). Risulterebbe intelligente personalizzare e differenziare la privacy al fine di soddisfare le esigenze individuali, mentre viene contemporaneamente proposto un modello contestuale di tutela della privacy che rispetta i bisogni unici (Zhou e Piramuthu, 2015). Le questioni legislative relative alla protezione della privacy sono ampiamente riconosciute e discusse, specialmente negli Stati Uniti, nell'Unione Europea e in Cina (Atzori et al., 2010; Winter, 2014). Gran parte delle discussioni si concentra sulle sfide legali, mettendo in discussione la necessità che le leggi disciplinino i cambiamenti introdotti dall'IoT, l'adeguatezza della legge esistente, il tipo di legge richiesto e il relativo periodo di attuazione (Winter, 2014). Anche se non vi è consenso in merito a ciò che risulta essere essenziale per la legge sulla privacy, vi sono degli elementi chiave che dovrebbero essere garantiti e tutelati. Alcuni di questi riguardano l'anonimizzazione dei dati, come la posizione ed i movimenti delle persone raccolte dai sistemi di tracciamento, dati che non dovrebbero essere collegabili alle identità degli utenti; perdite di informazioni e violazione della privacy, dovrebbero essere notificate agli utenti; i dati raccolti devono essere trattati al solo scopo di fornire servizi; la trasparenza della raccolta dei dati e la responsabilità

dei raccoglitori di dati dovrebbero essere migliorate (Atzori et al., 2010; Weber, 2009; Weber, 2013; Weber, 2015; Winter, 2014).

La seconda sfida riguarda dalla massiccia raccolta di informazioni nell'IoT. Diventerà quasi impossibile per un individuo evitare di essere monitorato e registrato dai sensori negli spazi pubblici. Una volta che l'informazione è generata, potrebbe essere mantenuta a tempo indeterminato e sarà impossibile controllare la divulgazione a livello personale (Atzori et al., 2010; Weber, 2013). Quando si progettano applicazioni IoT, la generazione di dati, la raccolta, l'estrazione, la trasmissione e l'interpretazione sono considerazioni centrali. La privacy quindi non gioca solo un ruolo di tutela nei confronti del consumatore, ma è anche parte stessa dell'esperienza dell'utilizzo dei servizi IoT. Garantire la privacy con l'utilizzo di questi sistemi si traduce direttamente in un atteggiamento favorevole nei confronti di questi da parte degli utenti. Pertanto, la protezione delle informazioni è fondamentale, poiché la protezione della privacy influenza direttamente l'esperienza del cliente e la fiducia nelle offerte IoT (Lee e Lee, 2015; Weinberg et al., 2015).

1.4– Privacy paradox e domanda di ricerca

La natura interattiva dell'IoT, ha prodotto contesti in cui le preoccupazioni per la privacy sono divenute estremamente rilevanti (Korgaonkar et al., 1999; Bickart and Schindler, 2001; Balmer and Yen, 2017). Se quello che stiamo vivendo è l'età dell'informazione, allora la privacy è il tema dei nostri tempi (Acquisti et al., 2015). La natura interattiva di Internet, che consente uno scambio bidirezionale di informazioni tra marketing e consumatori, ha prodotto contesti in cui le preoccupazioni relative alla privacy sono diventate estremamente rilevanti e, in quanto tali, offrono alle imprese e alle istituzioni opportunità e sfide (Korgaonkar et al., 1999; Bickart and Schindler, 2001; Balmer and Yen, 2017). In effetti, è ormai consolidato che le problematiche legate alla privacy giocano un ruolo sempre più importante nell'influenzare l'atteggiamento e i comportamenti dei consumatori online e, di conseguenza, le performance del mercato delle aziende (Akar e Topku, 2011; Diffley et al., 2011). Ad esempio, in seguito al recente scandalo Cambridge Analytica che ha violato i dati sensibili di oltre 87 milioni di profili Facebook, la società di Mark Zuckerberg ha perso oltre 3 milioni di utenti in Europa e 120 miliardi di dollari dal suo valore di mercato, con un crollo delle azioni la Borsa di New York di oltre il 20% (Isaak e Hanna, 2018). Alla luce di una tale rilevanza delle preoccupazioni sulla privacy, le aziende online devono affrontare un'arma a doppio taglio nel raccogliere le impronte digitali degli utenti per costruire relazioni con i consumatori (Belanger et al., 2002; Eastlick et al., 2006; Punji, 2018). Ottenere informazioni personali consente alle aziende di scegliere come target offerte personalizzate basato su interessi, bisogni e comportamenti del consumatore, rafforzando così il rapporto con il consumatore (Lustria et al., 2016). Allo stesso tempo, le preoccupazioni sulla privacy dei consumatori riguardo alla perdita di controllo sulle loro informazioni possono indebolire le relazioni (Parasuraman e Zinkhan, 2002; Martin and Murphy, 2017). Su questo punto, la letteratura accademica ha evidenziato un paradosso nel comportamento dei consumatori. Infatti, se da una parte alcuni studi hanno dimostrato che gli utenti online si dichiarano molto preoccupati per la raccolta e l'uso ambiguo delle loro informazioni personali da parte delle aziende (ad

esempio, Bansal et al., 2010; Rainie et al., 2013; TRUSTe, 2014), d'altra parte, sono disposti a divulgare dati sensibili, generando quindi impronte digitali per premi relativamente piccoli o spesso nulli. Ad esempio, Carrascal et al. (2013) hanno scoperto che gli utenti Internet apprezzano la loro cronologia di navigazione online per circa 7 euro, che equivale a un pasto Big Mac. Questa discrepanza tra l'atteggiamento della privacy e il comportamento sulla privacy è definita "*privacy paradox*" (Norberg et al., 2007; Mosteller and Poddar, 2017) e un tentativo di spiegare questo fenomeno è stato fornito dalla "teoria del calcolo della privacy" (Culnan e Armstrong, 1999; Kokolakis, 2017). Questa teoria postula che le persone eseguano un calcolo tra la perdita attesa della privacy e il potenziale guadagno dell'autodisposizione (Krasnova e Veltri, 2010). La loro decisione di rivelare o meno le informazioni personali dipende dal risultato di questo compromesso sulla privacy (Dinev and Hart, 2006; Xu et al., 2011; Jiang et al., 2013).

La letteratura ha cercato di spiegare il fenomeno del paradosso della privacy attraverso diversi metodi di ricerca, diversi contesti e concettualizzazioni ma, nonostante la rilevanza di queste indagini, i problemi rilevanti sono rimasti fino ad oggi inesplorati. Uno di questi problemi riguarda gli effetti che la personalizzazione può avere sull'utente online. Oggi, l'applicabilità della personalizzazione si espande in modo significativo negli ambienti online in cui la capacità di incorporare i comportamenti passati degli utenti consente alle aziende di aumentare la soddisfazione e la lealtà dei consumatori e agli utenti online di godere di prodotti e servizi migliori. Ad esempio, i motori di ricerca (ad es. Google) possono perfezionare i risultati di ricerca di ciascun utente incorporando le informazioni di ricerca precedenti; aziende online come Amazon e Netflix offrono consulenze personalizzate utilizzando sistemi di raccomandazione basati sul filtro collaborativo e dei contenuti. A questo punto, ci si potrebbe chiedere cosa succede quando gli utenti online ricevono servizi personalizzati. La loro percezione della vulnerabilità aumenta e quindi nega un'ulteriore auto-rivelazione, o saranno più disposti a lasciare impronte digitali perché percepiscono nella personalizzazione più benefici rispetto ai costi associati?

1.4.1 – Privacy Paradox

Le persone hanno davvero a cuore la loro privacy? Ciò che emerge dai vari sondaggi e studi condotti nel corso degli anni mostrano che la privacy è risultata essere una preoccupazione primaria per i consumatori nell'era digitale. Per contro, le persone rivelano informazioni personali in cambio di *reward* relativamente misere, spesso al solo fine di "mettersi in mostra" sui *social network*. Questa incoerenza comportamentale e nelle attitudini verso la privacy viene definita il "paradosso della privacy". Nella parte seguente della sezione 1.4.1 verrà presentata una breve revisione sulla letteratura di ricerca sul fenomeno della *privacy paradox*. Inoltre verranno esposte anche diverse interpretazioni del paradosso della privacy, derivanti dalla teoria sociale, dalla psicologia, dall'economia comportamentale ed anche dalla teoria quantistica.

Umberto Eco ne parlò in una celebre bustina di Minerva nel 2014, divertendosi a tradurre "*privacy"* con un neologismo italiano volutamente improbabile: la privatezza. "Detto alla buona significa che ciascuno ha diritto a farsi i fatti suoi senza che tutti, specie delle agenzie pagate dai centri di potere, lo vengano a sapere". Poi

Eco si pose la domanda “la gente ci tiene davvero alla privatezza?”. Persone di ogni età hanno un rapporto ambiguo con la privacy. A parole la reclamano come un diritto imprescindibile. Durante una cena od un convegno aziendale, basta accennare a come le nostre informazioni vengano sfruttate online, ed ecco che amici e colleghi lanciano grida di allarme. Passando ai fatti, emerge una situazione ben diversa (“Il paradosso della privacy, e quanto siamo disposti a pagare per averla”, Giulio Xhaët, Il sole 24 ore, 2018). La gente non fa quasi nulla di concreto per difendere il diritto a farsi i fatti propri. Il ricercatore Stewe Boyd nel 2009 coniò il termine *publicy*, descritto come il diritto di ciascuno di comunicare, esprimersi e mettere in pubblico la propria vita online per ottenere visibilità e riconoscimenti. Recentemente, gli psicologi NathalieNahai e Tomas Chamorro-Premuzic si sono domandati cosa saremmo disposti a fare per ritornare dalla *publicy* alla privacy e rimanerle fedele nel tempo. Partendo da questo presupposto: un tempo gli aggettivi “personale” e “privato” erano sinonimi. Nella realtà dei bit invece le informazioni personali sono quanto di meno privato possa esistere. Ecco dunque un elenco di perdite a cui dovremmo sottostare per tornare alla privatezza:

- **Niente più servizi online gratis**. La frase “Se non stai pagando per un servizio digitale, non sei il cliente, sei il prodotto” rappresenta in maniera esemplare il concetto. Per tornare ad una situazione in cui manteniamo privati i nostri dati personali, dovremmo pagare una quota. Il che oggi è impensabile. Anche se le piattaforme ci permettessero di scegliere se pagare in privacy o in denaro, stabilendo un prezzo di mercato, cosa sceglierebbero gli utenti? Facebook nel 2016 era valutata 35 miliardi di dollari con 1 miliardo e 650 milioni di utenti: il che significherebbe che il prezzo corrispettivo della privacy è di 212 dollari l’anno. Gli utenti sarebbero disposti a pagare tale cifra per usare Facebook così da impedire ogni singola analisi a scopo statistico e pubblicitario sui loro dati? Probabilmente qualcuno risponderebbe anche positivamente, ma il problema si pone nel momento in cui qualsiasi altra piattaforma gratuita applica lo stesso meccanismo. Dalle mail alle chat, dai servizi Google e YouTube a quelli di Apple e Amazon. La somma da esborsare diventerebbe ovviamente insostenibile per quasi la totalità dell’utenza. Ecco perché questo modello di funzionamento che ruota intorno alla privacy è troppo “comodo” perché venga sostituito facilmente.
- **Niente più personalizzazioni**. Senza più l’accesso dei dati personali e l’assenza dei *cookies* la navigazione risulterebbe molto più standardizzata e meno *focused* su quelli che sono i *consumer behavior* online.
- **Niente più gratificazioni istantanee**. L’appagamento reale è diventato lo standar che pretendiamo da un servizio digitale. Questa impazienza costante si riflette nel rapporto con la privacy: le condizioni di servizio di un’app appena scaricata non vengono, per la stragrande maggioranza dei casi, mai lette. Il dowload o un aggiornamento importante, alimentano il desiderio di gratificazione istantanea in grado di cancellare in un istante qualsiasi preoccupazione razionale portando i consumatori a non avere la minima idea di come i dati verranno utilizzati. Proprio in questo caso si parla di vero e proprio *privacy paradox* di massa: viene pretesa e difesa a parole, ma non viene compiuto nulla per proteggerla.

La maggior parte della ricerca sul paradosso della privacy considera le attività generali di internet, con particolare attenzione alle attività di *e-commerce* e *social networking*. Conosciuto come il paradosso della privacy, è un fenomeno documentato che dimostra come gli utenti abbiano una tendenza verso comportamenti lesivi della loro privacy online. Questo mette in luce una dicotomia tra atteggiamenti di privacy e comportamento reale (Acquisti, 2004; Barnes, 2006). Un certo grado di percezione del rischio implica una maggiore conoscenza delle strategie di protezione della privacy, ma sembra un motivatore insufficiente per applicare tali strategie (Oomen e Leenes, 2008). Pertanto, sebbene molti utenti mostrino interesse teorico alla loro privacy e mantengano un atteggiamento positivo nei confronti del comportamento di protezione della privacy, questo si traduce raramente in un reale comportamento protettivo (Joinson et al., 2010; Pötzsch, 2009; Tsai et al., 2006). Inoltre, mentre esiste l'intenzione di limitare la divulgazione dei dati, la divulgazione effettiva spesso supera significativamente l'intenzione (Norberg et al., 2007). La ricerca sui fornitori di servizi online ha dimostrato che le decisioni concrete sulla privacy e la consapevolezza del rischio astratto non sono intercambiabili. Le decisioni sulla privacy non cambiano in base alle preferenze modificate, il che potrebbe spiegare la disparità tra le preferenze dichiarate per la privacy e il comportamento reale (Flender e Müller, 2012). Sebbene gli utenti siano consapevoli dei rischi della privacy su Internet, tendono a condividere informazioni private in cambio di valore al dettaglio e servizi personalizzati (Acquisti e Grossklags, 2005, Sundar et al., 2013). Nel contesto delle attività dei social network degli utenti, si osserva uno schema simile. L'utilizzo di varie strategie di protezione della privacy quali la limitazione dell'accesso a wall post, la limitazione dei tag di foto e l'invio di messaggi privati invece di pubblicare contenuti aperti è progettato per controllare il flusso di informazioni tra amici e colleghi.

1.4.1.1 – Studi Recenti

Nel 2001, uno studio sull'uso di Internet indagava la popolarità dello shopping online e le preoccupazioni dei consumatori/utenti circa la loro privacy e sicurezza dei loro dati (Brown, 2001). Fu Brown per primo, attraverso varie sessioni di *deep interview* ad accorgersi di "un paradosso della privacy". Mentre le persone esprimevano le loro preoccupazioni sulla violazione dei loro dati personali, di fatto si dimostravano disposte a fornire dettagli personali ai rivenditori online in cambio di una *reward*. Gli intervistati hanno dichiarato di temere la raccolta massiva di informazioni sul loro conto, ma ciò non ha di fatto impedito loro di proseguire ad acquistare online. È successivamente emerso che carte fedeltà, sconti e regali offerti hanno avuto la funzione di catalizzatori per attirare i consumatori ad acquistare online. Queste implicazioni sono risultate coerenti con le ricerche fatte sulle carte fedeltà, le quali avevano dimostrato che gli acquirenti erano disposti a scambiare informazioni sui loro acquisti se in cambio potevano risparmiare al momento dell'emissione dello scontrino. (Savre & Horne, 2000). Nello stesso anno, Spiekermann et al. (2001) hanno presentato i risultati di uno studio volto a rivelare la relazione tra le preferenze sulla privacy e il comportamento reale nel contesto dell'e-commerce. Lo studio consisteva in un esperimento in grado di confrontare le preferenze sulla privacy autoregolate con il comportamento di divulgazione effettiva durante lo shopping online. I partecipanti hanno

inizialmente compilato un questionario in grado di catturare e misurare le loro attitudini e preferenze verso la privacy, e seguentemente hanno visitato un negozio online. Durante la fase di visita del sito e shopping online sono stati coinvolti, tramite *chatbot*, in una conversazione finalizzata alla vendita. I partecipanti hanno risposto a gran parte delle domande, nonostante queste fossero strettamente personali. Questo evidenzia come, nonostante gli utenti di Internet affermino che la privacy sia un elemento di massima priorità, nella pratica non si comportano di conseguenza. Un esempio ancor più eclatante sulla dicotomia esistente tra atteggiamento e comportamento è stato fornito dai ricercatori che hanno perseguito la via del comportamento economico. Acquisti (2004) ha affermato che "le persone potrebbero non essere in grado di agire come agenti economicamente razionali quando si tratta di privacy personale". Quello che la precedente frase vuole lasciar intendere è che le decisioni relative alla privacy sono influenzate da informazioni incomplete, razionalità limitata e pregiudizi psicologici, come *bias* di conferma, sconto iperbolico ed altri. Questi *bias* decisionali sono stati ben documentati nella letteratura di economia comportamentale (per esempio Gilovich et al., 2002). Acquisti ha costruito un modello economico in grado di spiegare parte dell'*attitude* verso la privacy e le incoerenze comportamentali. Il modello incorpora il pregiudizio immediato della gratificazione. Gratificazione immediata si riferisce alla tendenza da parte del consumatore di dare maggiore peso ai benefici presenti contro i rischi futuri. Pertanto, la valutazione euristica condotta dalle persone porta a considerare i benefici attuali ricevuti come un valido compromesso alla divulgazione delle informazioni personali ed i rischi futuri ad essi associati (Acquisti, 2004).

Passando dalla teoria economica alla ricerca empirica, Acquisti e Grossklags (2005) hanno raccolto dei dati in grado di supportare l'ipotesi secondo cui il processo decisionale che avviene sulla privacy sia influenzato da informazioni incomplete, razionalità limitata e pregiudizi psicologici (euristiche e *bias* cognitivi). È stato inoltre provato che sebbene la maggior parte dei soggetti (circa l'89%) abbia dichiarato di essere moderatamente o molto preoccupato per la privacy, oltre il 21% del campione ha ammesso di aver fornito dati strettamente personali in cambio di sconti o servizi. Un altro flusso di ricerca mirava a comprendere il comportamento auto-rivelante tra i giovani nei *social network.* Barnes (2006) usa il termine paradosso della privacy in riferimento al comportamento tenuto dai giovani ne confronti della privacy sui siti di *social networking* (SNS). I giovani tenderebbero a non rendersi conto che gli SNS forniscono uno spazio pubblico gratuito divulgando informazioni sensibili che potrebbero essere soggette ad un utilizzo improprio. Il termine paradosso della privacy inteso per come lo intendiamo oggi è da attribuirsi principalmente a Norberg et al., (2007). Sono stati condotti due studi, ciascuno dei quali composto da due fasi. Nella prima fase è stato chiesto ad un campione di studenti la disponibilità a rivelare informazioni specifiche. La seconda parte, oltre ad aver avuto luogo svariate settimane dopo la prima, consisteva nel richiedere ai soggetti lo stesso tipo di informazioni ma da parte di un ricercatore di mercato. Questo studio ha il merito di aver confermato l'ipotesi secondo cui gli individui avrebbero effettivamente rivelato una quantità significativamente maggiore di informazioni personali rispetto a quanto era stato indicato nelle intenzioni dichiarate.

1.4.1.2 – Studi a sostegno dell'esistenza della privacy paradox

Le prove preliminari fornite da Spiekermann et al., (2001), Acquisti e Grossklags (2005) e Norberg et al., (2007) sono stati ulteriormente confermati e supportati dalle ricerche svoltesi seguentemente, confermando sia le evidenze mostrate in situazioni transazionali (es. *e-commerce*), sia quelle in situazioni sociali (es. *social networking*). Huberman et al., (2005) hanno condotto una serie di aste sperimentali per cercare di comprendere il valore che le persone attribuiscono ai loro dati privati. In queste aste i partecipanti hanno indicato un prezzo per l'ottenimento dei loro dati. Le informazioni messe all'asta erano il peso e l'età. Il prezzo medio della domanda per l'età è risultato essere intorno ai 57,56$ contro i 74,06$ per il peso. L'esperimento ha inoltre rivelato una tendenza ad una valutazione più alta per quanto concerne le informazioni sul peso quando questo veniva percepito come imbarazzante. Come previsto, i giovani erano più disposti a comunicare la loro età rispetto ai più anziani. Un altro esperimento invece prevedeva di far affrontare una situazione di compromesso ai soggetti partecipanti, dove è stato chiesto loro di scegliere tra protezione della privacy incompleta e vantaggi (es. promozioni, sconti) (Hann et al., 2007). È stato stimato che la protezione dagli errori nei registri personali, l'accesso improprio delle informazioni personali e l'uso secondario di informazioni personali valgono tra i 30,49$ e i 44,62$. Beresford et al., (2012) hanno condotto un esperimento sul campo, nel quale è stato chiesto ai partecipanti di acquistare un DVD da uno di due negozi concorrenti. I due negozi erano quasi identici: il primo negozio richiedeva reddito e data di nascita, mentre il secondo negozio chiedeva il colore preferito e l'anno di nascita. Ovviamente, le informazioni richieste dal primo negozio sono significativamente più sensibili. Tuttavia, quando il prezzo era lo stesso in entrambi i negozi, si verificava quanto era auspicabile, ossia una maggiore vendita nel secondo negozio. Ma quando il prezzo nel prima negozio, per lo stesso prodotto, era stato fissato ad 1 euro in meno nel primo negozio, quasi tutti i partecipanti hanno scelto quello più economico, nonostante le informazioni richieste fossero più riservate. Un questionario somministrato in via post-sperimentale ha evidenziato come il 75% dei rispondenti si era comunque dichiarato fortemente interessato alla protezione dei dati, mentre il 95% ha affermato di essere interessato alla protezione delle proprie informazioni personali.

L'esistenza della dicotomia tra atteggiamento e comportamento è stata confermata anche dllo studio di Lee et al., (2013). Hanno condotto una serie di interviste semi-strutturate ed un esperimento per valutare l'influenza del beneficio atteso e del rischio futuro atteso sull'intenzione degli utenti di condividere le informazioni personali. Hanno concluso che gli utenti condividono attivamente le informazioni personali nonostante le loro preoccupazioni, perché non considerano solo i rischi, ma soprattutto i benefici attesi dalla condivisione.

1.4.2 – Domanda di ricerca

Nonostante gli utenti dichiarino di essere particolarmente attenti alla protezione della propria privacy, questo si traduce raramente in azioni concrete. Ciò significa che, nonostante sia a conoscenza dei rischi, l'utente non mette in atto comportamenti volti a proteggere i propri dati. In altri casi, invece, l'utente mette in atto dei comportamenti utili alla protezione dei propri dati. Spesso però, risulta piuttosto facile far sì che il consumatore

non compia più queste azioni, grazie a delle piccole reward di più vario genere (Acquisti e Grossklags, 2005, Sundar et al., 2013).

L'intenzione è quella di soffermarsi proprio su questa seconda casistica e di analizzare il meccanismo *privacy-reward* appena citato. Per analizzare al meglio tale fenomeno e trarre insight utili a definirne il funzionamento, il meccanismo di cui sopra può essere tradotto in una semplice domanda: "quanto/cosa vuoi perché tu acconsenta al trattamento dei tuoi dati personali?".

Adattando al settore *healthcare*, la domanda diventa: "quale servizio sanitario vuoi che ti sia garantito affinchè tu acconsenta al trattamento dei tuoi dati personali?".

Così facendo, la *reward* è rappresentata da un servizio sanitario. L'obiettivo della domanda di ricerca sarà quindi quello di andare a capire le seguenti meccaniche:

- Se un servizio sanitario è in grado essere percepito come una reward tale da consentire il trattamento dei dati personali (benessere percepito più forte della privacy);
- Quale servizio sanitario minimo deve essere garantito affinchè il consumatore conceda al fornitore del prodotto/servizio il trattamento dei suoi dati personali (non tutti i servizi potrebbero essere percepiti come equivalenti);
- Se un servizio sanitario garantito risulta essere tollerato su dispositivi non direttamente collegati all'ambito medico sanitario (rifiuto di un servizio su dispositivo diverso dallo scopo di tutela della salute);

Queste tematiche se ben indagate potranno dare un contributo in termini di comprensione dei bisogni del consumatore, aprendo nuove possibilità di targetizzazione del mercato e opportunità di cross-selling (es. assicurazioni con Applewatch).

CAPITOLO 2
Un nuovo modello concettuale

Il modello costruito per l'indagine si ispira a quello teorizzato da Hsu e Lin. Prima di mostrare le variabili in esso presenti, passeremo in rassegna gli elementi più importanti e i principali snodi attraverso i quali il modello si articola e dai quali successivamente svilupperemo quello utile alla nostra domanda di ricerca. Gli elementi originali del modello, trattati nel paragrafo 2.1, riguardano l'IoT, le esternalità di rete e il permesso al trattamento dei dati personali (CFIP). Infine, sarà presente la parte basata sul *Privacy Paradox Phenomenon*. Infatti, nel modello è stata introdotta una variabile a carattere di *reward.* Questa era, secondo letteratura, la causa scatenante del paradosso della privacy. In questa circostanza essa avrà natura di *reward* di servizio andando a giocare il ruolo di moderatore all'interno del modello. Si cercherà pertanto di capire se una *reward* di servizio di tipo sanitario è in grado di innescare lo stesso meccanismo che una *reward* monetaria o di personalizzazione era in grado di innescare nel consumatore. Una volta misurata si osserverà che effetto di moderazione viene esercitato rispettivamente su *attitude,* CFIP e benefici percepiti.

2.1 – Theoretical Background

2.1.1 – Internet of Things (IoT)

I servizi IoT utilizzano Internet al fine di formare una vasta rete di *smart device*. Mentre l'Internet "convenzionale" collega le persone al fine di scambiare informazioni, l'IoT è in grado di integrare macchine e oggetti tramite l'incorporamento, in essi, di sensori che consentono loro di comunicare in maniera autonoma su Internet (Somayya Madakam, R. Ramaswamy, Siddharth Tripathi, 2015). Quello che l'IoT rappresenta è stato descritto attraverso l'utilizzo di più denominazioni, tra cui *Machine to Machine* (M2M), rete di sensori, *smart planet*, *computing* pervasivo e *computing* obiquo. Generalmente però, l'IoT è definito come un processo in grado di integrare *smart devices*, intelligenza attiva, capacità di rete e utenti. Le architetture IoT sono in genere costituite da 3 livelli: dispositivo, connessione e applicazione (Bandyopadhyay, Balamuralidhar e Pal, 2013). Il livello "dispositivo" fa riferimento alla parte di acquisizione dei dati al livello più basso dell'architettura IoT standard. Le tecnologie a questo livello generalmente includono dispositivi ed applicazioni che utilizzano l'identificazione a radiofrequenza (RFID), *near field comunication* (NFC), reti di sensori *wireless* (WSN) e intelligenza integrata. Il livello "connessione" include i gateway e la rete *core/backbone*. Il *gateway* può fornire un'interfaccia uniforme per integrare dispositivi e tecnologie tra loro eterogenee a livello di dispositivo. La rete IoT *Core/Backbone* è una connessione IP che può essere supportata da varie infrastrutture di telecomunicazione come Zigbee, WiFi, WiMAX e reti cellulari (2G,3G,4G). Il *gateway* ed il livello "applicazione" possono essere tranquillamente collegati su queste varie reti. Inoltre, questo strato fornisce anche piattaforme di *cloud computing* che consentono di memorizzare e utilizzare i dati di rilevamento in modo intelligente per il monitoraggio e l'attivazione con *smart devices*. Il livello

"applicazione" è il più vicino all'utente finale e può supportare una vasta gamma di servizi e applicazioni, inclusi quelli utilizzati in casa (es. utilità ed accessori, salute, intrattenimento e sicurezza), nel trasporto (es. monitoramento del traffico, parcheggio assistito, etc..) e un'altra vasta gamma di categorie (es. misurazione intelligente, ambiente, vendita al dettaglio, fabbrica e sorveglianza) (Atzori, Iera e Morabito, 2010; Gubbi et al., 2013). In questo studio, i servizi IoT sono stati identificati come funzioni a livello "applicazione" che consentono agli utenti di interagire direttamente con l'hardware (es. *smartphone, applewatch*) e gli ambienti intelligenti in grado di migliorare la qualità della vita e la produttività del lavoro. Ad esempio, i dispositivi Apple Watch, considerabili come un'estensione dello *smartphone*, permettono agli utenti un facile controllo di alcune delle loro funzioni vitali di base, grazie ai sensori di cui il dispositivo stesso è dotato.

2.1.2 – Permesso al trattamento delle informazioni personali (CFIP)

Westin (1968) ha definito la privacy come "il diritto di scegliere quali informazioni personali su di me possano esser note a quali persone". Questa frase esprime perfettamente l'idea dell'autodeterminazione della classificazione delle informazioni da parte di persone in grado di valutare i loro rischi per la privacy di proteggerla adottando comportamenti adeguati a tale scopo. Maggiore è il controllo percepito su di essa, minore è il rischio. In ambienti "*offline*", la privacy individuale era più facilmente tutelabile per via della relativa inefficienza dei canali di comunicazione. Nell'ultimo decennio, a causa della proliferazione di Internet e delle tecnologie mobili ad esso affini, la privacy delle informazioni è diventata una vera e propria questione, nonché problematica urgente da risolvere, per le tecnologie emergenti (es. commercio elettronico, applicazioni *mobile*, servizi di localizzazione e servizi *cloud*) (Aloudat, Katina, Chen e Al-Debei, 2014; Cazier, Jensen e Dave, 2008; Slyke, Shim, Johnson e Jiang, 2006; Yang & Lin, 2015). Per far sì che i mezzi relativi alla tutela della privacy in ambito IoT trovassero un'applicazione concreta, Ziegeldorf et al. (2014) hanno suggerito che i fornitori di servizi IoT garantissero tre tipi di garanzie:

- Mettere a conoscenza gli utilizzatori dei possibili rischi della loro privacy derivanti dall'utilizzo degli *smart devices* e servizi ad essi associati.
- Fornire il controllo individuale sulla raccolta e elaborazione di dati personali.
- Messa a conoscenza degli utenti circa il successivo utilizzo e diffusione di informazioni personali da parte di tali soggetti a qualsiasi entità al di fuori della sfera di controllo personale e del soggetto.

Molti studi trattano il fatto che i problemi inerenti alla privacy debbano essere affrontati per poter garantire che l'IoT diventi una realtà. Vermesan et al. (2011) hanno suggerito ai fornitori di servizi IoT di sviluppare nuove tecniche e definire nuovi principi di *governance* al fine di garantire la tutela della privacy ed adattarsi alle nuove sfide tecnologiche e sociali. Con il lavoro di Miorandi et al. (2012) è stato posto l'accento su come i fornitori di servizi sviluppino meccanismi di conservazione della privacy tali da garantire l'accettazione da parte di tutti gli utenti e favorire l'adozione delle tecnologie IoT. Hanno così presentato ai *service provider* l'opportunità di:

- Definire un modello generale di gestione della privacy nell'IoT.

- Sviluppare tecniche di applicazione innovative e non invasive per supportare la scala e l'eterogeneità caratteristiche degli scenari IoT.
- Sviluppare soluzioni in grado di bilanciare la necessità di anonimato per alcune applicazioni basate sulla localizzazione ed i requisiti di tracciamento.

Chui et al. (2010) hanno mostrato come sarebbe più opportuno che i gruppi industriali e i regolatori governativi elaborassero delle regole atte alla protezione delle informazioni sensibili dei consumatori. Nonostante il forte interesse per i problemi in materia di privacy nel contesto IoT, pochi si sono concentrati su questo argomento. Inoltre, i servizi IoT sono molto simili ai servizi di *U-commerce*, poiché entrambi hanno come caratteristica comune il concetto dell'utilità "*anytime and anywhere*". Le tecnologie abilitanti (es. reti di sensori, tecnologie di rilevamento della posizione, interfacce biometriche, etc..) di *U-commerce* tendono a raccogliere facilmente i dati personali dell'utente. Specialmente quando andiamo a trattare una tipologia di servizio altamente personalizzata e specifica, il servizio di *U-commerce* deve monitorare da vicino l'utente nelle sue attività quotidiane. Inoltre, i problemi relativi alla privacy sono maggiormente presenti nei contesti degli *U-commerce* rispetto ad altri tipi di commercio (es. *e-commerce* o *m-commerce*) (Sheng, Nah e Siau, 2008).

Avendo quindi ampiamente esaminato ed esposto come l'IoT abbia caratteristiche simili ai servizi di commercio elettronico risulta corretto proporre la privacy come fattore determinante nell'adozione da parte dei consumatori per i servizi IoT. Smith,Milberg e Burke (1996) hanno identificato ed introdotto quattro categorie qualificanti le principali preoccupazioni relative alla privacy in risposta alle pratiche di riservatezza delle informazioni e dell'organizzazione: raccolta, uso secondario non autorizzato, accesso improprio ed errori. Come affermato da Stewart e Segars (2002), gli utenti potrebbero essere esposti ad elevati livelli di CFIP. Questo avverrebbe nel caso in cui:

- Gli utenti percepissero il servizio come una raccolta di dati personali eccessiva;
- I soggetti non autorizzati vengano autorizzati a utilizzare le informazioni personali per scopi non dichiarati;
- Disponibilità da parte di terzi non autorizzati alla visione e consultazione di dati personali;
- Errore nei dati personali.

Hanno esaminato empiricamente il *framework* CFIP e convalidato il modello di misurazione come un costrutto multidimensionale. I risultati ottenuti suggeriscono che la CFIP acquista maggiore valenza se rappresentata come una struttura riflessiva del fattore di secondo ordine piuttosto che una serie correlata di fattori del primo ordine. La successiva ricerca di modellizzazione della CFIP come fattore di secondo ordine è stata verificata e trovata coerente con i risultati di Stewart e Segart (Korzaan & Boswell, 2008). Pertanto, sulla base della proposta di Stewart e Segars (2002), il modello da cui partiremo propone l'inclusione della raccolta, uso secondario non autorizzato, accesso improprio ed errori, nella misurazione della CFIP nel contesto IoT.

2.1.3 – Privacy Paradox Phenomenon

Gli argomenti attraverso i quali si può approcciare e studiare la privacy sono numerosi, è possibile distinguere tre aspetti della privacy (Rosenberg, 1992; Holvast, 1993):

- La privacy territoriale, che riguarda l'area fisica che circonda una persona;
- La privacy di una persona, che si riferisce alla protezione di una persona contro indebite interferenze;
- La privacy informativa, che si occupa di controllare se e in che modo i dati personali possono essere raccolti, archiviati, elaborati e diffusi.

In questo caso lo studio è limitato a quello della privacy informativa. Quindi riferirsi in via generale al paradosso della privacy nella presente sezione, come vale per l'intero studio, equivale a riferirsi nello specifico al paradosso della privacy informativa.

Il paradosso della privacy, nella gran parte degli studi rilevanti, si riferisce alla dicotomia tra atteggiamento di riservatezza e comportamento effettivo tenuto verso la privacy. Alcuni ricercatori, in via alternativa, confrontano le preoccupazioni sulla privacy con il comportamento effettivo verso la privacy; nonostante siano strettamente correlati, sono fondamentalmente diversi. Le preoccupazioni sulla privacy possono essere a carattere molto generale, e nella maggior parte dei casi non sono legate ad un contesto specifico, mentre gli atteggiamenti della privacy si riferiscono alla valutazione di specifici comportamenti sulla privacy.

Un'altra distinzione che si può evidenziare è quella tra comportamento verso la privacy e intenzione alla privacy. Diversi studi hanno misurato l'intento della privacy anziché del comportamento verso la privacy. Questi studi però già di partenza si trovano orfani di un aspetto essenziale del paradosso: il fatto che generalmente le intenzioni sulla privacy non portano concretamente ad un comportamento protettivo. La letteratura attuale include alcuni studi che attribuiscono un significato completamente diverso alla definizione "paradosso della privacy" riqualificandolo come la tensione tra personalizzazione e privacy specialmente nell'*e-commerce*. Questa diversa definizione del paradosso viene anche chiamata come il paradosso della "personalizzazione-privacy". Sutanto et al., (2013) hanno misurato come l'impatto della personalizzazione abilitata all'IT e del marketing personalizzato esercita un effetto sulle preoccupazioni per la privacy degli utenti di *smarthpone*. Il fenomeno del paradosso della privacy mette in luce come gli utenti tendano ad avere comportamenti dannosi per la loro privacy online. Questo si verifica maggiormente in contesti quali le piattaforme di *e-commerce* e/o *social networking*. Molti utenti mostrano avere particolare riguardo per la tutela della loro privacy, ma in via meramente teorica. Questo significa che di fatto non vengono compiuti, dagli stessi, comportamenti tali da confermare nel pratico la preoccupazione mostrata. Inoltre, nonostante esista l'intenzione di limitare la divulgazione dei dati, quella effettiva risulta essere di gran lunga superiore. La letteratura ci fornisce gli strumenti per indagare a fondo questo fenomeno, ed è emerso che le decisioni prese in merito alla tutela della privacy e la consapevolezza del rischio ai quali gli utenti sono esposti, non sono intercambiabili. Sebbene gli utenti siano consapevoli dei rischi della privacy su Internet, tendono a condividere informazioni private in cambio di piccoli *reward* e servizi personalizzati (Acquisti e Grossklags, 2005, Sundar et al., 2013).

2.1.4 – Network Externality

In ultima istanza risulta opportuno, ai fini della ricerca, soffermarsi sul concetto delle esternalità di rete. Come presenti nel modello, queste vengono suddivise in dirette ed indirette e verrà posto maggiormente l'accento, nel corso dello studio, sulle seconde piuttosto che le prime.

Le esternalità di rete sono definite come "il valore o l'effetto che gli utenti ottengono da un prodotto o servizio determinato dall'aumento di utenti, prodotti complementari o servizi" (Katz & Shapiro, 1985). Studi precedenti hanno esaminato, in un ottica economica, questo fenomeno all'interno di un contesto IT, ed in particolar modo sulla sua adozione (Chiu et al., 2013, Lin & Bhattacherjee, 2009; Lin & Lu, 2011; Pae & Hyun, 2002; Wu, Chen, & Lin, 2007). Il valore di un particolare IT per un utente aumenta con il numero dei suoi utenti. Ad esempio, mentre i servizi di *social networking* come Facebook aumentano di popolarità, diventano sempre più preziosi per gli utenti, favorendo così una maggiore adozione. Molti ricercatori (Gupta e Mela, 2008; Katz & Shapiro, 1985; Lin & Bhattacherjee, 2008) hanno affermato che le esternalità della rete possono essere dirette o indirette. Le esternalità di rete diretta aumentano quando l'utilità degli utenti è direttamente proporzionale al numero di utenti che utilizzano lo stesso prodotto o servizio di rete. Utilizzando nuovamente i sii di *social network* come termine di paragone, l'aggiunta di nuovi utenti offre agli utenti preesistenti maggiori opportunità di comunicazione e condivisione, aumentando così l'utilità percepita a livello collettivo. Altri validi esempi riguardano le reti di telefonia mobile, siti di aste online, fax, e-mail e giochi online. Nello studio di Hsu e Lin (Hsu & Lin, 2016) le esternalità di rete dirette sono ulteriormente suddivise in due sottocategorie; in base al numero di servizi IoT ed in base alla massa critica percepita dagli utenti. Il numero di servizi IoT definisce il lato dell'offerta della rete, mentre il numero di utenti definisce il lato della domanda. Supponiamo che l'utilità ottenuta dall'uso dell'IoT non sia solo una funzione crescente del numero di servizi IoT disponibili, ma anche una funzione crescente del numero di utenti. Il numero sempre crescente di utenti va a creare la richiesta di ulteriori servizi e risorse IoT e nuove applicazioni vengono così lanciate in una gamma di domini fisici tra cui negozi, ospedali, banche, ristoranti e così via. Di conseguenza il numero di servizi IoT può funzionare come un'esternalità di rete diretta. Come stabilito dalla legge di Metcalfe, il valore di una rete è una funzione quadrata del numero dei suoi utenti. Internet può essere considerato una piattaforma di comunicazione per lo scambio di informazioni con altri utenti. Più utenti ci sono, più la rete sarà preziosa. Inoltre, gli utenti possono sviluppare una percezione della massa critica attraverso l'interazione con altri (Lou et al., 2000). All'aumento dell'adozione dei software ed hardware, aumenta la partecipazione alle attività di rete, la quale aumenterà di valore.

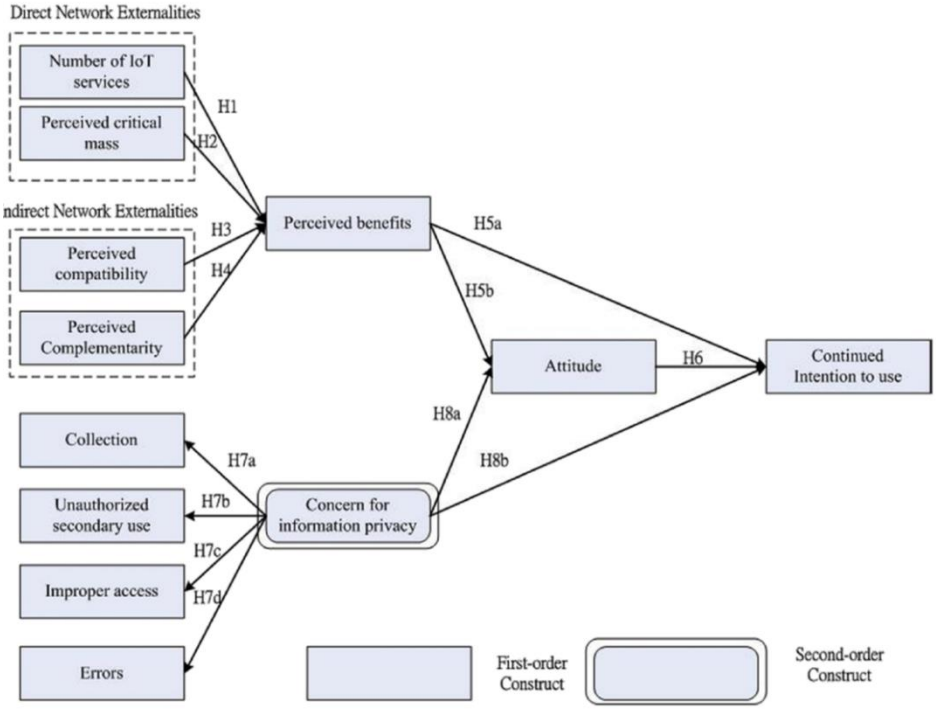
Le esternalità di rete indirette invece, derivano dalla disponibilità di prodotti e servizi complementari, ma non direttamente dal numero di partecipanti alla rete. Pertanto, le esternalità indirette derivano dal lato dell'offerta della rete (Lin & Bhattacherjee, 2008). Queste sono anche denominate esternalità di rete tra prodotti diversi: quando un prodotto o servizio complementare al prodotto primario viene offerto in quantità maggiore o ad un prezzo inferiore, il valore e la domanda per il prodotto primario aumenteranno. Un esempio pratico di questo

meccanismo riguarda i computer IBM compatibili con i PC che, negli anni ’80, avevano un vantaggio competitivo più elevato rispetto ai computer Macintosh poiché presentavano una gamma più ampia di applicazioni software tra cui database, fogli di calcolo, elaborazione testi e così via. Queste applicazioni complementari essendo popolari ed economiche, andavano ad aumentare il valore dei PC IBM. Da questo si deduce come l’aumento dei servizi complementari dell’IoT, come controlli di accesso alle porte, servizi di identificazione e quant’altro, siano in grado di aumentare in via reale e concreta l’utilità per gli utenti. Quindi la complementarità percepita è considerata un’esternalità di rete indiretta nel presente studio. Inoltre, studi precedenti, hanno proposto la compatibilità percepita come un altro tipo di esternalità di rete indiretta (Chiu et al., 2013; Gandal, 1994; Lin, Tsai, Wang, & Chiu, 2011). Lin et al., (2011). Lin et al., (2011) hanno indicato che gli utenti dell’IT in rete possono essere scoraggiati dalla mancanza di compatibilità IT e tali tecnologie potrebbero non ottenere economie di scala. Gandal (1994) ha riscontrato che gli utenti sono disposti a pagare un prezzo più alto per le applicazioni basate sull’effetto di rete diretto (numero maggiore di utenti esistenti) ma anche sull’effetto di rete indiretto (maggiore compatibilità con le altre applicazioni). Chiu et al., (2013) hanno riscontrato che gli utenti basano la loro intenzioni di continuare ad utilizzare i siti di *social network* in base alla compatibilità percepita. In effetti, studi precedenti indicano che la compatibilità gioca un ruolo importante nell'emergere di standard IT come PC, EDI e commercio elettronico (Damsgaard & Truex, 2000; West & Dedrick, 2000; Zhao, Xia, & Shaw, 2007). Pertanto, proponiamo la compatibilità percepita come un'altra esternalità di rete indiretta.

2.2 – Modello concettuale e qualificazione del moderatore

Il modello concettuale che andremo ad utilizzare si rifà principalmente a quello utilizzato da Hsu e Lin nel loro lavoro del 2016: “*An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives*”. Il modello da loro utilizzato, di cui in Figura 6, dimostrava come l’intenzione all’utilizzo dei sistemi IoT fosse determinata dai benefici percepiti dai consumatori, dalla preoccupazione che essi avevano per il trattamento delle informazioni sulla privacy e dal loro atteggiamento verso questi sistemi. Inoltre, l'atteggiamento media l'impatto dei benefici percepiti e la preoccupazione per la privacy delle informazioni. Il numero di servizi IoT e la massa critica percepita sono considerati esternalità di rete dirette e la compatibilità e complementarità percepite sono definite come esternalità di rete indirette. Questi quattro costrutti sono teorizzati per essere i predittori dei benefici percepiti. La preoccupazione per la riservatezza delle informazioni è trattata come un costrutto di secondo ordine che prende in considerazione la raccolta, l'uso secondario non autorizzato, l'accesso improprio e gli errori.

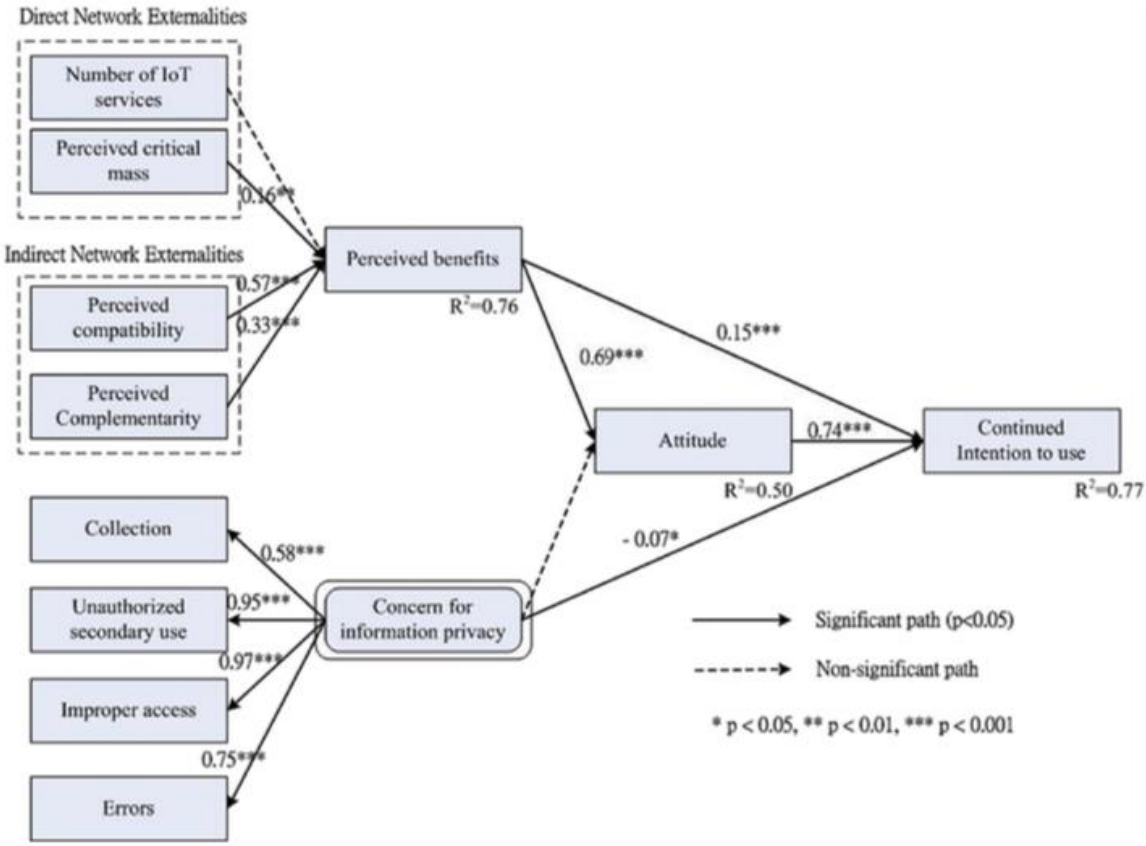
Figura 6 – Framework di riferimento



Sources: Hsu&Lin "An empirical examination of customer adoption of Internet of Things services: network externalities nd concern for information privacy perspectives", 2016

Con questo studio Hsu e Lin hanno contribuito a fornire le seguenti implicazioni teoriche. In primo luogo, a differenza di altri studi precedenti che esaminavano l'effetto delle esternalità di rete sull'adozione e standard di tecnologie informatiche specifiche, come servizi di telefonia mobile (Iimi, 2005), tecnologie di informazione interattiva (Lin & Bhattacherjee, 2008), social network (Chiu et al., 2013; Lin & Lu, 2011), *e-service* (Lin et al., 2011), videogiochi online (Yang & Mai, 2010) e servizi di comunicazione mobile (Kim, Park, & Oh, 2008), pochi studi però hanno esaminato l'effetto delle esternalità di rete sull'utilizzo del servizio IoT. Il loro studio scompone le esternalità di rete e esamina empiricamente la loro influenza sui benefici percepiti. I risultati confermano che la massa critica, la compatibilità e la complementarietà percepite hanno avuto effetti significativi sui benefici percepiti e, a loro volta, influenzano l'atteggiamento verso l'adozione e l'uso continuo dei servizi IoT. Inoltre, le variabili detenevano una vera e propria posizione dominante poiché in grado di spiegare gran parte della varianza nell'atteggiamento verso l'uso dell'IoT, che, a sua volta, era il fattore più influente nel determinare la continua intenzione dell'utente di utilizzare i servizi IoT (Figura 7).

Figura 7 – Framework di riferimento, con beta di regressione

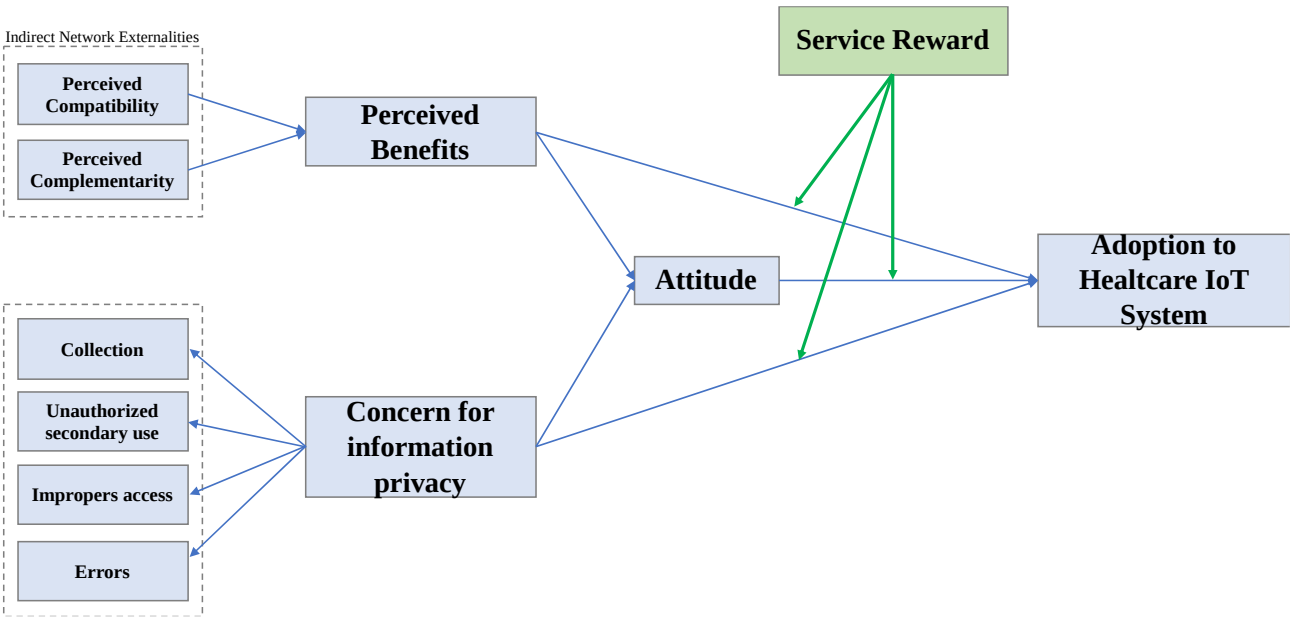


Sources: Hsu&Lin "An empirical examination of customer adoption of Internet of Things services: network externalities nd concern for information privacy perspectives", 2016

Un suggerimento proposto dallo studio riguarderebbe il miglioramento, dal lato dell'offerta, dei servizi IoT in termini di aumento di complementarietà e miglioramento della disponibilità degli stessi piuttosto che aumentarne il numero. In secondo luogo, i precedenti studi indicavano che i problemi di privacy avevano un impatto significativo sull'intenzione degli utenti all'adozione. Hsu e Lin hanno confermato empiricamente il dato, ma con un impatto piuttosto debole. Inoltre, lo studio contribuisce alla letteratura IoT suggerendo anche l'accesso improprio e l'uso secondario non autorizzato ("*improper access*" e "unauthorized *secondary use*") sono entrambi componenti importanti nella disponibilità a concedere informazioni personali CFIP ("*concern for information privacy*"). In conclusione, sono state evidenziate alcune importanti informazioni per i fornitori di servizi IoT. I benefici percepiti, avendo un impatto positivo sull'adozione dei servizi IoT, indicano come gli utenti siano preoccupati dei vantaggi d'uso dell'IoT e del valore che ne scaturisce dall'utilizzo. Inoltre, le esternalità indirette (compatibilità e complementarietà percepite) sono fondamentali per motivare l'adozione tra la maggior parte degli utenti. Quindi i fornitori dovrebbero essere consapevoli della loro importanza, garantendo l'adattamento ai valori e agli stili di vita degli utenti. Come detto precedentemente, i fornitori dovrebbero curare maggiormente l'aspetto della complementarietà dei servizi offerti piuttosto che il numero, questo perché il complementare percepito è risultato essere un fattore predittivo molto influente nella

formazione degli atteggiamenti positivi verso i servizi IoT. Infine, per eliminare i rischi per la privacy, è stato suggerito un aumento dell'offerta verso gli utenti in termini di maggiore concretezza del servizio per quanto riguarda le responsabilità dei provider e i meccanismi di conservazione dei dati. Poiché questo studio si basava su esternalità di rete e CFIP come antecedenti dell'intenzione comportamentale di continuare ad utilizzare i servizi IoT, potrebbero esserci presumibilmente più predittori di adozione come cultura, stile di vita, influenze sociali, personalità e costi. Pertanto, i risultati dello studio di Hsu e Lin non dovrebbero essere generalizzati e applicati all'adozione di IoT basata sull'impresa, come la piattaforma di informazioni logistiche. Proprio su questo spunto finale del loro lavoro sono state gettate le basi per questo studio. L'idea con cui mi sono approcciato all'argomento è stata quella di andare ad indagare quali potessero essere altri agenti in grado di influenzare il processo di adozione dei sistemi IoT da parte dei consumatori. In particolar modo mi sono focalizzato sull'ambito della privacy e trattamento dei dati personali cercando di capire quale fenomeno potesse essere in grado sia di smorzare l'effetto negativo che la CFIP aveva sull'intenzione all'adozione di sistemi IoT sia di incidere positivamente sui benefici percepiti. Per fare questo è stato introdotto un moderatore denominato "*service reward*" ossia "ricompensa di servizio". La variabile moderatrice viene concepita nel momento in cui si va a studiare il fenomeno della privacy *paradox*. L'idea è quella di proporre un servizio come *reward* al fine di modificare l'atteggiamento dei consumatori sia verso l'adozione dei sistemi IoT che verso la CFIP. Inoltre, il *framework* modificato, oltre ad includere la variabile moderatrice, esclude la parte delle esternalità dirette in quanto si erano dimostrate essere molto esplicative della variabile "benefici percepiti" e sarebbe risultato ridondante studiarle nuovamente. Per contro sono state tenute quelle definite come esternalità indirette. La motivazione è da ricercarsi nelle implicazioni che lo studio di Hsu e Lin ha generato. È stato rimarcato più volte quanto la complementarietà e la compatibilità dei servizi IoT dovessero essere implementate in termini di offerta di mercato anziché aumentare il numero di dispositivi/servizi. Da qui la decisione di trattenere solo le esternalità indirette all'interno del *framework* e non quelle dirette. Come riassunto in Figura 8 andremo a misurare come la variabile moderatrice impatta rispettivamente sull'"*attitude*", sulla CFIP e sui "*perceived benefits*" nei confronti dell'"*adoption to healthcare IoT system*". La variabile moderatrice "*service reward*" ha sostanzialmente la funzione di porre in maniera chiara e ben rappresentata l'offerta di servizio che il prodotto IoT è in grado di fornire. La *reward* di servizio in questo caso si identifica nella prevenzione di possibili complicazioni sanitarie ed ha anche la funzione di sensibilizzare ed informare il consumatore rispetto ai dispositivi IoT in ambito *healthcare*. L'effetto di moderazione si compone di un'immagine di un *wearable device* ed una descrizione in cui viene definita in maniera chiara e semplice l'applicazione che ne viene fatta ed i vantaggi/benefici che se ne possono trarre.

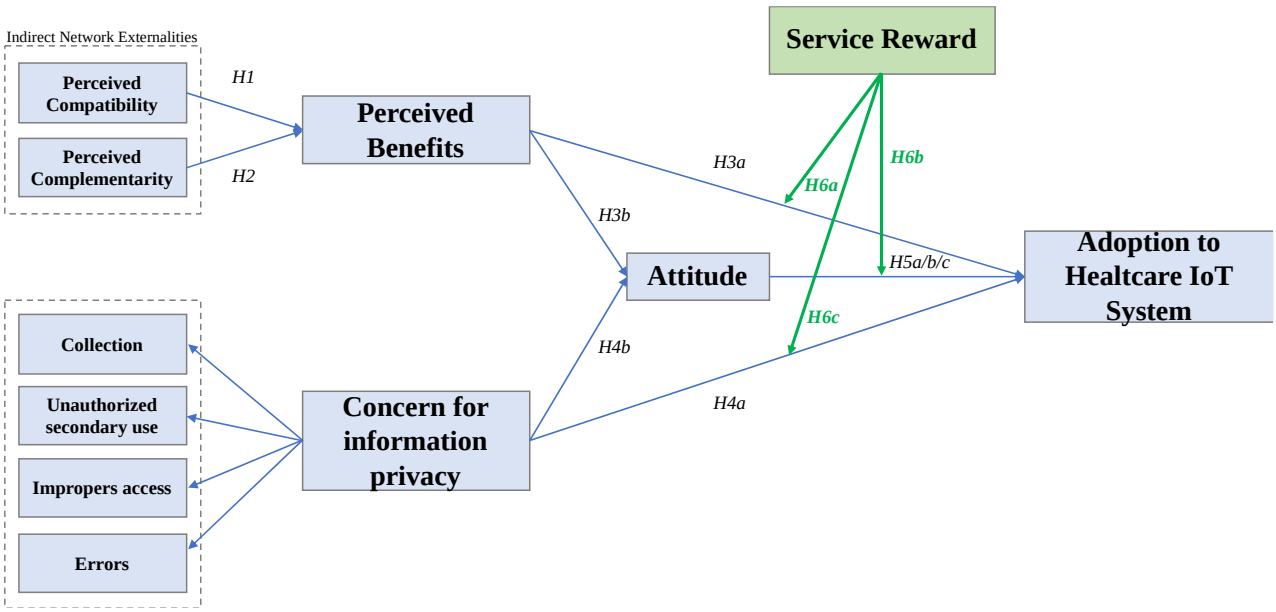
Figura 8– Nuovo Framework di riferimento



2.2.1 – Ipotesi e modello di ricerca

Come precedentemente detto, l'obbiettivo dello studio consiste nel riproporre il modello concettuale dell'articolo di Hsu & Lin (2016), escludendo le variabili riguardanti le esternalità dirette ma aggiungendo una variabile moderatrice denominata "*service reward*" che andrà ad impattare su *Perceived benefits*, CFIP ed *Attitude*. L'intento è quello di replicare l'esperimento estendendolo anche alla tassonomia di *device* in grado di fornire supporto medico, ma soprattutto quello di verificare se un servizio percepito come *reward* sia in grado di confermare il paradosso della privacy. Riassumendo si vuole verificare se e come un servizio ti tipo sanitario collegato ai sistemi IoT, proposto come *reward* in cambio di accesso ai dati personali degli utenti, riesca a verificare il *privacy paradox*. Di seguito vengono presentate le 14 ipotesi di ricerca che si vogliono studiare (Figura 9).

Figura 9– Nuovo Framework di riferimento con Hp



Le variabili che compongono le fondamenta del modello sono quelle inerenti alle esternalità di rete, che come precedentemente detto, in questo studio, saranno comprensive delle sole esternalità indirette. In linea con quanto affermato dall'autore, le esternalità indirette si compongono di due variabili: compatibilità percepita e complementarità percepita. Queste due variabili incorporano al loro interno i costrutti inerenti all'utilità percepita dall'utente in base alla compatibilità e complementarità che i dispositivi IoT hanno verso *device* di altro genere e natura. La compatibilità percepita è il grado in cui un servizio IoT viene percepito come coerente con i valori esistenti, i bisogni e le esperienze passate dei potenziali utilizzatori. Teoricamente, la teoria della diffusione dell'innovazione ha indicato che la compatibilità è l'elemento chiave nel motivare la maggior parte degli adottanti (Rogers, 1983). Studi precedenti hanno confermato che la compatibilità percepita di un'innovazione ha un'influenza positiva verso l'adozione del servizio IoT (Cooper & Zmud, 1990; Hardgrave et al., 2003; Tan & Teo, 2000). Ciò implica l'importanza della compatibilità percepita come antecedente dell'adozione. La variabile complementarietà percepita è invece definita come la disponibilità di funzioni o applicazioni che servono a compilare o completare i servizi IoT. Quando le esternalità di rete indirette riguardano un prodotto/servizio con prodotti/ servizi una maggiore complementarietà crea ulteriori vantaggi di rete per gli utenti (Lin & Bhattacherjee, 2008). Pertanto, nel contesto dei servizi IoT, ulteriori applicazioni complementari e funzioni quali identificazione, transazioni, accesso di controllo, tessere associative, biglietti elettronici e assistenza sanitaria, aumentano la convivialità della vita degli utenti ed efficienza del lavoro. Entrambe le variabili sono in grado di influenzare positivamente i benefici percepiti del consumatore i quali risultano essere un costrutto fondamentale in grado di influenzare direttamente l'intenzione all'adozione di sistemi IoT in ambito medico/sanitario. Di conseguenza, i costrutti e le ipotesi ad essi associati vengono preservati dal modello originale (H1, H2), e adattati al contesto di questa ricerca:

H1. *La compatibilità percepita ha un effetto positivo sui benefici percepiti dall'utilizzo di servizi IoT.*

H2. *La complementarità percepita ha un effetto positivo sui benefici percepiti dall'utilizzo di servizi Iot.*

Precedenti studi hanno confermato che i benefici hanno un effetto significativo sull'atteggiamento e l'intenzione comportamentale (Davis, 1989; Lin & Bhattacherjee, 2008; Yen, Wu, Cheng, & Huang, 2010). L'atteggiamento è stato definito come il grado in cui gli utenti provano sentimenti positivi utilizzando dei servizi IoT. L'intenzione di adozione è la misura in cui un utente crede di adottare i servizi IoT. In generale, gli utenti vorrebbero utilizzare i servizi IoT solo se li trovano utili nella vita o nel lavoro. Di conseguenza, ipotizziamo (H3a; H3b; H6):

H3a. *I benefici percepiti dei servizi IoT avranno un effetto positivo sull'intenzione all'adozione di servizi IoT*

H3b. *I benefici percepiti dei servizi IoT avranno un effetto positivo sull'atteggiamento verso l'adozione dei servizi IoT.*

H5a. *L'atteggiamento verso l'utilizzo dei servizi IoT avrà un effetto positivo sull'adozione di servizi IoT.*

H5b*. I benefici percepiti avranno un effetto positivo sull'atteggiamento verso ed adozione dei servizi IoT in ambito medico-sanitario.*

H5c *La preoccupazione per la privacy delle informazioni dei servizi IoT avrà un effetto negativo sull'atteggiamento verso l'utilizzo ed adozione dei servizi IoT in ambito medico-sanitario.*

Per quel che concerne la CFIP, questa viene presentata sotto diverse sfaccettature: raccolta, uso secondario non autorizzato, accesso improprio ed errori (Smith et., 1996). La "raccolta" riguarda il collezionamento di grandi quantità di informazioni personali da parte dei fornitori di servizi IoT. L'uso secondario non autorizzato è la preoccupazione che le informazioni raccolte per uno scopo possano essere infine utilizzate per altri scopi non autorizzati. L'accesso improprio è definito come la preoccupazione che i dati personali raccolti dai fornitori di servizi IoT siano accessibili alle parti autorizzate. Gli errori comportano la preoccupazione che procedure inadeguate vengano utilizzate per proteggere da errori accidentali o intenzionali nella memorizzazione dei dati personali. In particolare, Stewart e Segars (2002) suggeriscono che il CFIP è più accuratamente modellato come un fattore di secondo ordine piuttosto che quattro fattori correlati del primo ordine. Sostanzialmente, le aziende dovrebbero informare gli utenti su come verranno utilizzate le informazioni raccolte. Tali informazioni consentiranno ai consumatori di formarsi un'idea più accurata sui rischi di divulgazione di dati personali (Harris Interactive & Westin, 1997). Milne e Culnan (2004) hanno suggerito che gli utenti con maggiore preoccupazione per la privacy avranno maggiori probabilità di leggere le informative sulla privacy online rispetto alle persone meno interessate. Ciò suggerisce che il grado di preoccupazione guiderà l'intenzione comportamentale degli utenti. Molti studi hanno verificato empiricamente

che il CFIP ha un effetto negativo sull'intenzione comportamentale in una rete nomologica (Angst & Agarwal, 2009; Dinev & Hart, 2006; Malhotra, Kim, & Agarwal, 2004; Zhou & Li, 2014). Di conseguenza, ipotizziamo:

> ***H4a.*** *La preoccupazione per la privacy delle informazioni dei servizi IoT avrà un effetto negativo sull'intenzione all'adozione verso tali servizi*
> ***H4b.*** *La preoccupazione per la privacy delle informazioni dei servizi IoT avrà un effetto negativo sull'atteggiamento verso l'utilizzo di tali servizi*

Le relazioni tra la *reward* di servizio su benefici percepiti, atteggiamento e CFIP sono l'aspetto topico dello studio del modello. Queste rappresentano la moderazione inserita all'interno dello studio, elemento caratterizzante di tutta la ricerca. Tramite lo studio della variabile si cercherà di capire se questa ha ed eventualmente in che misura, un effetto positivo sulle variabili sopracitate. Di conseguenza ipotizziamo (H7a; H7b; H7c)

> ***H6a.*** *L'esposizione alla reward di servizio ha un effetto positivo sui benefici percepiti dall'utilizzo di servizi IoT.*
> ***H6b.*** *L'esposizione alla reward di servizio ha un effetto positivo sull'atteggiamento verso l'utilizzo di servizi IoT.*
> ***H6c.*** *L'esposizione alla reward di servizio ha un effetto positivo sulla concessione alle informazioni personali derivante derivanti dall'utilizzo di servizi IoT.*

2.3 – Il contributo della ricerca

L'impostazione data allo studio permetterà di andare ad esplorare l'effetto di un ulteriore fenomeno all'interno del *framework*. La moderazione inserita sarà in grado di farci capire se una maggiore presa di coscienza del servizio, con una chiara identificazione della sua *utility*, sia un elemento in grado di modificare le scelte del consumatore in merito all'adozione dei sistemi IoT. Ma non solo, rimane molto importante e sentito l'ambito della privacy, dove il moderatore offrendo un servizio "aggiuntivo" ad un dispositivo IoT (ossia la garanzia di prevenzione e monitoraggio sanitario), dovrebbe essere in grado di smorzare se non addirittura invertire l'avversione all'adozione dei sistemi IoT da parte dell'utente. In altre parole, indagherò se, un'esplicitazione chiara della funzione ed utilità associate ad un servizio IoT sanitario, sia in grado di:

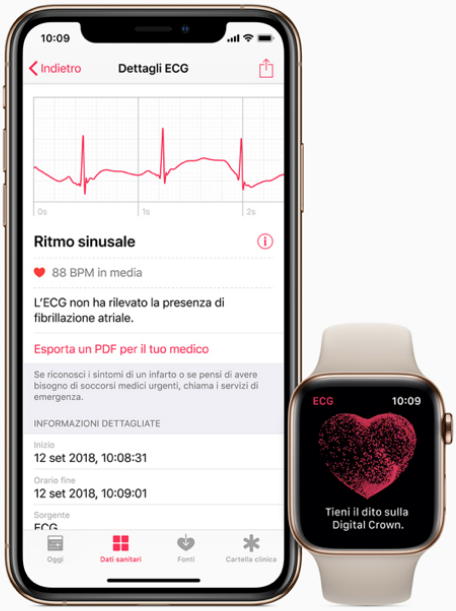
- aumentare la propensione a fornire i dati personali da parte dell'utente;
- aumentare i benefici percepiti dal servizio/dispositivo;
- impattare positivamente sull'attitude.

Se così dovesse essere il contributo netto che la ricerca potrebbe dare, sarebbe la dimostrazione che il meccanismo di *reward* della privacy *paradox*, funziona non solo con *reward* di tipo monetario ma anche con *reward* di servizio.

2.3.1 – Introduzione della variabile "*service reward*"

Come precedentemente introdotto nella parte finale della sezione 2.1, partendo dal modello appartenente allo studio di Hsu e Lin (2016), è stata inserita una nuova variabile definita come "*service reward*" con funzione di moderatore. Questa si va a collocare nella parte finale del modello, trovando spazio tra la variabile dipendente "*Adoption to Healtcare IoT System*" e le rispettive variabili indipendenti "*attitude*", CFIP e "*Perceived benefits*". La variabile si compone di due termini chiave che la identificano, tuttavia questi prima di unirsi coniandone il nome, seguono percorsi logici molto differenti tra loro e di diverso contesto. Per chiarire come nascono la variabile ed il suo nome è opportuno partire dalla parola "*reward*". "*Reward*", ossia "ricompensa" è un termine che compare spesso quando si tratta la tematica attinente al paradosso della privacy, infatti la sua provenienza nello studio deriva proprio da quell'ambito. Ci serviamo di questo termine perché la nostra variabile vuole avere questa funzione, ossia quella di ricompensa. Nel paradosso della privacy si parlava di *reward* come lo strumento/mezzo in grado di permettere ai fornitori di servizi IoT di abbattere la barriera di rifiuto verso l'adozione del prodotto, da parte dei consumatori, a causa del trattamento dei dati personali. In parole semplici, il consumatore non vuole che, tramite l'utilizzo del prodotto/servizio, il fornitore ottenga i suoi dati personali, anche se, in cambio di una r*eward* questo si dichiara disposto ad accettare la raccolta e il trattamento dei dati personali. Generalmente negli studi sul paradosso della privacy, la ricompensa in grado di innescare il repentino cambiamento delle preferenze nel consumatore, consisteva in una *reward* prettamente monetaria. Il termine "*reward*" è stato quindi inserito come componente del nome della variabile proprio per via della sua natura funzionale che è esattamente la stessa che vuole avere la variabile moderatrice. Per quel che riguarda invece la parola "*service*" questa fa riferimento al carattere della *reward*. Se come è stato detto precedentemente la *reward* nell'ambito del paradosso della privacy era solita essere di carattere monetario, in questa circostanza abbiamo voluto cambiare questa sua peculiarità, trasformandola da monetaria a "di servizio". Il motivo per cui la variabile viene caratterizzata in questa maniera è dovuto al fatto che vogliamo andare a capire se un soggetto che non è disponibile a fornire i propri dati personali lo diventa nel momento in cui gli viene fornita una *reward* non più monetaria ma identificata in una garanzia di servizio personalizzato nell'ambito medico/sanitario. Non bisogna dimenticare, infatti, che i dati di cui si parla in questa fase sono quelli strettamente collegati alla sfera della salute di una persona. Quindi la *reward* che l'utente riceve, in cambio dei suoi dati, risulta essere fortemente personalizzata e compatibile. Cosa si intende: a seconda del tipo di problematica che il dispositivo riscontra, l'utente riceverà una *reward* commisurata al problema riscontrato. Avendo quindi così concepito questa variabile, la moderazione è stata inserita nel questionario tramite un'immagine ed una descrizione (Figura 10) ad essa associata in grado di esplicare in maniera chiara e univoca la natura del dispositivo e ponendo l'accento sulle caratteristiche della *reward*.

Figura 10 – Immagine e descrizione con funzione moderatrice



L'immagine raffigura un dispositivo IoT in grado di raccogliere dati in merito alla tua salute e condizione fisica. Adesso immagina che il dispositivo in questione sia in grado di notificare a te ed al tuo medico curante un'anomalia fisica riguardante la patologia maggiormente ti preoccupa, con un preavviso tale da permettere un intervento preventivo in grado di, non solo evitare complicazioni, ma evitare completamente una potenziale situazione critica.

CAPITOLO 3
I Risultati dell'analisi empirica

3.1 – Metodologia di ricerca

Secondo Thomas H.Huxley la scienza non è altro che senso comune opportunamente addestrato ed organizzato; dello stesso parere era Albert Einstein, il quale era solito dire: "la scienza non è altro che un affinamento del pensiero quotidiano". Infatti, sia lo scienziato che l'uomo comune, per la produzione di conoscenza raccolgono le informazioni (garantite da evidenza empirica) al fine di trovare la soluzione ad un determinato problema, o la risposta ad una precisa domanda per la quale non si ritiene di possederne una accettabile.

Le procedure per raccogliere informazioni in tutte le discipline scientifiche sono dette metodi, mentre con metodologia si intende tutto ciò che riguarda l'applicazione dei metodi stessi. La definizione di "metodologia" appena enunciata riflette due principi fondamentali:

- Il carattere normativo e operativo della metodologia: essa esplicita i criteri che guidano una buona ricerca e mette in chiaro come deve essere condotta per ottenere risultati scientificamente validi. Questo carattere pragmatico differenzia la metodologia da altre discipline che si occupano dei principi che guidano la conoscenza, attraverso un livello di maggiore attenzione, come la filosofia della scienza e l'epistemologia; come anche la sociologia della scienza, che si occupa invece del lavoro effettivo degli scienziati, sociali e non (Bruschi, 1991; Ricolfi, 1997).
- Il carattere transdisciplinare della metodologia di ricerca. Nonostante la formazione delle singole metodologie è spesso legata ad una specifica scienza sociale, esse sono tenute ad allargare le loro competenze per riuscire a condurre correttamente determinati tipi di ricerca il cui ambito di applicazione va molto al di là della singola disciplina. La metodologia di ricerca di riferimento in questo caso riguarda la psicologia, la sociologia, la scienza politica, l'antropologia e la statistica.

È utile definire sinteticamente alcuni aspetti fondamentali della ricerca scientifico-sociale:

- L'osservazione: si riferisce al processo di raccolta dati;
- Il fatto: è ciò che viene osservato;
- Le leggi (o principi): sono generalizzatori universali relative a classi di fatti. Esse si presentano come modelli universali e non accidentali;
- La teoria: è una spiegazione sistematica dei fatti e delle leggi osservate in un particolare aspetto della vita;
- I concetti: sono elementi astratti rappresentanti le proprietà che ci si pone di indagare con i quali si costruisce la teoria;
- Le variabili: costituiscono la controparte empirica dei concetti;

Pur essendo, ogni progetto di ricerca, unico per argomento e indagine, è possibile identificare alcune fasi comuni a tutti gli studi.

- **Definizione del problema oggetto di indagine**.

Riguarda l'individuazione e l'analisi del problema per il quale si intende trovare una soluzione/risposta. La ricerca inizia attraverso un attento studio ed analisi della letteratura esistente sull'argomento. Questa fase è necessaria al fine di assicurare che le ipotesi generate tengano conto degli studi e delle ricerche condotte da altri ricercatori. Generalmente è consigliabile riassumere l'obiettivo della ricerca in una singola frase.

- **La concettualizzazione**

Dopo la definizione dell'ipotesi di partenza, questa viene scomposta nelle relative componenti. Vengono elencati e specificati i concetti prima di entrare nel vivo della ricerca. Vengono impostati vari livelli di indagine delineando così il disegno della ricerca, procedendo così alla costruzione delle variabili riducendone il livello di astrazione e dimensione.

- **La scelta del metodo**

Ogni metodo ha i suoi punti di forza e i suoi punti di debolezza. Alcuni concetti vengono studiati in maniera più appropriata tramite alcuni metodi piuttosto che altri. Bisogna valutare in maniera corretta gli obbiettivi del lavoro e in base a quelli scegliere il metodo di ricerca che risulta essere il più confacente.

- **La popolazione ed il campionamento**

A seguito dell'individuazione dei principali concetti e la definizione del processo di operazionalizzazione, viene scelto chi o cosa si intende studiare. La popolazione di uno studio è costituita da il gruppo su cui si intende condurre lo studio. Tendenzialmente si tende a ridurre la popolazione ad un campione che dovrà essere il più possibile rappresentativo della popolazione. Questo vale in base alla scelta del campione; nel caso in cui lo studio riguardasse un target mirato di soggetti il campione dovrà essere anch'esso focalizzato su di essi e non dovrebbe quindi più essere rappresentativo della popolazione ma bensì rappresentativo per lo studio.

- **Definizione del campo di osservazione**

Il metodo di raccolta dei dati cambia a seconda del metodo di ricerca adottato. Nel caso di questo studio sono stati utilizzati questionari quantitativi, condivisi tramite link anonimi e diffusi tramite pubblicazioni su *social network* e inoltro su applicazioni di messaggistica istantanea.

- **Classificazione e misurazione**

Classificare significa effettuare operazioni sostanzialmente analoghe alla classificazione compiuta nella conoscenza comune. Nella conoscenza scientifica però bisogna rispettare rigorosamente delle regole. (Marradi, 1995)

- **Analisi e misurazione dei dati**

In base alla tipologia di rilevazione effettuata, dovranno essere condotte elaborazioni statistiche e trattamento dei dati più o meno complessi al fine di trarre delle conclusioni pertinenti agli interessi dello studio. Inizialmente vengono condotte le analisi definite come "esplorative" o "descrittive". Sono quelle analisi che non richiedono una grande complessità di elaborazione e che restituiscono generalmente un dato descrittivo del campione in maniera molto superficiale. Successivamente vengono condotte le analisi più approfondite attraverso l'ausilio di *software* di analisi (es. STATA, R, SPSS).

- **La divulgazione**

Infine, se le conclusioni risultano essere significative, possono essere pubblicate con suggerimenti su come poter migliorare l'esperimento qualora qualcuno volesse ripeterlo ed andare oltre.

Questo studio si basa utilizza come metodologia di ricerca quella denominata: metodo sperimentale. Questo tipo di metodologia si prepone di indagare rapporti di causa-effetto stabilendone la certezza o meno. Il ricercatore deve ricorrere all'ambiente controllato. Il metodo sperimentale permette così di ridurre sensibilmente (se non addirittura eliminare) il rischio che ipotesi alternative minaccino la validità delle conclusioni dell'indagine. Risulta evidente l'implicazione per cui è necessario il completo controllo di un fattore o di una variabile, della quale ne viene supposto il ruolo causale, e il controllo sulla selezione dei soggetti-casi che costituiscono sia il gruppo sperimentale che quello di controllo. Assume, pertanto, la massima importanza selezionare due gruppi identici: il gruppo sperimentale ed il gruppo di controllo. I membri di ciascun gruppo devono verosimilmente essere rappresentativi dello stesso spaccato della popolazione, avere quindi somiglianza rispetto alle variabili conosciute. Il gruppo sperimentale viene sottoposto al "trattamento" ed il gruppo di controllo no. Viene infine monitorato il comportamento e l'effetto che il trattamento ha avuto sul primo gruppo e confrontato con il comportamento dei componenti del secondo gruppo.
I maggiori vantaggi di questo metodo stanno nella capacità di controllo e rigore logico che esso offre.

3.2 – Variabili del modello ed item scale

La misurazione dei costrutti utili ai fini dello studio è avvenuta tramite la somministrazione di un sondaggio nel quale erano presenti delle scale specifiche in grado di catturare l'intensità di tali costrutti. Per minimizzare la componente di errore durante il processo di misurazione, gli *item* utilizzati sono stati presi da scale empiricamente già validate e presenti in letteratura. Partendo dal presupposto che non è possibile definire un numero "corretto" di *item* necessari a misurare un costrutto (Hinkin, 1998), le scale di misurazione possono

esser composte talvolta da un numero maggiore di domande, talvolta da un numero minore. Le domande utilizzate sono state fedelmente tradotte da quelle originali ed inserite nel questionario. La traduzione dei vari *statement* è stata letterale, tranne nei casi in cui la traduzione andava a generare un'ambiguità all'interno della frase tale da perdere, o rendere poco chiaro, il concetto espresso. In tal caso la frase è stata rimaneggiata e riscritta in modo da renderla il più orientata possibile ai fini della ricerca, rimanendo chiara, semplice ed inequivocabile per il target di rispondenti. Gli item consistono in semplici affermazioni in base alle quali è stato chiesto al rispondente di indicare il grado di accordo o disaccordo. L'intensità della risposta è stata misurata tramite l'ausilio di scale Likert a 5 punti, dove 1 era indicativo di "fortemente in disaccordo" e 5 "fortemente d'accordo". Il questionario invece è stato così strutturato da avere una prima sezione di carattere introduttiva ed altre più mirate sull'argomento. La prima parte si occupava di misurare dati meramente descrittivi, in gran parte anagrafiche del rispondente, utili per poter andare a delineare in una fase successiva, i profili dei rispondenti e quindi del campione. La sezione seguente alla prima invece si occupava di misurare i costrutti attraverso le *item scale*, parte uguale per tutti i rispondenti. L'ultima sezione invece, attraverso una randomizzazione, era la parte in cui veniva somministrata la manipolazione. Questa è la parte in cui si manifesta il *core* della ricerca sin qui condotta. Gli item misurati risultano essenziali per la misurazione della variabile moderatrice. Di seguito le scale utilizzate per la misurazione dei vari costrutti proposti.

3.3.1 – Esternalità Indirette

Il primo dei costrutti presenti nel modello è quello delle "*Network externalities"* definito come la disponibilità di prodotti e servizi compatibili e complementari con i bisogni del rispondente (Lin & Bhattacherjee, 2008). La misurazione di questo unico costrutto va però scomposta in due sottocategorie: una riguardante la compatibilità percepita e l'altra riguardante la complementarità. La scala utilizzata per entrambi i sotto-costrutti rimane fedele a quella del *paper* di riferimento (Hsu & Lin, 2016), traducendo gli item e rendendoli adatti ai fini della ricerca ed al contesto di riferimento. Nel questionario è stato richiesto di indicare quanto ci si trovasse d'accordo, o meno, con le relative affermazioni, utilizzando un punteggio da 1 a 5 su scala Likert dove 1 rappresenta "fortemente in disaccordo" e 5 "fortemente d'accordo".

3.3.1.1 – Compatibilità Percepita

Il costrutto della "*Perceived Complementarity*" rientra sotto il sovra-costrutto delle esternalità di rete indirette e misura l'aumento di utilità percepita dai rispondenti verso i servizi complementari forniti dall'IoT. Nel questionario è stato richiesto di indicare quanto ci si trovi d'accordo, o meno, con le relative affermazioni, utilizzando un punteggio da 1 a 5 su scala Likert dove 1 rappresenta "fortemente in disaccordo" e 5 "fortemente d'accordo". Nella seguente tabella vengono riportati gli item utilizzati nel questionario, la versione in lingua originale e la fonte.

Perceived Compatibility	
• *L'utilizzo dei sistemi IoT è compatibile con tutti gli aspetti della mia salute*	• *Using IoT services is compatible with all aspects of my work.*
• *Penso che l'utilizzo dei servizi IoT si adatti bene al modo in cui mi piace vivere*	• *I think that using IoT services fits well with the way I like to work.*
• *L'utilizzo dei sistemi IoT si adatta al mio stile di vita*	• *Using IoT services fits into my work style.*

***Fonte**: Hsu&Lin "An empirical examination of customer adoption of Internet of Things services: network externalities nd concern for information privacy perspectives", 2016*

3.3.1.2 – Complementarità Percepita

Il costrutto della "*Perceived Compatibility*" è il secondo costrutto facente parte delle esternalità di rete indirette (Chiu et al., 2013; Gandal, 1994; Lin, Tsai, Wang, & Chiu, 2011). Questo si occupa di misurare l'utilità percepita dai rispondenti in merito ad una maggiore compatibilità dei sistemi IoT verso altre applicazioni (Lin et al., 2011). Nel questionario è stato richiesto di indicare quanto ci si trovi d'accordo, o meno, con le relative affermazioni, utilizzando un punteggio da 1 a 5 su scala Likert dove 1 rappresenta "fortemente in disaccordo" e 5 "fortemente d'accordo". Nella seguente tabella vengono riportati gli item utilizzati nel questionario, la versione in lingua originale e la fonte.

Perceived Complementarity	
Una vasta gamma di:	*A wide range of:*
• *Applicazioni è disponibile su sistemi IoT*	• *Applications is available on IoT.*
• *Servizi è disponibile su sistemi IoT*	• *Services is available on IoT*
• *L'utilizzo dell'IoT mi consentirà di completare varie attività*	• *Using IoT will allow me to finish various tasks*
• *Servizi IoT è disponibile su smartphone*	• *IoT services is available on smartphone.*

	• *Support mobile apps is available on IoT*
• *Mobile app di supporto è disponibile su IoT*	

***Fonte**: Hsu&Lin "An empirical examination of customer adoption of Internet of Things services: network externalities nd concern for information privacy perspectives", 2016*

3.3.2 – Benefici Percepiti

Il secondo costrutto presente nel modello riguarda i *"Perceived benefits"*, ed è definito come i benefici che i rispondenti percepiscono grazie all'utilizzo dei dispositivi IoT. Precedenti studi hanno confermato come i benefici abbiano un effetto significativo sull'atteggiamento e l'intenzione comportamentale (Davis, 1989; Lin & Bhattacherjee, 2008; Yen, Wu, Cheng, & Huang, 2010). È stato così misurato il beneficio percepito, in termini di utilità derivante dall'utilizzo di dispositivi IoT. La misurazione del costrutto avviene attraverso l'utilizzo di 5 *items* misurati attraverso scala Likert a 5 punti, dove ad 1 corrispondeva "fortemente in disaccordo" ed a 5 "fortemente d'accordo". Nella seguente tabella vengono riportati gli item utilizzati nel questionario, la versione in lingua originale e la fonte.

Perceived Benefit	
L'Uso dei Servizi IoT:	*Using IoT Services:*
• *migliorerebbe la mia condizione di salute*	• *would improve my work/life performance.*
• *migliora la mia efficacia quotidiana*	• *enhances my work/life effectiveness*
• *mi consente di svolgere i miei compiti quotidiani più serenamente*	• *enables me to accomplish my work/life tasks more quickly*
• *mi aiuta a ottenere informazioni utili sulla mia salute* • *è molto utile per la mia salute*	• *help me get useful information for my work/ life* • *is very useful for me*

***Fonte**: Hsu&Lin "An empirical examination of customer adoption of Internet of Things services: network externalities nd concern for information privacy perspectives", 2016*

3.3.3 – CFIP

Per quel che concerne il costrutto della "*Concern For Information Privacy*" (CFIP) questo risulta essere il frutto di: "*Collection*", "*Unauthorized secondary use*", "*Improper access*" ed "*Errors*" (Smith et al., 1996). Questo costrutto risulterà essere in seguito il risultato di una *factor analysis* condotta con le appena menzionate variabili. In particolare, Stewart e Segars (2002) suggeriscono che la CFIP è modellata più accuratamente come un fattore di secondo ordine piuttosto che quattro fattori correlati del primo ordine. Gli item di misurazione ci permettono di comprendere come i consumatori, una volta informati del trattamento e raccolta delle loro informazioni, valuteranno i rischi di divulgazione dei propri dati (Harris Interactive & Westin, 1997). Milne e Culnan (2004) hanno suggerito che gli utenti con maggiore preoccupazione per la privacy avranno maggiori probabilità di leggere le informative sulla privacy online rispetto alle persone meno interessate. Questo suggerisce che le preoccupazioni per la privacy avranno funzione di *driver* per gli utenti. Tra tutti, questo risulta essere il costrutto contenente il maggior numero di item, 14 per l'esattezza, 4 per le dimensioni di *collection* e *errors* e 3 per *secondary unathorized* use e *improper access*. La misurazione del costrutto avviene attraverso l'utilizzo di scale Likert a 5 punti, dove ad 1 corrisponde "fortemente in disaccordo" ed a 5 "fortemente d'accordo".

3.3.3.1 – Collezionamento

La raccolta dei dati ("*collection*") riguarda la raccolta di grandi quantità di informazioni personali identificabili da parte dei fornitori di servizi IoT.

3.3.3.2 – Utilizzo Secondario non Autorizzato

L'uso secondario non autorizzato è la preoccupazione che le informazioni raccolte per uno scopo possano essere infine utilizzate per altri scopi non autorizzati.

3.3.3.3 – Accesso Improprio

L'accesso improprio è definito come la preoccupazione che i dati personali raccolti dai fornitori di servizi IoT siano accessibili alle parti autorizzate.

3.3.3.4 – Errori

Gli errori comportano la preoccupazione che procedure inadeguate vengano utilizzate per proteggere da errori accidentali o intenzionali nella memorizzazione dei dati personali.

CFIP	
Collezionamento	***Collection***
• *Di solito mi infastidisce quando i fornitori di servizi IoT mi chiedono informazioni personali sulla mia salute/storia clinica*	• *It usually bothers me when IoT service providers ask me for personal information.*
• *Quando i fornitori di servizi IoT mi chiedono informazioni personali sulla mia salute/storia clinica, a volte ci penso due volte prima di fornirle*	• *When IoT service providers ask me for personal information, I sometimes think twice before providing it.*
• *Sono preoccupato che i fornitori di servizi IoT stiano raccogliendo troppe informazioni personali su di me in merito alle mie funzioni vitali*	• *I am concerned that IoT service providers are collecting too much personal information about me.*
• *Mi da fastidio dare informazioni personali a così tanti fornitori di servizi IoT*	• *It bothers me to give personal information to so many IoT service providers*
Utilizzo Secondario non Autorizzato	***Unathorized Secondary Access***
• *I fornitori di servizi IoT non dovrebbero utilizzare le informazioni personali per scopi non autorizzati*	• *IoT service providers should not use personal information for any unauthorized purpose*
• *Quando le persone forniscono informazioni personali ai fornitori di servizi IoT per qualche motivo, i fornitori di servizi IoT non dovrebbero mai usare le informazioni per nessun altro scopo*	• *When people give personal information to the IoT service pro- viders for some reason, the IoT service providers should never use the information for any other purpose.*
• *I fornitori di servizi IoT non dovrebbero mai vendere informazioni personali ad altre compagnie se non specificatamente autorizzati a farlo*	• *IoT service providers should never share personal information with other companies unless specifically authorized to do so by user.*
Accesso Improprio	***Improper Access***
• *I fornitori di servizi IoT dovrebbero dedicare più tempo e sforzi per prevenire l'accesso non autorizzato alle informazioni personali*	• *IoT service providers should devote more time and effort to preventing unauthorized access to personal information.*

• *I fornitori di servizi IoT dovrebbero prendere ulteriori provvedimenti per assicurarsi che le informazioni personali nei loro file siano accurate*	• *IoT service providers should take more steps to make sure that the personal information in their files is accurate.*
• *I fornitori di servizi IoT dovrebbero prendere ulteriori provvedimenti per assicurarsi che le persone non autorizzate non possano accedere alle informazioni personali nei loro computer*	• *IoT service providers should take more steps to make sure that unauthorized people cannot access personal information in their computers.*
Errori	***Errors***
• *Tutte le informazioni personali nei database dei computer dei fornitori di servizi IoT dovrebbero essere verificate con maggiore accuratezza, indipendentemente da quanto costi*	• *All the personal information in IoT service providers' computer databases should be double-checked for accuracy - no matter how much this costs*
• *I fornitori di servizi IoT dovrebbero prendere ulteriori provvedimenti per garantire che le informazioni personali nei loro file siano accurate*	• *IoT service providers should take more steps to make sure that the personal information in their files is accurate.*
• *I fornitori di servizi IoT dovrebbero avere procedure migliori per correggere gli errori nelle informazioni personali*	• *IoT service providers should have better procedures to correct errors in personal information.*
• *I fornitori di servizi IoT dovrebbero dedicare più tempo e sforzi a verificare l'esattezza delle informazioni personali nelle loro schede.*	• *IoT service providers should devote more time and effort to verifying the accuracy of the personal information in their databases.*

***Fonte**: Hsu&Lin "An empirical examination of customer adoption of Internet of Things services: network externalities nd concern for information privacy perspectives", 2016*

3.3.4 – Attitude

Il costrutto dell'atteggiamento risulta essere molto importante ai fini dello studio, in quanto questo assume la funzione di mediatore tra benefici percepiti e CFIP. L'atteggiamento è stato definito come la percezione di sentimenti positivi da parte degli utenti durante l'utilizzo dei servizi IoT. La misurazione del costrutto avviene attraverso l'utilizzo di scale Likert a 5 punti, dove ad 1 corrisponde "fortemente in disaccordo" ed a 5 "fortemente d'accordo".

Attitude	
L'Uso dei Servizi IoT:	*Using IoT Services:*
• *Mi piace usare servizi IoT* • *Mi sento a mio agio nell'utilizzare i servizi IoT* • *Nel complesso, la mia attitudine verso l'utilizzo dei sistemi IoT è favorevole*	• *I like using IoT services.* • *I feel good about using IoT services.* • *Overall, my attitude towards using IoT services is favorable.*

***Fonte**: Hsu&Lin "An empirical examination of customer adoption of Internet of Things services: network externalities nd concern for information privacy perspectives", 2016*

3.3.5 – Adozione dei sistemi IoT destinati all'ambito medico/sanitario

L'intenzione all'adozione dei sistemi IoT in ambito medico/sanitario è la misura in cui un utente intende accettare l'utilizzo di un servizio IoT. In generale gli utenti vorrebbero adottare i servizi IoT solo se li trovano utili nella vita o nel lavoro. I collegamenti tra questo costrutto ed i benefici percepiti, la CFIP e l'atteggiamento sono quelli che risentono anche dell'effetto della variabile moderatrice. Infatti, questa risulta essere la variabile dipendente che in base alle risposte date dai rispondenti e dalle future analisi in profondità ci permetterà di capire se la variabile moderatrice avrà svolto o meno l'effetto ricercato. La misurazione del costrutto avviene attraverso l'utilizzo di scale Likert a 5 punti, dove ad 1 corrisponde "fortemente in disaccordo" ed a 5 "fortemente d'accordo".

IoT system Adoption	
L'Uso dei Servizi IoT:	*Using IoT Services:*
• *Intendo adottare sistemi IoT in futuro* • *Intendo adottare i servizi medici IoT* • *Intendo raccomandare ai miei amici l'adozione di sistemi medici IoT in futuro*	• *I intend to keep using IoT in the future.* • *I intend to continue using IoT services.* • *I intend to recommend my friends to use IoT services in the future.*

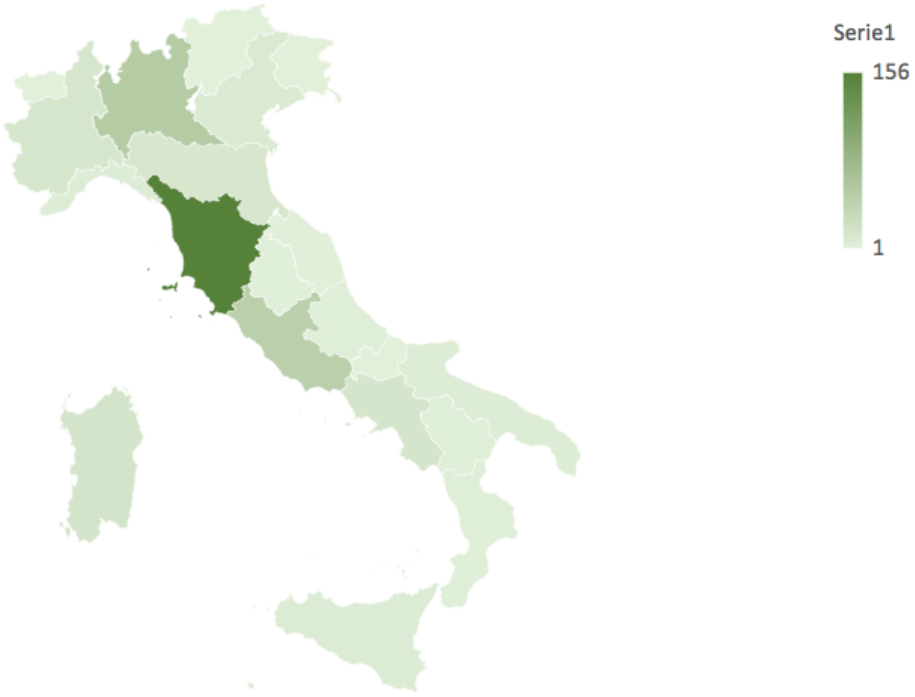
***Fonte**: Hsu&Lin "An empirical examination of customer adoption of Internet of Things services: network externalities nd concern for information privacy perspectives", 2016*

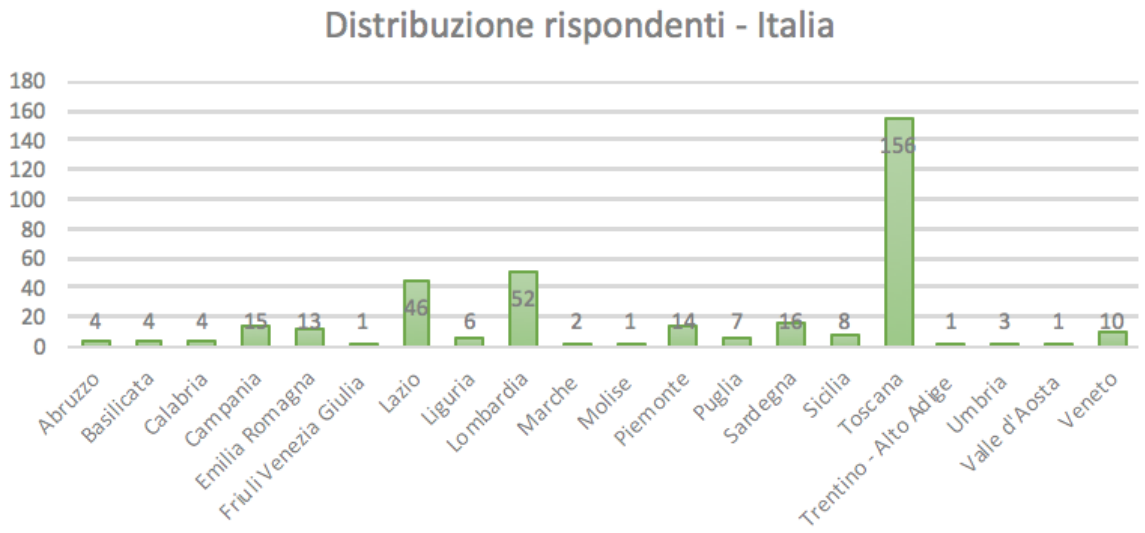
3.3 – Data Collection

Come ampiamente esposto nella sezione 3.1 del capitolo, la dimensione, nonché la composizione del campione, risultano essere elementi cruciali soprattutto per le ricerche di tipo quantitativo. Un campione di dimensione troppo ridotta risulterebbe essere inadeguato e potrebbe presentare delle importanti problematiche

in termini di analisi dei dati e nella fase di verifica delle ipotesi, specialmente nella particolare fattispecie delle analisi con ausilio di tecniche di regressione, come nel caso di questa ricerca. In virtù di quanto detto il questionario è stato somministrato ad un campione comprensivo di 446 rispondenti, equamente suddiviso tra questionari con effetto di moderazione e non. Inoltre, la distribuzione dei rispondenti sul territorio nazionale è risultata essere comprensiva di tutte le regioni d'Italia, con una frequenza di questionari ottenuti abbastanza omogenea, tranne per quanto riguarda la regione Toscana fortemente polarizzata. (Tabella 3.1).

Tabella 3.1– Distribuzione geografica dei rispondenti a livello nazionale





Il sondaggio online è stato distribuito attraverso link sui principali *social network* (postando il sondaggio in svariate community di più varia natura ed interesse) e via whatsapp. Come in precedenza, il campione finale

si compone di 446 rispondenti, che dopo una prima scrematura dei dati, è risultato ridotto a 271 unità. L'eliminazione di questi dati è da imputarsi principalmente ad una importante mancanza di campi compilati, ossia di domande risposte del questionario, ed in seconda battuta ad eventuali sbarramenti non superati imputabili alle *question check*. I due sottogruppi che ne derivano pertanto si compongono, rispettivamente, di 134 rispondenti per il campione di controllo e di 137 per il campione sperimentale. Le informazioni demografiche ed anagrafiche dei rispondenti sono riportati rispettivamente nelle tabelle 3.2 e 3.3.

3.3.1 – Campione degli utenti senza manipolazione

Il campione di controllo è risultato essere abbastanza equilibrato, nonostante il genere tenda a favore di quello femminile (59,3% femmine e 39,7% maschi), mentre l'età risulta essere fortemente concentrata nelle fasce di età comprese tra 20-24 e 25-29 che, se sommate, coprono il 62,7% del campione. Per quel che concerne la professione, il 42,52% dei rispondenti ha un'occupazione mentre il 45,5% sono studenti, dato che si dimostra in linea con l'età media restituita dal campione (il restante 11,9% rientrano nelle categorie di disoccupati o pensionati). Per quel che riguarda il livello di istruzione del campione il 54,4% ha conseguito almeno una laurea di primo livello, il 33,5% possiede un diploma di istituto superiore e solo il 6,7% non va oltre la terza media. Risulta interessante notare come, nonostante la maggioranza del campione abbia ammesso di non avere familiarità con il concetto di IoT (62,7% no contro il 37,3% si), quasi la totalità si è dichiarata "abbastanza" (29,1%) o "molto" (63,4%) preoccupata in merito alla tutela dei dati personali raggiungendo un totale pari al 92,5% del campione. Sono stati rilevati dati analoghi anche quando la domanda è stata posta in maniera specifica verso la tutela dei dati contenenti informazioni sulla propria salute con una copertura quasi totale del campione (91%) dettata nuovamente da "abbastanza" (23,1%) e "molto" (63,4%). Le patologie che si sono rivelate essere le principali cause di preoccupazioni nei rispondenti vedono in primis le complicazioni di natura cardiovascolare con quasi la metà del campione pari al 41%, seguite da altre complicazioni di varia natura equivalenti al 38%. I rispondenti hanno inoltre messo in luce come le motivazioni di tali preoccupazioni siano dovute alla conoscenza di queste patologie ma senza che ve ne sia mai stato un reale interessamento a livello di storia clinica da parte loro (55,2%). Infine, il 78% dei rispondenti si è dichiarato favorevole a spendere in una fascia compresa tra gli 0 ed i 300€ per usufruire di un servizio IoT a carattere sanitario.

Tabella 3.2– Dati anagrafici. Campione senza manipolazione

Informazioni Demografiche	Categoria	Frequenza	Percentuale (%)
Genere	Maschio	54	40,2985075
	Femmina	80	59,7014925
	Totale	134	100
Età	Under 20	4	2,98507463
	20 - 24	45	33,5820896
	25 - 29	39	29,1044776
	30 - 39	21	15,6716418
	40 - 49	8	5,97014925
	Over 50	17	12,6865672
	Totale	134	100
Occupazione	Studente	33	24,6268657
	Studente/Lavoratore	28	20,8955224
	Dipendente	38	28,358209
	Libero Professionista	19	14,1791045
	Disoccupato	7	5,2238806
	Pensionato	9	6,71641791
	Totale	134	100
Titolo di Studio	Pensionato		
	Licenza Elementare	1	0,74626866
	Licenza 3° media	8	5,97014925
	Diploma	45	33,5820896
	Laurea di 1° Grado	38	28,358209
	Laurea di 2° Grado	35	26,119403
	Altro	6	4,47761194
	Totale	133	99,2537313
Familiarià con il concetto di IoT	Si	50	37,3134328
	No	84	62,6865672
	Totale	134	100
Importanza della tutela della privacy	Per niente	1	0,74626866
	Poco	3	2,23880597
	Indifferente	6	4,47761194
	Abbastanza	39	29,1044776
	Molto	85	63,4328358
	Totale	134	100
Importanza della tutela della privacy inerente a dati sulla propria salute	Per niente	1	0,74626866
	Poco	3	2,23880597
	Indifferente	8	5,97014925
	Abbastanza	31	23,1343284
	Molto	91	67,9104478
	Totale	134	100
Patolodie di maggiore preoccupazione	Cardiovascolari	55	41,0447761
	Diabete	12	8,95522388
	Problemi respiratori	14	10,4477612
	Altro	51	38,0597015
	Totale	132	98,5074627
Motivazione	Conosco ma non ne soffro	74	55,2238806
	Conosco e ne ho sofferto/n	27	20,1492537
	Altro	33	24,6268657
	Totale	134	100
Disposizione a pagare	0 - 100 €	45	33,5820896
	100 - 300 €	60	44,7761194
	300 - 600 €	23	17,1641791
	600 - 900 €	1	0,74626866
	più di 1000€	2	1,49253731

3.3.2 – Campione degli utenti con manipolazione

Per quel che riguarda il campione di rispondenti esposto alla manipolazione i risultati sono piuttosto in linea con quanto visto nella sezione 3.3.1. In questo caso, la distribuzione di genere risulta essere più omogenea (51,8% femmine e 48,2% maschi); anche in questo caso l'età media dominante risulta essere occupata dalle fasce di età compresa tra 20-24 e 25-29 che aggregate interessano il 60,5% del campione. In merito alla professione si osservano dati analoghi: il 46,7% dei rispondenti ha dichiarato di avere un'occupazione ed il 45,9% che rientra nella categoria studenti (il restante 7,2% riguarda disoccupati o pensionati). Il livello di istruzione del campione conferma le stime precedenti con il 57,6% di rispondenti avente almeno la laurea di primo livello, il 31,3% possiede un diploma di istituto superiore e solo il 7,2% non va oltre la terza media. In questo caso risulta interessante osservare come il campione sia variato in termini di familiarità con il concetto di IoT. Infatti, la percentuale di rispondenti non avente familiarità con tale concetto diminuisce al 54,7% (contro il 62,7% della sezione 3.3.1) mentre aumenta al 44,5% quella di coloro che hanno confidenza con esso (contro il 37,3% della sezione 3.3.1). Una significativa differenza la si nota invece quando viene richiesta l'importanza della tutela dei dati della privacy, nonostante anche in questo caso quasi la totalità del campione si colloca tra "abbastanza" (30,6%) e "molto" (53,2%) per un totale di 83,9%, si vede come abbia perso quasi 10 punti percentuali rispetto al campione senza manipolazione. Stessa sorte si verifica per la tutela della privacy riguardante i dati di natura sanitaria, il campione si polarizza sempre su "abbastanza" (29,19%) e "molto" (56,20%) per un totale di copertura pari all'85,4%, ma anche in questo caso perde quasi 6 punti percentuali rispetto a quanto visto nella sezione 3.3.1. Le stime ottenute in merito alle patologie percepite come principali cause di preoccupazioni nei rispondenti invece sono sostanzialmente invariate rispetto al campione di controllo: vedono anche in questo caso i problemi cardiovascolari al primo posto seguiti da altre patologie di varia natura. Lo stesso vale per le motivazioni messe in gioco dai rispondenti nel momento in cui dovevano dare una risposta alla domanda precedente. Infine, il 75% dei rispondenti si è dichiarato favorevole a spendere in una fascia compresa tra gli 0 ed i 300€ per usufruire di un servizio IoT a carattere sanitario.

Tabella 3.3– Dati anagrafici. Campione con manipolazione

Informazioni Demografiche	Categoria	Frequenza	Percentuale (%)
Genere	Maschio	66	48,1751825
	Femmina	71	51,8248175
	Totale	137	100
Età	Under 20	6	4,37956204
	20 - 24	39	28,4671533
	25 - 29	44	32,1167883
	30 - 39	13	9,48905109
	40 - 49	15	10,9489051
	Over 50	20	14,5985401
	Totale	137	100
Occupazione	Studente	34	24,8175182
	Studente/Lavoratore	29	21,1678832
	Dipendente	43	31,3868613
	Libero Professionista	21	15,3284672
	Disoccupato	5	3,64963504
	Pensionato	5	3,64963504
	Totale	137	100
Titolo di Studio	Licenza Elementare	0	0
	Licenza 3° media	10	7,29927007
	Diploma	43	31,3868613
	Laurea di 1° Grado	40	29,1970803
	Laurea di 2° Grado	39	28,4671533
	Altro	5	3,64963504
	Totale	137	100
Familiarià con il concetto di IoT	Si	61	44,5255474
	No	75	54,7445255
	Totale	136	99,270073
Importanza della tutela della privacy	Per niente	2	1,45985401
	Poco	4	2,91970803
	Indifferente	15	10,9489051
	Abbastanza	42	30,6569343
	Molto	73	53,2846715
	Totale	136	99,270073
Importanza della tutela della privacy inerente a dati sulla propria salute	Per niente	2	1,45985401
	Poco	3	2,18978102
	Indifferente	13	9,48905109
	Abbastanza	40	29,1970803
	Molto	77	56,2043796
	Totale	135	98,540146
Patolodie di maggiore preoccupazione	Cardiovascolari	53	38,6861314
	Diabete	12	8,75912409
	Problemi respiratori	20	14,5985401
	Altro	52	37,9562044
	Totale	137	100
Motivazione	Conosco ma non ne soffro	89	64,9635036
	Conosco e ne ho sofferto/n	19	13,8686131
	Altro	28	20,4379562
	Totale	136	99,270073
Disposizione a pagare	0 - 100 €	42	30,6569343
	100 - 300 €	62	45,2554745
	300 - 600 €	21	15,3284672
	600 - 900 €	6	4,37956204
	più di 1000€	3	2,18978102

3.4 – Analisi preliminari

3.4.1 – Alpha di Cronbach

Le scale utilizzate al fine di misurare i costrutti presentati nel modello concettuale si basano su una struttura multi-item variabile. Ogni item è inserito con lo scopo di misurare diversi aspetti di uno stesso concetto, questo per avere, quanto più possibile, una visione d'insieme del costrutto. Per essere sicuri che ogni item sia effettivamente in grado di misurare lo stesso concetto è necessario testare la loro affidabilità in termini di consistenza interna (*internal consistency reliability*). L'affidabilità (*reliability*), in questa circostanza, viene intesa come il grado con cui una scala riesce a produrre risultati coerenti se venissero effettuate molteplici misurazioni (Malhotra, Birks e Wills, 2012). Per poter asserire che l'affidabilità di una scala sia effettivamente significativa in termini di *internal conisstency* è necessario condurre dei test su di essa. Il più diffuso e comunemente riconosciuto è l'alpha di Cronbach, un coefficiente che varia da 0 ad 1, dove 0.6 rappresenta il valore soglia del valore minimo richiesto per ritenere accettabile la scala che si vuole utilizzare. Prima di poter testare le ipotesi di ricerca, sono state condotte delle analisi preliminari su tutti i set di item scale utilizzati per misurare i vari costrutti. Per lo studio sono state utilizzate delle scale precedentemente testate e validate in letteratura, questo al fine di ridurre i rischi collegati al possibile ottenimento di un risultato non soddisfacente. Le aspettative sono state confermante, infatti, tutti i coefficienti *alpha* sono risultati superiori ad un valore di 0.70, confermando così una robusta affidabilità delle scale scelte per questa ricerca. Una volta accertato che ogni item di ciascuna scala misurasse complessivamente lo stesso costrutto, sono state generate le variabili finali sulle quali si basano le analisi statistiche presenti nel prossimo paragrafo. Sulla base dei risultati ottenuti, di seguito viene riportata una tabella (Tabella 3.4) contenente informazioni statistiche di natura descrittiva, riportante i valori degli *alpha* dei rispettivi item, la *composite reliability* (affidabilità generale della scala), e l'AIC (*Average Interitem Covariance)*.

Tabella 3.4– Analisi preliminari. Item scale ed alpha di Cronbach

Misurazione dell'Item		Item Reliability	Composite Reliability	AIC
PY1	*L'utilizzo dei sistemi IoT è compatibile con tutti gli aspetti della mia salute*	0.88	0.78	0.60
PY2	*Penso che l'utilizzo dei servizi IoT si adatti bene al modo in cui mi piace vivere*	0.57		
PY3	*L'utilizzo dei sistemi IoT si adatta al mio stile di vita*	0.59		
PC1	*Una vasta gamma di applicazioni è disponibile su sistemi IoT*	0.79	0.83	0.34
PC2	*Una vasta gamma di servizi è disponibile su sistemi IoT*	0.78		
PC3	*L'utilizzo dell'IoT mi consentirà di completare varie attività*	0.83		
PC4	*Una vasta gamma di servizi IoT è disponibile su smartphone*	0.78		
PC5	*Una vasta gamma di mobile app di supporto è disponibile su IoT*	0.80		
PB1	*L'uso dei servizi IoT migliorerebbe la mia condizione di salute*	0.77	0.81	0.40
PB2	*L'uso dei servizi IoT migliora la mia efficacia quotidiana*	0.80		
PB3	*L'uso dei servizi IoT mi consente di svolgere i miei compiti quotidiani più serenamente*	0.79		
PB4	*L'uso dei servizi IoT mi aiuta a ottenere informazioni utili sulla mia salute*	0.77		
PB5	*L'uso dei servizi IoT è molto utile per la mia salute*	0.76		
CN1	*Di solito mi infastidisce quando i fornitori di servizi IoT mi chiedono informazioni personali sulla mia salute/storia clinica*	0.89	0.90	0.81
CN2	*Quando i fornitori di servizi IoT mi chiedono informazioni personali sulla mia salute/storia clinica, a volte ci penso due volte prima di fornirle*	0.86		
CN3	*Sono preoccupato che i fornitori di servizi IoT stiano raccogliendo troppe informazioni personali su di me in merito alle mie funzioni vitali*	0.87		
CN4	*Mi da fastidio dare informazioni personali a così tanti fornitori di servizi IoT*	0.86		
SU1	*I fornitori di servizi IoT non dovrebbero utilizzare le informazioni personali per scopi non autorizzati*	0.52	0.70	0.24
SU2	*Quando le persone forniscono informazioni personali ai fornitori di servizi IoT per qualche motivo, i fornitori di servizi IoT non dovrebbero mai usare le informazioni per nessun altro scopo*	0.54		
SU3	*I fornitori di servizi IoT non dovrebbero mai vendere informazioni personali ad altre compagnie se non specificatamente autorizzati a farlo*	0.71		
IA1	*I fornitori di servizi IoT dovrebbero dedicare più tempo e sforzi per prevenire l'accesso non autorizzato alle informazioni personali*	0.73	0.79	0.25
IA2	*I fornitori di servizi IoT dovrebbero prendere ulteriori provvedimenti per assicurarsi che le informazioni personali nei loro file siano accurate*	0.73		
IA3	*I fornitori di servizi IoT dovrebbero prendere ulteriori provvedimenti per assicurarsi che le persone non autorizzate non possano accedere alle informazioni personali nei loro computer*	0.69		
ERR1	*Tutte le informazioni personali nei database dei computer dei fornitori di servizi IoT dovrebbero essere verificate con maggiore accuratezza, indipendentemente da quanto costi*	0.83	0.85	0.37
ERR2	*I fornitori di servizi IoT dovrebbero prendere ulteriori provvedimenti per garantire che le informazioni personali nei loro file siano accurate*	0.83		
ERR3	*I fornitori di servizi IoT dovrebbero avere procedure migliori per correggere gli errori nelle informazioni personali*	0.79		
ERR4	*I fornitori di servizi IoT dovrebbero dedicare più tempo e sforzi a verificare l'esattezza delle informazioni personali nelle loro schede.*	0.80		
ATT1	*Mi piace usare servizi IoT*	0.86	0.90	0.61
ATT2	*Mi sento a mio agio nell'utilizzare i servizi IoT*	0.83		
ATT3	*Nel complesso, la mia attitudine verso l'utilizzo dei sistemi IoT è favorevole*	0.90		
AD1	*Intendo adottare sistemi IoT in futuro*	0.90	0.94	0.71
AD2	*Intendo adottare i servizi medici IoT*	0.90		
AD3	*Intendo raccomandare ai miei amici l'adozione di sistemi medici IoT in futuro*	0.94		

3.5 – Risultati: i test di verifica delle ipotesi

Per verificare la bontà delle ipotesi di ricerca presentate nella sezione 2.2.1 del secondo capitolo, è stata condotta una serie di test d'ipotesi grazie all'ausilio di modelli di regressione lineare semplice e multipla.

Queste ci hanno permesso di identificare l'esistenza o meno di una relazione causale statisticamente significativa tra le variabili indipendenti e la variabile dipendente del modello. Per i test condotti sulle ipotesi, e sul campione raccolto, è stato adottato un intervallo di confidenza del 95%. Questo è rappresentativo dell'intervallo di valori nel quale si ritiene debba ricadere il valore vero della popolazione, tollerando così un margine di errore α con soglia massima del 5% (0.05). Utilizzare un livello di confidenza del 95% significa che se si volesse ripetere l'analisi 100 volte seguendo lo stesso metodo ma su 100 campioni diversi, in 95 casi il vero valore della popolazione ricadrebbe all'interno dell'intervallo di confidenza selezionato nel nostro campione, "sbagliando" soltanto 5 volte. Lo stesso meccanismo lo si può applicare per un intervallo di confidenza del 99%, in questo caso il margine di errore risulta essere più contenuto in quanto sarebbe equivalente ad un α di 0.01. Se un valore statistico *t* della variabile indipendente del modello di regressione lineare dovesse essere superiore al valore soglia di 1.96 (per un intervallo di confidenza del 95%) o addirittura 2.58 (per un intervallo di confidenza del 99%), con una probabilità associata α minore di 0.05 (o minore 0.01), sarebbe possibile rifiutare l'ipotesi nulla *H0*, confermando la relativa ipotesi di ricerca che si vuole testare *H1*. L'ipotesi nulla corrisponde allo *status quo* delle cose; semplificando significa che si verifica l'opposto della nostra affermazione corrispondente all'ipotesi di ricerca (H1). Si prenda ad esempio la prima ipotesi (H1) tra quelle proposte nel capitolo 2: "*La compatibilità percepita ha un effetto positivo sui benefici percepiti dall'utilizzo di servizi IoT".* L'ipotesi nulla (H0) corrisponderà quindi all'affermazione: "*La compatibilità percepita NON ha un effetto positivo sui benefici percepiti dall'utilizzo di servizi IoT".* Seguendo una dicitura statistica appropriata l'ipotesi nulla e l'ipotesi alternativa possono essere rappresentate come segue:

$$H_0: \beta_1 \leq 0$$
$$H_1: \beta_1 > 0$$

Dove il coefficiente β_1 rappresenta il coefficiente angolare della retta di regressione. Se quindi i risultati delle analisi condotte con un modello di regressione semplice confermassero che la variabile indipendente *X* (in questo caso la compatibilità) fosse statisticamente significativa, tale da instaurare un rapporto di relazione lineare con la variabile dipendente *Y* (in questo caso i *benefici percepiti*), sarebbe possibile determinare il valore della *Y* tramite una semplice equazione lineare: $Y = \beta_0 + \beta_1 X_1 + e_1$. Questa equazione rappresenta una retta in grado di approssimare la nuvola di punti dei dati campionari. Per quanto riguarda i modelli di regressione multipla, invece, è possibile affermare che questi seguono la stessa logica spiegata sin ora, con l'unica differenza che le variabili indipendenti del modello saranno più di una e si avranno tanti β quanti sono i regressori inseriti nel modello al fine di spiegare la relazione causale tra le variabili *X* ed *Y*. Da questo punto in avanti si procederà alla presentazione dei risultati ottenuti grazie alle analisi statistiche condotte, commentando alcuni indicatori utili a testare le ipotesi di ricerca proposte quali:

- il *p-value* del modello di regressione: utile a comprendere il livello di significatività del modello o della singola variabile.

- il valore statistico *t* dei singoli regressori
- il coefficiente di regressione (β) delle variabili indipendenti
- il coefficiente di determinazione *R-squared* del modello: in grado di misurare la forza della relazione tra le variabili indicando la porzione di varianza totale della variabile dipendente *Y* spiegata dalla variabile/i indipendente/i *X*.

Di seguito sono analizzate le ipotesi formulate durante la ricerca:

> ***H1.*** *La compatibilità percepita ha un effetto positivo sui benefici percepiti dall'utilizzo di servizi IoT.*

L'ipotesi formulata sulla compatibilità percepita risulta essere supportabile, in quanto la *t* statistica della variabile *perceived compatibility* risulta pari a 6.32 per il totale del campione misurato (Appendice 1). La probabilità associata è inferiore a 0.01 in quanto il *p-value* < 0.0001, delineando una significatività statistica accettabile ad un livello di confidenza sia del 95% che del 99%. Viene quindi rifiutata l'ipotesi nulla.
Il coefficiente di regressione della *perceived compatibility* è pari a 0.39, ciò significa che all'aumentare di una unità della variabile indipendente, varierà il beneficio percepito esattamente di +0.39. Il coefficiente di determinazione *R-squared* del modello risulta di 0.13; questo modello di regressione è quindi in grado di spiegare il 13% della varianza dei *perceived benefits* sull'intero campione.

> ***H2.*** *La complementarità percepita ha un effetto positivo sui benefici percepiti dall'utilizzo di servizi Iot.*

L'ipotesi formulata sulla complementarità percepita risulta essere validabile, in quanto la *t* statistica della variabile *perceived complementarity* risulta pari a 14.20 per il totale del campione misurato (Appendice 2). La probabilità associata è inferiore a 0.01 in quanto il *p-value* < 0.0001, delineando una significatività statistica accettabile ad un livello di confidenza sia del 95% che del 99%. Viene quindi rifiutata l'ipotesi nulla.
Il coefficiente di regressione della *perceived complementarity* è pari a 0.52, ciò significa che all'aumentare di una unità della variabile indipendente, varierà il beneficio percepito esattamente di +0.52. Il coefficiente di determinazione *R-squared* del modello risulta di 0.43; questo modello di regressione è quindi in grado di spiegare il 43% della varianza dei *perceived benefits* sull'intero campione.

> ***H3a.*** *I benefici percepiti dei servizi IoT avranno un effetto positivo sull'intenzione all'adozione di servizi IoT*
> ***H3b.*** *I benefici percepiti dei servizi IoT avranno un effetto positivo sull'atteggiamento verso l'adozione dei servizi IoT.*

Per testare queste due ipotesi sono state utilizzate due regressioni lineare semplice utile a testare, nella prima ipotesi il *main effect* della variabile *perceived benefits* su *adoption to healthcare IoT system*, mentre nella seconda veniva misurato l'effetto dei benefici percepiti sull'*attitude*. Per quel che riguarda l'ipotesi *H3a*, questa è risultata essere soddisfacente, in quanto la *t* statistica della variabile *perceived benefits* è risultata essere uguale a 10.16 (Appendice 3). La probabilità associata è inferiore a 0.01 in quanto il *p-value* < 0.0001, evidenziando una significatività statistica accettabile per intervalli di confidenza pari a 95% e 99%. Si rifiuta quindi, l'ipotesi nulla. Il coefficiente di regressione della variabile è pari a 0.64, questo equivale a dire che all'aumentare di una unità di questa, l'adozione dei sistemi IoT aumenterà di +0.64. Il coefficiente di determinazione *R-squared* del modello risulta essere uguale a 0.28; questo modello di regressione è in grado di spiegare il 28% della varianza dell'adozione dei sistemi IoT. Anche per l'ipotesi *H3b* la regressione ci ha permesso di analizzare l'effetto dei *perceived benefits* sull'*attitude*. Il modello risulta essere significativo, la *t statistica* risulta essere uguale a 10.53 e la probabilità associata è inferiore a 0.01 in quanto il *p-value* < 0.0001, evidenziando una significatività statistica accettabile per intervalli di confidenza pari a 95% e 99% (Appendice 4). Si rifiuta quindi, l'ipotesi nulla. Il coefficiente di regressione della variabile è pari a 0.64, questo equivale a dire che all'aumentare di una unità di questa, l'adozione dei sistemi IoT aumenterà di +0.64. Il coefficiente di determinazione *R-squared* del modello risulta essere uguale a 0.29; questo modello di regressione è in grado di spiegare il 2% della varianza dell'atteggiamento dei rispondenti.

> ***H4a.*** *La preoccupazione per la privacy delle informazioni dei servizi IoT avrà un effetto negativo sull'intenzione all'adozione verso tali servizi*
> ***H4b.*** *La preoccupazione per la privacy delle informazioni dei servizi IoT avrà un effetto negativo sull'atteggiamento verso l'utilizzo di tali servizi*

Anche in questo caso le ipotesi sono state testate tramite l'ausilio di regressioni semplici. L'ipotesi *H4a* risulta essere non significativa a livello statistico. Questo perché l'intero modello non risulta essere statisticamente significativo (Prob > F = 0.3487), ciò non ci permette quindi di verificare l'esistenza del *main effect* della CFIP sull'adozione dei servizi IoT. *H4b* non è risultata essere significativa né a livello di coefficiente né a livello di modello. La *t* statistica della variabile *CFIP* è risultata essere uguale a 1.39 (Appendice 5). La probabilità associata è superiore a 0.05 in quanto il *p-value* > 0.05. Per via di questi risultati non è possibile evidenziare alcuna significatività statistica accettabile per un intervallo di confidenza pari a 95%. Si accetta quindi, l'ipotesi nulla. Pertanto, non è possibile asserire l'esistenza di alcuna relazione lineare tra la variabile *CFIP* e l'atteggiamento dei consumatori verso l'adozione dei sistemi IoT (Appendice 6).

> ***H5a.*** *L'atteggiamento verso l'utilizzo dei servizi IoT avrà un effetto positivo sull'adozione di servizi IoT.*
> ***H5b****. I benefici percepiti avranno un effetto positivo sull'atteggiamento verso ed adozione dei servizi IoT in ambito medico-sanitario.*

***H5c**. La preoccupazione per la privacy delle informazioni dei servizi IoT avrà un effetto negativo sull'atteggiamento verso l'utilizzo ed adozione dei servizi IoT in ambito medico-sanitario.*

Per verificare l'insieme di ipotesi *H5* è risultato opportuno servirsi di una regressione semplice, che andrà a misurare in maniera specifica l'ipotesi *H5a*, e due regressioni multiple per misurare le ipotesi *H5b* e *H5c*. L'ipotesi *H5a* riguarda il *main effect* dell'atteggiamento verso la variabile dipendente adozione dei sistemi IoT. La *t* statistica della variabile *attitude* è risultata essere uguale a 11.58 (Appendice 7), mentre la probabilità associata è inferiore a 0.01 in quanto il *p-value* < 0.0001, mostrando così una significatività statistica accettabile sia per intervalli di confidenza del 95% sia del 99%. Si rifiuta quindi, l'ipotesi nulla. Il coefficiente di regressione della variabile è uguale a 0.61, il che significa che all'aumentare di una unità della variabile *attitude*, l'adozione dei sistemi IoT aumenterà di +0.61. Il coefficiente di determinazione *R-squared* del modello è uguale a 0.33, il che equivale a dire che il modello è in grado di spiegare il 33% della varianza dell'adozione dei sistemi IoT.

Per testare le seguenti due ipotesi sono stati utilizzati modelli di regressione multipla, in grado di analizzare gli effetti congiunti delle variabili indipendenti sull'adozione dei sistemi IoT da parte dei rispondenti. Per quanto riguarda l'ipotesi *H5b*, le analisi condotte cercano di verificare l'esistenza di un effetto congiunto positivo tra le variabili *perceived benefits* ed *attitude* sull'*adoption to healtchare IoT systems*. Il modello presenta una probabilità dello 0.00001 tale da poter sostenere una rilevanza statistica dello stesso. Inoltre, l'*R-squared* risulta è tale da spiegare il 41% della varianza dell'adozione dei sistemi IoT. Per andare a testare l'ipotesi *H5b* inoltre, sono stati analizzati i singoli regressori all'interno del modello, ossia i *perceived benefits* e l'*attitude*. Il modello presenta quindi per la variabile *perceived benefits* una *t* statistica pari a 5.58 ed un *p-value* < 0.0001; il coefficiente di regressione assume valore pari a 0.38. La variabile *attitude* presenta anch'essa risultati positivi, con una *t* statistica del 7.18 ed un *p-value* <0.0001; il coefficiente di regressione assume valore pari a 0.41. Questi dati consentono quindi di rifiutare l'ipotesi nulla ad un livello di confidenza sia del 95% che del 99%, supportando così l'ipotesi di ricerca *H5b*. Inoltre, è stata condotta una verifica sulla multicollinearità, essendo questa una regressione multipla. Non sussiste alcun problema di questo tipo in quanto il VIF del modello è risultato essere ben inferiore alla soglia massima consentita di 10 (Appendice 8). Il discorso si articola maggiormente per la verifica dell'ipotesi *H5c*. Questa verificava la presenza di un effetto congiunto negativo della *CFIP* e positivo dell'*attitude* verso l'*adoption to healthcare IoT systems*. Il modello presenta una probabilità dello 0.00001 tale da poter sostenere una rilevanza statistica dello stesso. Inoltre, l'*R-squared* è tale da spiegare il 34% della varianza dell'adozione dei sistemi IoT. Per andare a testare l'ipotesi *H5c* inoltre, sono stati analizzati i singoli regressori all'interno del modello, ossia la *CFIP* e l'*attitude*. Il modello presenta quindi per la variabile *CFIP* una *t* statistica pari a -2.12 ed un *p-value* < 0.035 che definisce la variabile come marginalmente significativa; il coefficiente di regressione assume valore pari a -0.19. La variabile *attitude* presenta risultati positivi, con una *t* statistica del 11.71 ed un *p-value* < 0.0001; il coefficiente di regressione assume valore pari a 0.62. Questi dati consentono quindi di rifiutare l'ipotesi nulla ad un livello

di confidenza sia del 95% che del 99%, supportando così l'ipotesi di ricerca *H5c*. Inoltre, è stata condotta una verifica sulla multicollinearità, essendo questa una regressione multipla. Non sussiste alcun problema di questo tipo in quanto il VIF del modello è risultato essere ben inferiore alla soglia massima consentita di 10. (Appendice 9)

> ***H6a.*** *L'esposizione alla reward di servizio ha un effetto positivo sui benefici percepiti dall'utilizzo di servizi IoT.*
> ***H6b.*** *L'esposizione alla reward di servizio ha un effetto positivo sull'atteggiamento verso l'utilizzo di servizi IoT.*
> ***H6c.*** *L'esposizione alla reward di servizio ha un effetto positivo sulla concessione alle informazioni personali derivante derivanti dall'utilizzo di servizi IoT.*

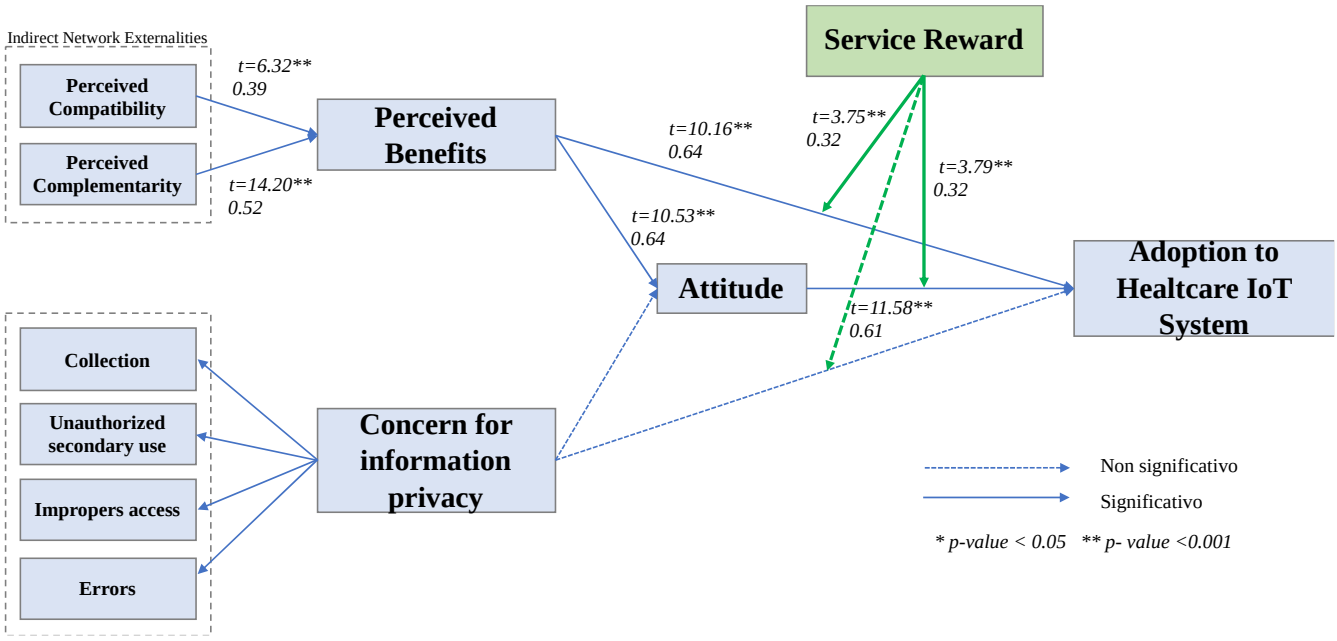
L'ultimo insieme di ipotesi, quelle appartenenti ai rami H6, risultano essere le più interessanti ai fini dello studio. Infatti, queste ipotesi sono quelle contenenti l'effetto di moderazione la cui interazione verrà verificata rispettivamente sul *main effect* dei *percieved benefits* (*H6a*), sul *main effect* dell'*attitude* (*H6b*) e sul *main effect* della *CFIP* (*H6c*) verso la variabile dipendente *adoption to healthcare IoT services*. Essendo la variabile moderatrice *service reward* configurata come una variabile dummy occorre puntualizzare che gli effetti che verranno misurati, andranno ad impattare solo sulla parte del campione che è stato esposto a questa variabile. Per quel che concerne la parte del modello in cui la moderazione viene misurata su *perceived benefits* verso la variabile dipendente (*H6a*) si può asserire che il modello risulta essere significativo con una probabilità dello 0.00001 tale da poter sostenere la rilevanza statistica dello stesso. L'*R-squared* ha ottenuto un punteggio tale da essere in grado di spiegare il 32% della varianza. Per poter testare l'ipotesi *H6a* e misurane gli effetti, sono stati presi in considerazione i singoli regressori all'interno del modello, ossia i *perceived benefits* ed il moderatore *service reward*. I benefici percepiti hanno ottenuto una *t* statistica pari a 10.48 ed un *p-value* < 0.0001; il coefficiente di regressione assume valore uguale a 0.38. La variabile *mod* (rappresentativa della *service reward*) ottiene una *t* statistica pari a 3.75 con un *p-value* < 0.0001; il coefficiente di regressione assume valore 0.32. L'analisi condotta sulla multicollinearità rivela l'assenza di alcun tipo di ridondanza tra le variabili utilizzati in quanto il VIF ottenuto è risultato essere uguale ad 1.0, valore ben lontano dalla soglia massima accettabile di 10. Questi dati consentono di rifiutare l'ipotesi nulla confermando quella alternativa definendo stabilito un rapporto tale per cui la variabile moderatrice influisce positivamente sui benefici percepiti dal rispondente aumentandone quindi la propensione all'adozione dei sistemi IoT in ambito sanitario. Questo risulta maggiormente evidente se si confrontano i risultati ottenuti (Appendice 10) con quelli conseguiti nella regressione in cui la variabile moderatrice non era presente (Appendice 3).

Si analizza adesso il frammento di modello in cui la moderazione agisce sull'*attitude* verso la variabile dipendente (*H6b*). Il modello risulta essere significativo con una probabilità dello 0.00001 tale da poter sostenere la rilevanza statistica dello stesso. L'*R-squared* ha ottenuto un punteggio tale da essere in grado di spiegare il 37% della varianza. Per poter testare l'ipotesi *H6b* e misurane gli effetti, sono stati presi in

considerazione i singoli regressori all'interno del modello, ossia l'*attitude* ed il moderatore *service reward*. L'atteggiamento ha ottenuto una *t* statistica pari a 11.93 ed un *p-value* < 0.0001; il coefficiente di regressione assume valore uguale a 0.61. La variabile *mod* (rappresentativa della *service reward*) ottiene una *t* statistica pari a 3.79 con un *p-value* < 0.0001; il coefficiente di regressione assume valore 0.32 (valori quasi identici al modello precedentemente misurato (Appendice 10). L'analisi condotta sulla multicollinearità rivela l'assenza di alcun tipo di ridondanza tra le variabili utilizzati in quanto il VIF ottenuto è risultato essere uguale ad 1.0, valore ben lontano dalla soglia massima accettabile di 10. Questi dati consentono di rifiutare l'ipotesi nulla confermando quella alternativa definendo stabilito un rapporto tale per cui la variabile moderatrice influisce positivamente sull'atteggiamento dell rispondente aumentandone quindi la propensione all'adozione dei sistemi IoT in ambito sanitario. Questo risulta maggiormente evidente se si confrontano i risultati ottenuti (Appendice 11) con quelli conseguiti nella regressione in cui la variabile moderatrice non era presente (Appendice 7). Infine, si verifica l'ipotesi in cui la moderazione agisce sulla *CFIP* verso la variabile dipendente (*H6c*). Il modello risulta essere significativo con una probabilità dello 0.007 tale da poter sostenere la rilevanza statistica dello stesso. L'*R-squared* ha ottenuto un punteggio tale da essere in grado di spiegare il 3% della varianza. Per poter testare l'ipotesi *H6c* e misurane gli effetti, sono stati presi in considerazione i singoli regressori all'interno del modello, ossia la *CFIP* ed il moderatore *service reward*. La *CFIP* ha ottenuto una *t* statistica pari a -1 ed un *p-value* > 0.05, questo implica che purtroppo il regressore non risulta essere statisticamente significativo. La variabile *mod* (rappresentativa della *service reward*) ottiene una *t* statistica pari a 3.03 con un *p-value* < 0.005; il coefficiente di regressione assume valore 0.32. L'analisi condotta sulla multicollinearità rivela l'assenza di alcun tipo di ridondanza tra le variabili utilizzati in quanto il VIF ottenuto è risultato essere uguale ad 1.0, valore ben lontano dalla soglia massima accettabile di 10 (Appendice 12). Questi dati non consentono di rifiutare l'ipotesi nulla, pertanto non è possibile stabilire alcun effetto di moderazione sulla variabile *CFIP*. Riassumendo le analisi condotte, 4 delle 12 ipotesi non sono state confermate, per la precisione tutte le ipotesi riguardanti la *CFIP* (*H4a, H4b, H5c, H6c*). Per maggiore chiarezza di seguito viene presentata una tabella contente tutte le relazioni ipotizzate con i rispettivi indicatori utili a comprenderne la loro significatività statistica.

Ipotesi di ricerca		**t1**	**t2**	**Coeff**	**Coeff 2**	**Risultato**
H1:	*Pc -> Pb*	6.32		0.63		Confermato
H2:	*Py -> Pb*	14.20		0.52		Confermato
H3a:	*Pb -> Adopt*	10.16		0.64		Confermato
H3b:	*Pb -> Att*	10.53		0.64		Confermato
H4a:	*CFIP-> Adopt*	-0.94		-0.10		Non Confermato
H4b	*CFIP -> Att*	1.39		0.14		Non Confermato
H5a:	*Att -> Adopt*	11.58		0.61		Confermato
H5b:	*Pb + Att -> Adopt*	5.58	7.18	0.38	0.42	Confermato
H5c:	*CFIP + att -> Adopt*	-2.12	11.71	-0.19	0.62	Non Confermato
H6a:	*Pb + mod -> Adopt*	10.48	3.75	0.65	0.32	Confermato
H6b:	*CFIP + mod -> Adopt*	-1	3.03	-0.1	0.32	Non Confermato
H6c:	*Att + mod -> Adopt*	11.93	3.79	0.61	0.32	Confermato

Grazie ai risultati ottenuti è adesso possibile disegnare un nuovo *framework* di riferimento rispetto a quello di partenza, contenente i dati inerenti alle interazioni con moderazione e senza, evidenziandone le relazioni significative e non.



Lungo le linee che stabiliscono le relazioni tra le variabili sono stati inseriti i valori statistici delle *t* con il livello di significatività associato (un asterisco per quelle confermate al 95% e due asterischi per quelle al 99%), oltre al coefficiente di regressione. Una volta testate tutte le ipotesi proposte ha senso interrogarsi su quali siano le principali differenze sulla base dei dati raccolti tra gli utenti esposti alla moderazione *service reward* e non.

3.6 – Discussioni ed implicazioni manageriali

Giunti alla fine dello studio procediamo con un'analisi complessiva dei risultati ottenuti, sia da un lato prettamente empirico sia da quello economico-manageriale. L'intenzione di questa sezione è pertanto quella di andare a capire cosa si cela oltre il semplice numero, quello che è comunemente noto come *insight*. Verranno brevemente riproposti gli obbiettivi dello studio e si cercherà di dare, attraverso i dati empirici ottenuti, un significato non solo teorico ma anche realmente applicabile alle dinamiche di mercato. Delle 12 ipotesi formulate, 4 non sono state confermate, tutte riguardanti il ramo inerente alla privacy. Con grande rammarico per questo risultato, non sarà possibile generare alcun tipo di implicazione che riguardi la parte sulla privacy, tanto meno il paradosso della privacy. In linea di massima però, possiamo ritenerci sufficientemente soddisfatti della parte restante del modello studiato. Questo è dovuto al fatto che le altre ipotesi sono state confermate con risultati, in termini di significatività dei modelli, eccellenti. In alcuni casi si è arrivati a registrare dei valori per gli *R-squared* che rasentano il 50%, risultato da ritenersi di spessore statistico. Partendo dal modello originale l'introduzione della variabile moderatrice *service reward* è stata accolta in maniera positiva: 2 delle 3 ipotesi che la riguardavano sono state confermate e l'unica a non esserlo riguardava la privacy. La causa per

cui questa non è stata confermata non è da imputarsi al moderatore, che altrimenti non avrebbe funzionato neanche per le altre ipotesi, ma alla mancanza di significatività del *main effect* che andava a moderare. Dopo questo appunto sulla variabile inserita si vuole procedere con ordine andando a commentare le ipotesi alla base del modello. In primis ci interfacciamo con le esternalità di rete indirette composte dalla *perceived compatibility* (*H1*) e *perceived complementarity* (*H2*). Questo blocco delle esternalità di rete non era stato volutamente escluso in quanto risultava essere uno degli aspetti che il modello originale aveva evidenziato come estremamente rilevante per l'influenza esercitata sui benefici percepiti. Per lo studio condotto, le domande utili alla misurazione dei costrutti erano state modificate ad *hoc*, quindi indirizzate a sottintendere una compatibilità e complementarità di servizi IoT a livello medico-sanitario. In base ai risultati conseguiti è possibile affermare che, anche per dispositivi in grado di impattare più o meno direttamente la salute di un utente, la compatibilità e la complementarità dei servizi IoT sono risultati essere elementi molto importanti ai fini dell'aumento dei benefici percepiti. (Appendice 1-2)

Sulla stessa verticale nel modello incontriamo le variabili che andranno a comporre la variabile CFIP "*Concern For Information privacy"*, queste sono: *collection, unauthorized secondary use, improper access* e *errors.* Per quanto riguarda queste variabili non sono state formulate ipotesi per via del fatto che la costruzione della CFIP attraverso queste variabili risultava essere molto complessa e diversa da qualsiasi altra variabile sin ora studiata; costruzione che di fatto non siamo riusciti a replicare, tematica che verrà approfondita nella sezione seguente 3.7.

Entriamo finalmente nel vivo della ricerca andando a verificare i *main effect* delle variabili *perceived benefits* (*H3a*) e *CFIP* (*H4a*) verso la variabile dipendente *Adoption to Healthcare system* ma anche dell'effetto di mediazione condotto dalla variabile *attitude (H5/a/b/c*), il tutto letto in un'ottima pre e post moderazione. La variabile dei benefici percepiti ha risposto in maniera coerente con quanto ci si aspettasse. Oltre ad essere risultata significativa all'interno del modello, ha dimostrato possedere un effetto positivo sull'adozione dei sistemi IoT sanitari da parte dei consumatori (Appendice 3). Questo effetto si è dimostrato ancora più accentuato a seguito dell'introduzione del moderatore. Infatti, confrontando i beta di regressione del modello senza moderatore con quelli del modello moderato si può notare come la variabile *service reward* sia stata in grado di aumentare la propensione all'adozione dei servizi IoT in ambito sanitario dei rispondenti (Appendice 10). Questo significa che chi è stato esposto ad uno stimolo informativo maggiore ha risposto positivamente ad esso. Ricordiamo che la variabile moderatrice consisteva sostanzialmente in un'immagine di tipo informativo, con lo scopo di far immedesimare il rispondente in una situazione quanto più realistica e a lui familiare possibile. Visti i risultati si può supporre che quindi una maggiore conoscenza del servizio IoT sanitario possa effettivamente garantire una maggiore propensione all'adozione di questi servizi. La variabile *CFIP*, creata tramite un'analisi fattoriale sulle 4 variabili della privacy del modello, nonostante abbia conseguito ottimi risultati in fase di pre-test, non è risultata essere significativa verso *adoption healthcare IoT system* (Appendice 5). Questo significa che è stato impossibile verificarne alcun tipo di relazione tra la variabile indipendente e quella dipendente (*H4a*). In tal caso non siamo in grado di compiere nessuna

assunzione in merito. Ovviamente, data la circostanza, perdiamo anche l'ipotesi moderatrice (*H6c)* andando essa ad agire su una relazione, di fatto, inesistente (Appendice 12). Prima di verificare l'effetto che la variabile *attitude* ha in via esclusiva sulla variabile dipendente (*H5a*) ci occuperemo di commentare le relazioni che questa ha con i benefici percepiti (*H3b*) e la CFIP (*H4b*). Per quel che riguarda la relazione tra *perceived benefits* ed *attitude* possiamo dire che l'ipotesi viene confermata e che quindi la percezione positiva di un servizio IoT di tipo medico si riflette in un aumento dell'atteggiamento che l'utilizzatore ha verso il dispositivo (Appendice 4). Questo risulta essere abbastanza plausibile anche a livello logico, in quanto una maggiore utilità percepita è normale sfoci in un atteggiamento maggiormente positivo dell'utilizzatore verso il prodotto. Anche in questo caso non è stato possibile identificare alcuna relazione statistica significativa tra la variabile *CFIP* ed *attitude* (*H4b*) (Appendice 6). Vista anche la mancata relazione tra queste due variabili risulta inutile soffermarsi sull'ipotesi che vedeva coinvolte la *CFIP* e l'*attitude* in maniera congiunta sull'adozione dei sistemi IoT sanitari (*H5c*), decisione che risulta essere confermata anche dai dati (Appendice 9). Verifichiamo adesso l'effetto della variabile *attitude* direttamente sulla variabile dipendente (*H5a*). Questa è risultata essere confermata dai dati in maniera significativa (Appendice 7). Possiamo quindi asserire che un atteggiamento positivo verso i dispositivi IoT da parte del consumatore è in grado veicolarlo in maniera più efficace verso l'adozione dei servizi. Se confrontiamo i risultati dell'ipotesi appena citata con quelli dell'ipotesi affetta da moderazione (*H6b*) potremo notare come i risultati ottenuti differiscano (Appendice 11). Come era accaduto per la moderazione sul *main effect* "benefici vs adozione" lo stesso si verifica in questa circostanza. Infatti, l'atteggiamento subisce un sostanziale aumento dovuto all'effetto della *service reward*. In questo caso però l'implicazione che ci si sente di fornire non riguarda più solamente l'aumento di utilità percepita dovuta ad una immedesimazione del rispondente in una circostanza ben definita, ma, trattandosi dell'atteggiamento, si potrebbe essere portati a pensare che l'effetto positivo scaturito derivi dalla capacità di comprensione del messaggio grazie alla sua chiarezza ed immediatezza. L'effetto congiunto generato dai *percieved benefits* e *attitude* verso *adoption to healthcare IoT system* è risultato essere significativo è complessivamente positivo. In breve, si è potuto vedere come l'effetto combinato di queste variabili sia in grado di aumentare significativamente l'adozione dei sistemi IoT (Appendice 8). Si può quindi suppore che i benefici percepiti risultano giocare un ruolo chiave in quanto influenzano, seppure in parte, l'atteggiamento il quale dimostra avere (se preso singolarmente) un coefficiente beta minore rispetto a quello dei benefici sulla variabile dipendente ma anche un *R-squared* maggiore e quindi maggiormente esplicativo della varianza di essa (Appendice 3 vs Appendice 7).

Dopo aver riassunto i risultati con qualche spunto di riflessione, si cercherà di realizzare una visione d'insieme degli elementi, sperando di fornire qualche assunzione di tipo manageriale che possa essere utile nel concreto. Nonostante uno degli obbiettivi principali di questa ricerca non sia stato confermato, ossia la dimostrazione che una *reward* di servizio potesse essere in grado di attenuare l'effetto di rifiuto all'adozione di sistemi IoT a causa dell'eccessiva raccolta di dati, siamo comunque in grado di portare un modello che potenzialmente può ancora dirci qualcosa. Se dividiamo il *framework* di riferimento sull'asse orizzontale potremo analizzarlo

in due emisferi, quello superiore, ipotesi confermate, e quello inferiore, ipotesi non confermate. Per questo motivo saremo in grado di analizzare solo la parte superiore. Cercando di inquadrare i risultati ottenuti in un'ottica più generale possibile, possiamo dire che abbiamo individuato un nuovo elemento in grado di favorire l'adozione ai sistemi IoT. Sostanzialmente il modello non è altro che un piccolo frammento della fase definibile come *attraction* all'interno della *customer journey*. Per dirla semplicemente, partendo dal modello di Hsu & Lin 2016, abbiamo studiato quali elementi un servizio IoT deve avere o garantire affinchè questo venga "adottato". Per usare un sinonimo un po' più tecnico si potrebbe dire che questo *framework* mette in mostra come potrebbe essere possibile favorire il *first trial* di un dispositivo IoT dedicato ai servizi medici sanitari da parte di un consumatore. Questo era quello che il modello di base già era in grado di dire. Quello che siamo riusciti ad aggiungere con il nostro moderatore è un tassello che precedentemente non era stato considerato: l'esposizione informativa chiara e immediata. Ricordando nuovamente che il moderatore inserito si configurava come un'immagine a scopo informativo, ne sono stati successivamente misurati gli effetti, che oltre ad esser risultati significativamente statistici hanno messo in mostra come questo tipo di variabile generi un effetto positivo sull'adozione dei sistemi IoT. L'informazione finale che si evince, in un'ottica imprenditoriale, potrebbe riguardare i seguenti aspetti.

Al fine di favorire l'adozione dei servizi IoT nonché il *first trial* e di conseguenza le vendite, il dispositivo/prodotto deve essere compatibile, rispecchiando ciò che il consumatore vuole, risultato ottenibile grazie ad un alto livello di personalizzazione, ma anche complementare, ovvero dispositivi in grado di comunicare tra di loro, abbattendo le eventuali barriere dovute a sistemi operativi diversi. La componente utilitaristica risulta essere fondamentale ed anche la formazione di un atteggiamento da parte del consumatore gioca un ruolo cruciale. Essendo queste due caratteristiche elementi non prettamente tecnici, ossia che non si possono aumentare o decidere in maniera operativa durante il processo in filiera produttiva (e ci si riferisce in particolar modo alla formazione dell'atteggiamento del consumatore verso un prodotto/servizio), ecco che risulta cruciale la variabile *service reward*. Questa potrebbe effettivamente diventare un elemento importante tramite il quale formare l'atteggiamento dei consumatori verso un prodotto. Quindi attraverso l'esposizione informativa del servizio ed una comunicazione chiara e immediata si può andare a pensare di intaccare in maniera importante la fase di *attraction* dei consumatori.

3.7 – Limiti della ricerca e prospettive future

Il limite principale di questa ricerca riguarda il non esser stati in grado di confermare le ipotesi sulla privacy andando a perdere una parte corposa dello studio. La motivazione principale è da ricercarsi nella creazione della variabile CFIP. Questa è stata definita come una variabile autoriflessiva di secondo ordine, mentre in questo studio è stata generata semplicemente attraverso un'analisi multifattoriale inclusiva delle variabili *collection, unauthorized secondary use, improper access, errors*. Purtroppo, nonostante la fase di pre-test con le alpha di Cronbach dimostrassero una buona *reliability*, questa non è stata sufficiente a far si che la variabile risultasse significativa nel modello per nessuna delle ipotesi formulate (*H4a, H4b, H5c*). Sicuramente uno

spunto per eventuali ricerche future riguarda proprio il prestare maggiore attenzione alla costruzione di questo costrutto, che se ben generato, può effettivamente dare un grande contributo alle implicazioni finali offerte dalla ricerca. Per quando riguarda invece l'evoluzione del modello proponiamo due possibili strade:

- continuare l'arricchimento del *framework* attraverso nuove variabili e cercando di rendere sempre più completo il mosaico che porta all'adozione di sistemi IoT in ambito sanitario.
- Andare oltre lo step dell'*attraction* concentrandosi sulla fase di retention, ossia studiare quali meccanismi siano in grado di far mantenere costante nel tempo l'utilizzo di dispositivi IoT.

La prima strada aiuterebbe lo studio del fenomeno e, se fatta a distanza di anni, a fattori costanti, potrebbe permettere di capire come i bisogni dei consumatori si evolvano nel tempo. La seconda invece, consentirebbe di ottenere, infine, una visione continua del consumatore, intesa come un percorso che si articola nelle fasi basilari di *attraction*, *retention* ed *evolution*.

APPENDICE

Appendice 1

```
. regress pb pc
```

Source	SS	df	MS	Number of obs	=	263
				F(1, 261)	=	39.99
Model	17.2797582	1	17.2797582	Prob > F	=	0.0000
Residual	112.770428	261	.432070606	R-squared	=	0.1329
				Adj R-squared	=	0.1295
Total	130.050186	262	.496374757	Root MSE	=	.65732

pb	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
pc	.3988374	.0630673	6.32	0.000	.2746518	.5230229
_cons	2.135706	.236725	9.02	0.000	1.669572	2.60184

Appendice 2

```
. regress pb py
```

Source	SS	df	MS	Number of obs	=	267
				F(1, 265)	=	201.70
Model	57.3644773	1	57.3644773	Prob > F	=	0.0000
Residual	75.3663056	265	.284401153	R-squared	=	0.4322
				Adj R-squared	=	0.4300
Total	132.730783	266	.498987906	Root MSE	=	.53329

pb	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
py	.5281707	.0371893	14.20	0.000	.4549465	.6013948
_cons	1.886691	.1263488	14.93	0.000	1.637915	2.135466

Appendice 3

```
. regress adopt pb
```

Source	SS	df	MS	Number of obs	=	261
				F(1, 259)	=	103.17
Model	54.4591617	1	54.4591617	Prob > F	=	0.0000
Residual	136.713257	259	.527850412	R-squared	=	0.2849
				Adj R-squared	=	0.2821
Total	191.172418	260	.735278532	Root MSE	=	.72653

adopt	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
pb	.6492769	.0639219	10.16	0.000	.5234041	.7751498
_cons	1.24702	.2353855	5.30	0.000	.7835066	1.710533

Appendice 4

```
. regress att pb
```

Source	SS	df	MS	Number of obs	=	261
				F(1, 259)	=	110.91
Model	53.766601	1	53.766601	Prob > F	=	0.0000
Residual	125.554813	259	.484767618	R-squared	=	0.2998
				Adj R-squared	=	0.2971
Total	179.321414	260	.689697746	Root MSE	=	.69625

att	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
pb	.6427818	.0610343	10.53	0.000	.5225951	.7629684
_cons	1.28356	.2248741	5.71	0.000	.840746	1.726375

Appendice 5

```
. regress adopt CFIP
```

Source	SS	df	MS	Number of obs	=	265
				F(1, 263)	=	0.88
Model	.673021005	1	.673021005	Prob > F	=	0.3487
Residual	200.836418	263	.763636568	R-squared	=	0.0033
				Adj R-squared	=	-0.0004
Total	201.509439	264	.763293328	Root MSE	=	.87386

adopt	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
CFIP	-.1038221	.1105908	-0.94	0.349	-.3215781	.1139339
_cons	3.774553	.1961032	19.25	0.000	3.388421	4.160685

Appendice 6

```
. regress att CFIP
```

Source	SS	df	MS	Number of obs	=	265
				F(1, 263)	=	1.92
Model	1.3080735	1	1.3080735	Prob > F	=	0.1665
Residual	178.765722	263	.679717573	R-squared	=	0.0073
				Adj R-squared	=	0.0035
Total	180.073795	264	.682097709	Root MSE	=	.82445

att	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
CFIP	.1445804	.1042215	1.39	0.167	-.0606345	.3497952
_cons	3.360567	.1851003	18.16	0.000	2.9961	3.725034

Appendice 7

```
. regress adopt att
```

Source	SS	df	MS	Number of obs	=	266
				F(1, 264)	=	134.15
Model	67.950318	1	67.950318	Prob > F	=	0.0000
Residual	133.72053	264	.50651716	R-squared	=	0.3369
				Adj R-squared	=	0.3344
Total	201.670848	265	.761022069	Root MSE	=	.7117

adopt	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
att	.6160832	.0531913	11.58	0.000	.51135	.7208163
_cons	1.3794	.1965409	7.02	0.000	.9924126	1.766387

Appendice 8

```
. regress adopt att pb
```

Source	SS	df	MS	Number of obs	=	260
				F(2, 257)	=	89.32
Model	78.24545	2	39.122725	Prob > F	=	0.0000
Residual	112.572931	257	.438026967	R-squared	=	0.4101
				Adj R-squared	=	0.4055
Total	190.818381	259	.736750504	Root MSE	=	.66184

adopt	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
att	.4247088	.0591261	7.18	0.000	.3082754	.5411421
pb	.3881134	.069545	5.58	0.000	.2511627	.525064
_cons	.6647255	.2283582	2.91	0.004	.2150341	1.114417

Appendice 9

```
. regress adopt CFIP att
```

Source	SS	df	MS	Number of obs	=	264
				F(2, 261)	=	69.25
Model	69.7387804	2	34.8693902	Prob > F	=	0.0000
Residual	131.412318	261	.503495473	R-squared	=	0.3467
				Adj R-squared	=	0.3417
Total	201.151099	263	.764833075	Root MSE	=	.70957

adopt	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
CFIP	-.1907013	.0901384	-2.12	0.035	-.3681924	-.0132101
att	.624515	.0533357	11.71	0.000	.5194919	.7295381
_cons	1.675509	.2403499	6.97	0.000	1.202238	2.148781

Appendice 10

```
. regress adopt pb mod
```

Source	SS	df	MS	Number of obs	=	261
				F(2, 258)	=	61.20
Model	61.5156865	2	30.7578432	Prob > F	=	0.0000
Residual	129.656732	258	.502545472	R-squared	=	0.3218
				Adj R-squared	=	0.3165
Total	191.172418	260	.735278532	Root MSE	=	.7089

adopt	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
pb	.6539866	.0623836	10.48	0.000	.5311407	.7768324
mod	.3290407	.0878096	3.75	0.000	.156126	.5019554
_cons	1.069889	.2344881	4.56	0.000	.6081343	1.531643

```
.
. vif
```

Variable	VIF	1/VIF
mod	1.00	0.999594
pb	1.00	0.999594
Mean VIF	1.00	

Appendice 11

```
. regress adopt CFIP mod
```

Source	SS	df	MS	Number of obs	=	265
				F(2, 262)	=	5.05
Model	7.47875169	2	3.73937585	Prob > F	=	0.0071
Residual	194.030687	262	.740575141	R-squared	=	0.0371
				Adj R-squared	=	0.0298
Total	201.509439	264	.763293328	Root MSE	=	.86057

adopt	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
CFIP	-.1087348	.1089201	-1.00	0.319	-.3232051	.1057354
mod	.3205499	.1057408	3.03	0.003	.1123398	.5287599
_cons	3.623262	.1994639	18.17	0.000	3.230506	4.016018

```
.
. vif
```

Variable	VIF	1/VIF
CFIP	1.00	0.999779
mod	1.00	0.999779
Mean VIF	1.00	

Appendice 12

```
. regress adopt att mod
```

Source	SS	df	MS	Number of obs	=	266
				F(2, 263)	=	77.66
Model	74.8793815	2	37.4396908	Prob > F	=	0.0000
Residual	126.791467	263	.482096832	R-squared	=	0.3713
				Adj R-squared	=	0.3665
Total	201.670848	265	.761022069	Root MSE	=	.69433

adopt	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
att	.6193893	.0519006	11.93	0.000	.5171958	.7215828
mod	.3228403	.0851565	3.79	0.000	.1551651	.4905155
_cons	1.206068	.1971199	6.12	0.000	.8179343	1.594203

```
.
. vif
```

Variable	VIF	1/VIF
att	1.00	0.999718
mod	1.00	0.999718
Mean VIF	1.00	

BIBLIOGRAFIA

Acquisti, A., 2004. *Privacy in electronic commerce and the economics of immediate gratification*. In: EC ’04 Proceedings of the 5th ACM Conference on Electronic Commerce, USA, 21-29.

Acquisti, A., Brandimarte, L., & Loewen- stein, G. (2015). *Privacy and human be- havior in the age of information*. *Science*, *347*(6221), 509-514.

Acquisti, A., Grossklags, J., 2005. *Privacy and rationality in individual decision makin*g. IEEE Secur. Priv. 3 (1), 26–33.Agarwal, R., Sambamurthy, V., Stair, R., 1997. Cognitive absorption and the adoption of new information technologies. In: Dosier, L., Keys, J. (Eds.), Academy of Management Best Paper Proceedings. Office of Publications and Faculty Research Services in the College of Business Administration, Georgia Southern University, Statesboro, pp. 293–297.

Aggarwal, R. and Lal Das, M. (2012) RFID Security in the Context of “Internet of Things”. *First International Confe- rence on Security of Internet of Things*, Kerala, 17-19 August 2012, 51-56.

Akar, E., & Topcu, B. (2011). An examina- tion of the factors influencing consumers’ attitudes toward social media marketing. *Journal of Internet Commerce*, *10*(1), 35-67.

Aloudat, A., Katina, M., Chen, X., & Al-Debei, M. M. (2014). Social acceptance of location-based mobile government services for emergency management. Tele- matics and Informatics, 31, 153e171.

Andersson, P., Mattsson, L.-G., 2015. Service innovations enabled by the “internet of things”. IMP J. 9, 85–106.

Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: the elaboration likelihood model and individual persuasion. MIS Quarterly, 33(2), 339e370.

Atzori, L., Iera, A., Morabito, G., 2010. The Internet of things: a survey. Comput. Netw. 54 (15), 2787–2805.

Baldini, G., Botterman, M., Neisse, R., Tallacchini, M., 2016. Ethical design in the internet of things. Sci. Eng. Ethics 1–21.

Bailey, D.A., 2012. Moving 2 mishap: M2M's impact on privacy and safety. IEEE Secur. Priv. 10 (1), 84–87.

Balmer, J. M., & Yen, D. A. (2017). The Internet of total corporate communica- tions, quaternary corporate communica- tions and the corporate marketing Inter- net revolution. *Journal of Marketing Man- agement*, *33*(1-2), 131-144.

Bandyopadhyay, S., Balamuralidhar, P., & Pal, A. (2013). Interoperation among IoT standards. Journal of ICT Standardization, 1, 253e270.

Bansal, G., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Deci- sion support systems*, *49*(2), 138-150.

Barnes, S.B., 2006. A privacy paradox: Social networking in the United States. First Monday, 11(9).

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic com- merce: the role of privacy, security, and site attributes. *The journal of strategic Infor- mation Systems*, *11*(3-4), 245-270.

Bickart, B., & Schindler, R. M. (2001). Inter- net forums as influential sources of con- sumer information. J*ournal of interactive marketing*, *15*(3), 31-40.

Biddlecombe, E. (2009) UN Predicts “Internet of Things”. Retrieved July 6.

Bradley, J., Barbier, J., Handler, D., 2013. Embracing the Internet of everything to capture your share of 14.4 trillion. CISCO

Bradley, T., Thibodeau, P., Ng, V., 2014. The internet of things – threats and challenges. In: NetworkWorld Asia. 11. pp. 16–18.

Braun, E., Wield, D., 1994. Regulation as a means for the social control of technology. Tech. Anal. Strat. Manag. 6 (3), 259–272.

Bremer, A., 2015. Diffusion of the "internet of things" on the world of skilled work and resulting consequences for the man-machine interaction. In: Empirical Research in Vocational Education and Training. 7.

Brill, J., 2014. The internet of things: building trust and maximizing benefits through consumer control. Fordham Law Rev. 83, 205–217.

Brody, P., Pureswaran, V., 2015. The next digital gold rush: how the internet of things will create liquid, transparent markets. Strateg. Leadersh. 43, 36–41.

Brown, B. (2001), Studying the internet experience. HP Laboratories Technical Report (HPL- 2001-49). Savre & Horne, 2000

Chui, M., Löffler, M., Roberts, R., 2010. The internet of things. McKinsey Q. 70–79.

Caron, X., Bosua, R., Maynard, S.B., Ahmad, A., 2016. The internet of things (IoT) and its impact on individual privacy: an Australian perspective. Comp. Law Sec. Rev. 32, 4–15.

Cheng,M.N.,Cheung,C.F.,Fung,S.H.&Tsang, K. K. (2014), “A hybrid roadmapping method for technology forecasting and assessment: A case study in an Information and Communication Technology Company”. In: Management of Engineer- ing Technology (PICMET), 2014 Portland International Conference on, pp. 2882-2890.

Caron, X., Bosua, R., Maynard, S.B., Ahmad, A., 2016. The internet of things (IoT) and its impact on individual privacy: an Australian perspective. Comp. Law Sec. Rev. 32, 4–15.

Carrascal, J. P., Riederer, C., Erramilli, V., Cherubini, M., & de Oliveira, R. (2013, May). Your browsing behavior for a big mac: Economics of personal information online. *In Proceedings of the 22nd interna- tional conference on World Wide Web* (pp. 189-200). ACM.

Castellani, A., Dissegna, M., Bui, N. & Zorzi, M. (2012), “WebIoT: A web application framework for the internet of things”. In: Wireless Communications and Networking Conference Workshops (WCNCW), 2012 IEEE, pp. 202-207.

Cazier, J. A., Jensen, A. S., & Dave, D. S. (2008). The Impact of consumer perceptions of information privacy and security risks on the adoption of residual RFID technologies. Communications of the Association for Information Systems, 23(1), 236e256.

Chen, K.C., 2012. Machine-to-machine communications for healthcare. JCSE 6 (2), 119–126.

Chiu, C. M., Cheng, H. L., Huang, H. Y., & Chen, C. F. (2013). Exploring individuals' subjective well-being and loyalty towards social network sites from the perspective of network externalities: the Facebook case. International Journal of Information Management, 33(3), 539e552.

Cooper, R. B., & Zmud, R. W. (1990). Information technology implementation research: a technological diffusion approach. Management Science, 36(2), 123e139.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An em- pirical investigation. *Organization science*, *10*(1), 104-115.

Damsgaard, J., & Truex, D. (2000). Binary trading relations and the limits of EDI standards: the Procrustean bed of standards. European Journal of Information Systems, 9(3), 173e188.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13, 319-340.

Del Giudice, M., 2016. Discovering the internet of things (IoT) within the business process management: a literature review on technological revitalization. Bus. Process. Manag. J. 22, 263–270.

Diffley, S., Kearns, J., Bennett, W., & Kawalek, P. (2011). Consumer behaviour in social networking sites: implications for marketers. *Irish Journal of Management*.

Dinev, T., & Hart, P. (2006). Internet privacy and social awareness as determinants of Intention to transact. International Journal of Electronic Commerce, 10(2), 7e29.

Dlodlo, N., Foko, T., Mvelase, P., Mathaba, S., 2012. The state of Affairs in internet of things research. Electron. J. Inform. Syst. Eval. 15, 244–258.

Dutton, W.H., 2014. Putting things to work: social and policy challenges for the internet of things. Info 16, 1–21.

Eastlick, M. A., Lotz, S. L., & Warring- ton, P. (2006). Understanding online B-to- C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research*, *59*(8), 877-886. Elmaghraby, A.S., Losavio, M.M., 2014. Cyber security challenges in smart cities: safety, security and privacy. J. Adv. Res. 5, 491–497.

Flender, C., Müller, G., 2012. Type indeterminacy in privacy decisions: the privacy paradox revisited. In: Busemeyer, J., Dubois, F., Lambert-Mogiliansky, A., Melucci, M. (Eds.), Quantum interaction. Lecture notes in Computer Science. Springer-Verlag, Berlin, Heidelberg, pp. 148–159. 7620.

Gandal, N. (1994). Hedonic price indexes for spreadsheets and an empirical test for network externalities. The RAND Journal of Economics, 25(1), 160e170.

Gerpott, T.J., May, S., 2016. Integration of internet of things components into a firm's offering portfolio – a business development framework. Info 18, 53–63.

Gilovich, T., Griffin, D., and Kahneman, D. (eds), (2002), Heuristics and biases: The psychology of intuitive judgment. Cambridge University Press

Giulio Xhaët, Il sole 24 ore, 2018. *Il paradosso della privacy, e quanto siamo disposti a pagare per averla*

Gretzel, U., Sigala, M., Xiang, Z., Koo, C., 2015. Smart tourism: foundations and devel- opments. Electron. Mark. 25, 179–188;

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): a vision, architectural elements, and future directions. Future Generation Com- puter Systems, 29(7), 1645e1660.

Guillemin, P., Friess, P., 2009. Internet of things strategic research roadmap. The cluster of European research projects. In: Technical report.

Gupta, S., & Mela, C. F. (2008). What is a free customer worth? Harvard Business Review, 86, 102e109.

Hann, I.H., Hui, K.L., Lee, S.Y.T., and Png, I. P. (2007), Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management*

Hardgrave, B. C., Davis, F. D., & Riemenschneider, C. K. (2003). Investigating de- terminants of software developers' intentions to follow methodologies. Journal of Management Information Systems, 20(1), 123-151.

Harris Interactive, Inc, & Westin, A. (2003). Commerce communication and Privacy online. Hackensack: Privacy and American Business.

Holvast, J. (1993), Vulnerability and Privacy: Are We on the Way to a Risk-Free Society? In: Proceedings of the IFIP-WG9.2 Conference, May 20–22, 1993, Namur, Belgium.

Hsu & Lin, (2016). An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives

Iimi, A. (2005). Estimating demand for cellular phone services in Japan. Telecom- munications Policy, 29, 3e23.Ives, B., Palese, B., Rodriguez, J.A., 2016. Enhancing customer service through the in- ternet of things and digital data streams. MIS Q. Exec. 15, 279–297.

Isaak, J., & Hanna, M. J. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer*, *51*(8), 56-59.

Istepanian,R.S.H.,Hu,S.,Philip,N.Y.&Sungoor, A. (2011), "The potential of Internet of m-health Things 'm-IoT' for non-invasive glucose level sensing". In: Engineering in Medicine and Biology Society, EMBC, 2011 Annual International Conference of the IEEE, pp. 5264-5266.

Istepanaian,R.S.H.&Zhang,Y.T.(2012),"Intro- duction to the Special Section: 4G Health-The Long- Term Evolution of m-Health", IEEE Transactions on Information Technology in Biomedicine 16(1), 1-5

Jara, A.J., Parra, M.C., Skarmeta, A.F., 2014. Participative marketing: extending social media marketing through the identification and interaction capabilities from the internet of things. Pers. Ubiquit. Comput. 18, 997–1011.

Jara,A.J.,Zamora,M.A.&Skarmeta,A.F.G.(2010), "An Architecture Based on Internet of Things to Support Mobility and Security in Medical Environ- ments". In: Consumer Communications and Network- ing Conference (CCNC), 2010 7th IEEE, pp. 1-5

Jiang, Z., Heng, C. S., & Choi, B. C. (2013). Research note privacy concerns and privacy-protective behavior in syn- chronous online social interactions. *Infor- mation Systems Research*, *24*(3), 579-595.

Joinson, A.N., Reips, U.-D., Buchanan, T., Paine Schofield, C.B., 2010. Privacy, trust, and self-disclosure online. Hum.-Comput. Interact. 25, 1–24.

Jung, S.J., Chung, W.Y., 2013. Wireless machine-to-machine healthcare solution using android mobile devices in global networks. IEEE Sensors J. 13, 1419–1424.

Katz, M. L., & Shapiro, C. (1985). Network externalities, competition, and compatibility. American Economic Review, 75, 424e440

Kim, S., Kim, S., 2016. A multi-criteria approach toward discovering killer IoT application in Korea. Technol. Forecast. Soc. Chang. 102, 143–155.

Kim, G. S., Park, S. B., & Oh, J. (2008). An examination of factors influencing consumer adoption of short message service (SMS). Psychology & Marketing, 25 769-786.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of cur- rent research on the privacy paradox phe- nomenon. *Computers & security*, *64*, 122- 134.

Korgaonkar, P. K., & Wolin, L. D. (1999). A multivariate analysis of web usage. *Journal of advertising research*, *39*(2), 53-53.

Korzaan, M. L., & Boswell, K. T. (2008). The Influence of personality traits and in- formation privacy concerns on behavioral intentions. The Journal of Computer Information Systems, 48(4), 15e24.

Kosmatos, E.A., Tselikas, N.D. and Boucouvalas, A.C. (2011) Integrating RFIDs and Smart Objects into a Unified In- ternet of Things Architecture. *Advances in Internet of Things*: *Scientific Research*, **1**, 5-12.

Krasnova, H., & Veltri, N. F. (2010, Jan- uary). Privacy calculus on social networking sites: Explorative evidence from Ger- many and USA. *In 2010 43rd Hawaii Inter- national Conference on System Sciences* (pp. 1-10). IEEE.

Kreps, D., Kimppa, K., 2015. Theorising web 3.0: ICTs in a changing society. Inf. Technol. People 28, 726–741.

Lee, I., Lee, K., 2015. The internet of things (IoT): applications, investments, and chal- lenges for enterprises. Bus. Horiz. 58, 431–440.

Lee, H., Park, H. and Kim, J. (2013), Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *International Journal of Human-Computer Studies*, **71**(9), 862-877

Li, S., Tryfonas, T., Li, H., 2016. The internet of things: a security point of view. Int. Res. 26, 337–359.

Lin, C. P., & Bhattacherjee, A. (2008). Elucidating individual intention to use inter- active information technologies: the role of network externalities. International Journal of Electronic Commerce, 13, 85e108.

Lin, C. P., & Bhattacherjee, A. (2009). Understanding online social support and its antecedents: a socio-cognitive model. The Social Science Journal, 46, 724e737.

Lin, C. P., Tsai, Y. H., Wang, Y. J., & Chiu, C. K. (2011). Modeling IT relationship quality and its determinants: a potential perspective of network externalities in e- service. Technological Forecasting & Social Change, 78(1), 171e184.

Lin, K. Y., & Lu, H. P. (2011). Why people use social networking sites: an empirical study integrating network externalities and motivation theory. Computers in Human Behavior, 27(3), 1152e1161.

Lou, H., Luo, W., & Strong, D. (June 2000). Perceived critical mass effect on group- ware acceptance: a revised technology acceptance model. European Journal of Information Systems, 9(2), 91e103.

Luo,X.,Liu,T.,Liu,J.,Guo,X.&Wang,G.(2012), "Design and implementation of a distributed fall detection system based on wireless sensor net- works", EURASIP Journal on Wireless Communica- tions and Networking 2012(1), 1-13.

Lustria, M. L. A., Cortese, J., Gerend, M. A., Schmitt, K., Kung, Y. M., & McLaugh- lin, C. (2016). A model of tailoring ef- fects: A randomized controlled trial ex- amining the mechanisms of tailoring in a web-based STD screening intervention. *Health Psychology*, *35*(11), 1214.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. Information Systems Research, 15(4), 336e355.

Man, L.C.K., Na, C.M., Kit, N.C., 2015. IoT-based asset management system for health- care-related industries. Int. J. Eng. Bus. Manag.

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*(2), 135-155.

Michele Iaselli, Stefano Gorla –ed. Lex et Ars-2015. "Storia della Privacy".

Miorandi, D., Sicari, S., De Pellegrini, F., Chlamtac, I., 2012. Internet of things: vision, applications and research challenges. Ad Hoc Netw. 10 (7), 1497–1516.

Monares, A., Ochoa, S. F., Santos, R., Orozco, J. & Meseguer, R. (2014), "Modeling IoT-Based Solu- tions Using Human-Centric Wireless Sensor Networks", Sensors 14(9), 15687-15713.

Mosteller, J., & Poddar, A. (2017). To share and protect: Using regulatory focus the- ory to examine the privacy paradox of consumers' social media engagement and online privacy protection behaviors. *Jour- nal of Interactive Marketing*, *39*, 27-38

Ng, V., 2014b. Drivers and Obstacles to IoT Adoption in Asia Pacific. 11. NetworkWorld Asia, pp. 12–14

Ng, I., Scharf, K., Pogrebna, G., Maull, R., 2015. Contextual variety, internet-of-things and the choice of tailoring over platform: mass customisation strategy in supply chain management. Int. J. Prod. Econ. 159, 76–87.

Nolin, J., Olson, N., 2016. The internet of things and convenience. Int. Res. 26, 360–376. O'Leary, D.E., 2013. 'Big data', the 'internet of things' and the 'internet of signs'. In: Intelligent Systems in Accounting, Finance and Management. 20. pp. 53–65.

Norberg, P.A., Horne, D.R., Horne, D.A., 2007. The privacy paradox: personal information disclosure intentions versus behaviors. J. Consum. Affairs 41 (1), 100–126.

Oomen, I., Leenes, I., 2008. Privacy risk perceptions and privacy protection strategies. In: de Leeuw, E., Fischer-Hübner, S., Tseng, J., Borking, J. (Eds.), Policies and Research in Identity Management. Springer Verlag, Boston, pp. 121–138.

Ortiz, A.M., Hussein, D., Park, S., Han, S.N., Crespi, N., 2014. The cluster between in- ternet of things and social networks: review and research challenges. IEEE Int. Things J. 1, 206–215.

Pae, J. H., & Hyun, J. S. (2002). The impact of technology advancement strategies on consumers' patronage decisions. Journal of Product Innovation Management, 19, 375e383.

Pang,Z.,Chen,Q.,Tian,J.,Zheng,L.&Dubrova,E. (2013), "Ecosystem analysis in the design of open platform-based in-home healthcare terminals towards the internet-of-things". In: Advanced Communication Technology (ICACT), 2013 15th International Conference on, pp. 529-534.

Parasuraman, A., & Zinkhan, G. M. (2002). Marketing to and serving cus- tomers through the Internet: An overview and research agenda. *Journal of the academy of marketing science*, *30*(4), 286-295.

Pisano, P., Pironti, M., Rieple, A., 2015. Identify innovative business models: can in- novative business models enable players to react to ongoing or unpredictable trends? Entrep. Res. J. 5, 181–199.

Popescul, D., Georgescu, M., 2013. Internet of things - some ethical issues. In: USV Annals of Economics & Public Administration. 13. pp. 208–214

Pötzsch, S., 2009. Privacy awareness: a means to solve the privacy paradox? In: Vashek, M., Fischer-Hübner, S., Cvrcˇek, D., Švenda, P. (Eds.), The Future of Identity in the Information Society. Springer-Verlag, Berlin Heidelberg, pp. 226–236.

Punji, G. (2018). Consumer intentions to falsify personal information online: un- ethical or justifiable?. *Journal of Marketing Management*, *33*(15-16), 1402-1412.

Quigley, M., Burke, M., 2013. Low-cost internet of things digital technology adoption in SMEs. Int. J. Manag. Pract. 6, 153–164.

Rainie, L., Kiesler, S., Kang, R., Madden, M., Duggan, M., Brown, S., & Dabbish, L. (2013). Anonymity, privacy, and security online. *Pew Research Center*, *5*.

Rau, P.-L.P., Huang, E., Mao, M., Gao, Q., Feng, C., Zhang, Y., 2015. Exploring interactive style and user experience design for social web of things of Chinese users: a case study in Beijing. Int. J. Hum. Comput. Stud. 80, 24–35.

Rogers, E. M. (1983). Diffusion of innovations (3rd ed.). New York: Free Press.

Rosenberg, R. (1992), The social impact of computers. Academic Press Inc

Santoro, G., Vrontis, D., Thrassou, A., Dezi, L., 2017. The internet of things: building a knowledge management system for open innovation and knowledge management capacity. Technol. Forecast. Soc. Chang(https://www.sciencedirect.com/science/ article/pii/S0040162517302846 Available online 16 March 2017 In Press).

Sabonienė, A., 2010. The contradictions of industrial policy in the context of economic integration. Econ. Manag. 2010 (15), 212–218.

Sebestyen, G., Hangan, A., Oniga, S. & Gal, Z. (2014), "eHealth solutions in the context of Internet of Things". In: Automation, Quality and Testing, Robotics, 2014 IEEE International Conference on, pp. 1-6.

Shahamabadi, M. S., Ali, B. M., Noordin, N. K., Rasid, M. F. B. A., Varahram, P. & Jara, A. J. (2014), "A NEMO-HWSN Solution to Support 6LoWPAN Network Mobility in Hospital Wireless Sensor Network", Computer Science and Information Sys- tems 11(3), 943-960.

Sheng, H., Nah, F. F.-H., & Siau, K. (2008). An experimental study on ubiquitous commerce adoption: impact of personalization and privacy concerns. Journal of the Association for Information Systems, 9(6), 344e376.

Shin, D., 2014. A socio-technical framework for internet-of-things design: a human-cen- tered design for the internet of things. Telematics Inform. 31, 519–531.

Slyke, C. V., Shim, J. T., Johnson, R., & Jiang, J. (2006). Concern for information pri- vacy and online consumer purchasing. Journal of the Association for Information Systems, 7(6), 415e444.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring in- dividuals' concerns about organizational practices. MIS Quarterly, 20(2), 167-196

Speed, C., 2010. An internet of old things. Digit. Creat. 21, 239–246.Stankovic, J.A., 2014. Research directions for the internet of things. IEEE Internet Things J. 1, 3–9.

Stankovic, J.A., 2014. Research directions for the internet of things. IEEE Internet Things J. 1, 3–9.

Sundar, S.S., Kang, H., Wu, M., Go, E., Zhang, B., 2013. Unlocking the privacy paradox: Do cognitive heuristics hold the key?. In: Proceedings of CHI'13 Extended Abstracts on Human Factors in Computing Systems, France, 811–816.

Sung,W.-T.&Chang,K.-Y.(2013),"Evidence-based multi-sensor information fusion for remote health care systems", Sensors and Actuators A: Physical 204, 1-19.

Sung, W.-T. & Chiang, Y.-C. (2012), "Improved Particle Swarm Optimization Algorithm for An- droid Medical Care IOT using Modified Parame- ters", Journal of Medical Systems 36(6), 3755-3763

Tan, M., & Teo, T. S. H. (2000). Factors influencing the adoption of Internet banking. Journal of the Association for Information Systems, 1(5), 1-42.

Tarouco, L., Bertholdo, L., Granville, L., Arbiza, L., Carbone, F., Marotta, M. & de Santanna, J. (2012), "Internet of Things in healthcare: Interoperability and security issues,". In: Communications (ICC), 2012 IEEE International Conference on, pp. 6121-6125

TRUSTe, T. R. U. S. T. (2014). *US con- sumer confidence privacy report: consumer opinion and business impact*. Research Re- port, TRUSTe Inc.

Tsai, J., Cranor, L., Acquisti, A., Fong, C., 2006. What's it for you? A survey of online privacy concerns and risk. NET Institute Working Paper, No. 06–29, 1–20.

UK Research Council, 2013. Research in the wild - Internet of Things 2013.Uzelac, A., Gligoric, N., Krco, S., 2015. A comprehensive study of parameters in physical environment that impact students' focus during lecture using internet of things. Comput. Hum. Behav. 53, 427–434.

Uzelac, A., Gligoric, N., Krco, S., 2015. A comprehensive study of parameters in physical environment that impact students' focus during lecture using internet of things. Comput. Hum. Behav. 53, 427–434.

Weber, R.H., 2009. Internet of things - need for a new legal environment? Comp. Law Sec. Rev. 25, 522–527.

Weber, R.H., 2011. Accountability in the Internet of things. Comput. Law Secur. Rev. 27 (2), 133–138.

Weber, R.H., 2013. Internet of things - governance quo vadis? Comp. Law Sec. Rev. 29, 341–347.

Weber, R.H., 2015. Internet of things: privacy issues revisited. Comp. Law Sec. Rev. 31, 618–627.

Weinberg, B.D., Milne, G.R., Andonova, Y.G., Hajjat, F.M., 2015. Internet of things: convenience vs. privacy and secrecy. Bus. Horiz. 58 (6), 615–624

West, J., & Dedrick, J. (2000). Innovation and control in standards architectures: the rise and fall of Japan's PC-98. Information Systems Research, 11(2), 197e216.

Winter, J.S., 2014. Surveillance in ubiquitous network societies: normative conflicts re- lated to the consumer in-store supermarket experience in the context of the internet of things. Ethics Inf. Technol. 16, 27–41.

Wu, J. H., Chen, Y. C., & Lin, L. M. (2007). Empirical evaluation of the revised end user computing acceptance model. Computers in Human Behavior, 23, 162e174.

Xu, X., 2012. Internet of things in service innovation. In: Amfiteatru Economic. 14. pp. 698–719.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information Privacy Concerns: Linking Individual Perceptions with Insti- tutional Privacy Assurances. *Journal of the Association for Information Systems*, *12*(12), 798-824.

Yan, B.N., Lee, T.S., Lee, T.P., 2015. Mapping the intellectual structure of the internet of things (IoT) field (2000–2014): a co-word analysis. Scientometrics 105, 1285–1300

Yang,G.,Xie,L.,Mantysalo,M.,Zhou,X.L.,Pang, Z. B., Xu, L. D., Kao-Walter, S., Chen, Q. & Zheng, L. R. (2014), "A Health-IoT Platform Based on the Integration of Intelligent Packaging, Unobtrusive Bio-Sensor, and Intelligent Medicine Box", Industri- al Informatics, IEEE Transactions on 10(4), 2180-2191.

Yang, J., & Mai, E. (2010). Experiential goods with network externalities effects: an empirical study of online rating system. Journal of Business Research, 63, 1050e1057.

Yang,L,Ge,Y.,Li,W.,Rao,W.&Shen,W.(2014a), "A home mobile healthcare system for wheelchair users". In: Computer Supported Cooperative Work in Design (CSCWD), Proceedings of the 2014 IEEE 18th I.nternational Conference on, pp. 609-614.

Yang, L., Yang, S.H., Plotnick, L., 2013. How the internet of things technology enhances emergency response operations. Technol. Forecast. Soc. Chang. 80, 1854–1867.

Yang Lu, Savvas Papagiannidis, Eleftherios Alamanos 2018. Internet of Things: A systematic review of the business literature from the user and organisational perspectives.

Yen, D. C., Wu, C. S., Cheng, F. F., & Huang, Y. W. (2010). Determinants of users' intention to adopt wireless technology: an empirical study by integrating TTF with TAM. Computers in Human Behavior, 26, 906e915.

Zhao, K., Xia, M., & Shaw, M. J. (2007). An integrated model of consortium-based e- business standardization: collaborative development and adoption with network externalities. Journal of Management Information Systems, 23(4), 247e27

Zhou, T., & Li, H. (2014). Understanding mobile SNS continuance usage in China from the perspectives of social influence and privacy concern. Computers in Human Behavior, 37, 283e289.

Zhou, W., Piramuthu, S., 2015. Information relevance model of customized privacy for IoT. J. Bus. Ethics 131, 19–30.

Dipartimento Impresa e Management

Corso di Laurea Magistrale in Marketing
indirizzo in Analisi e Misure di Marketing

Cattedra di Marketing Metrics

ANALISI DEI FATTORI CRITICI SULL'ADOZIONE DEI SERVIZI IOT IN AMBITO MEDICO E SANITARIO: TRATTAMENTO DEI DATI PERSONALI, PRIVACY PARADOX ED ESTERNALITÀ DI RETE

Relatore:
Prof. Costabile Michele

Candidato
Sergenti Pietro

Correlatore:
Prof. Tedeschi Piermario

Anno Accademico 2018/2019

1. Introduzione

Sempre più frequentemente interagiamo nel quotidiano con dispositivi elettronici, dai semplici elettrodomestici alle apparecchiature digitali di ultima generazione. Soprattutto verso questi ultimi si rivolge l'attenzione del mercato. Da molti anni a questa parte il *trend* di utilizzo di nuove tecnologie è in forte crescita e questo fenomeno risulta essere presente in diversi settori e contesti. Il più affascinante di tutti riguarda sicuramente l'ambito applicativo dell'*Internet of Things*, che tradotto significa banalmente Internet delle cose. L'*Internet of Things*, da cui l'acronimo IoT, fa riferimento alla capacità di oggetti o dispositivi, di interagire con il mondo esterno. I dispositivi IoT quindi, non si limitano più a registrare in maniera passiva i dati, ma bensì ad immagazzinarli, rielaborarli e trasmetterli ad altri dispositivi. Questa è pertanto la loro principale peculiarità, la capacità di interfacciarsi in maniera semplice con l'utilizzatore e di comunicare tra loro. Una tale duttilità di applicazione ha permesso a tutti i dispositivi IoT, meglio noti come *smart device*, di fare facilmente breccia nel mercato, e di riflesso, nella vita degli utilizzatori. Grazie a questi dispositivi di più vario genere (si pensi dagli orologi, ai telefoni, ai visori a realtà aumentata) si sono modificate, in un lasso di tempo relativamente breve, le abitudini dei consumatori. Questo cambiamento comportamentale, denotabile come un crescente utilizzo e disposizione di dispositivi *smart*, ha portato ad un aumento esponenziale dei dati generati, in particolar modo quelli di natura privata/personale. Proprio sulla raccolta dei dati personali sono nate, e tutt'oggi presenti, molte discussioni riguardanti la tutela della privacy degli utilizzatori spesso ignari o inconsapevoli della grande mole di dati generati e raccolti sulla loro persona. Inoltre, trattandosi di tipologie di dati etichettabili come *big data*, a causa della mole generata, sono soggetti a molti rischi, uno dei quali riguarda l'anonimizzazione che può essere facilmente aggirata. Nonostante si sia denotata una forte preoccupazione verso la tutela dei dati personali e della propria privacy, l'atteggiamento reale tenuto dai consumatori non sempre rispecchia l'atteggiamento teorico da loro stessi indicato. Questo perché malgrado la privacy sia risultata essere una preoccupazione primaria nell'era digitale, i consumatori sono disposti a concedervici accesso in cambio di *reward*, anche di bassa valenza. L'osservazione di questa incoerenza comportamentale ha portato molti studiosi a domandarsi il perché questo avvenga ma soprattutto ad interrogarsi sul "cosa" fosse necessario per far sì che si "attivasse" questa inversione comportamentale. Proprio in risposta a questi quesiti è stato definito il paradosso della privacy (*privacy paradox*).

In questo studio, pertanto, si cercherà di comprendere se una determinata tipologia di *reward* possa essere in grado di innescare l'inversione comportamentale del consumatore circa la disponibilità alla raccolta, elaborazione e condivisione dei propri dati personali. Nello specifico la *reward* utilizzata sarà una ricompensa di servizio e non monetaria. Lo studio verterà sui sistemi IoT a carattere medico sanitario, fenomeno di business che dimostra avere un grande seguito in termini di crescita per gli anni futuri. Specialmente negli ultimi anni il settore sanitario ha concentrato gli sforzi sull'ottimizzazione delle procedure di gestione dell'inventario attraverso l'integrazione della tecnologia di informazione e comunicazione, ma soprattutto sulla ristrutturazione dell'assistenza sanitaria utilizzante tecnologie IoT nella gestione ed ottimizzazione delle risorse mediche, monitoraggio delle situazioni sanitarie ed aumento dell'uso dell'assistenza medica

domiciliare. L'IoT *healthcare* è un promettente scenario di applicazione B2C, in cui i consumatori (pazienti) vengono tenuti sotto osservazione da remoto, grazie l'ausilio di *smart devices* e la generazione/raccolta di bio-dati.

Vale la pena chiedersi quindi, come possano coesistere dispositivi IoT *healthcare* e problematiche di privacy dovute alla raccolta dei dati. L'obbiettivo di questo studio è proprio quello di comprendere come poter rendere questo possibile, utilizzando come moderatore una ricompensa di servizio a carattere medico-sanitario. Integrare quindi ad un dispositivo IoT di carattere generale una competenza medica e vedere se questa è ritenuta sufficientemente importante da innescare il paradosso della privacy facendo così adottare il servizio IoT al consumatore. Inoltre, il modello di riferimento utilizzato può dirci molto su altri elementi cruciali ai fini dell'adozione, quali le esternalità di rete indirette, i benefici percepiti e l'atteggiamento.

Nel primo capitolo verrà esposta la revisione della letteratura in merito agli *hot topic* della ricerca, ossia la nascita e definizione dell'*Internet of Things*, con identificazione della *market size, forecast* di mercato ed applicazione all'area medico/sanitaria; definizione ed inquadramento del concetto di privacy, *privacy paradox* e domanda di ricerca. Il secondo capitolo invece presenterà il modello da cui ha origine lo studio, con formulazione delle ipotesi ed introduzione della variabile aggiuntiva (*service reward).* L'ultimo capitolo, il terzo, esporrà le analisi condotte sul campione di riferimento ottenuto tramite la raccolta di dati grazie a questionari condivisi sulle principali piattaforme social. Grazie ad esse la parte conclusiva esporrà alcune implicazioni manageriali derivanti dai risultati ottenuti, nonché limiti della ricerca e spunti per eventuali lavori futuri.

2. Internet Of Things

Inutile dire come dai primi anni '90 ad oggi la definizione dell'IoT abbia subito molti cambiamenti. L'aumento degli *smart device* ha definitivamente consacrato l'avvento di quest'ultimo arricchendone sia il palinsesto applicativo che quello letterario. Come già rimarcato in precedenza l'*Internet of Things* prometteva sin dall'inizio un nuovo paradigma tecnologico in grado di connettere tutto e tutti in un qualsiasi momento ed in un qualsiasi posto utilizzando qualunque percorso/rete o servizio (Baldini et al., 2016; Guillemin and Friess, 2009; Man et al., 2015; UK Research Council, 2013). La visione dell'IoT è quella di uno "*smart world*" attrezzato di tecnologie di rilevamento e componenti intelligenti. L'*Internet of Things* si colloca in quello che viene definito Web 3.0; un web che a differenza del suo predecessore, il Web 2.0, coinvolge in maniera molto più profonda i suoi utenti. Ciò è dovuto al fatto che questi si relazionano con un ambiente fisico e non più prettamente informatico e che va ben oltre la semplice creazione e condivisione di contenuti (Kreps and Kimppa, 2015). Non stupisce che una visione così audace abbia destato l'interesse di accademici e professionisti. È opportuno ritenere che l'IoT impatterà significativamente individui, aziende e politiche mettendo in discussione modelli aziendali, societari ed erogazione di servizi per come oggi sono conosciuti (Shin, 2014; Stankovic, 2014). Per contro la natura pervasiva dell'IoT e la continua generazione di dati

potrebbero seriamente suscitare importanti preoccupazioni sull'invasione della privacy in un mondo completamente connesso. Proprio in virtù di quanto sopra citato, la mole di pubblicazioni correlate all'IoT è aumentata esponenzialmente negli ultimi anni (Olson et al.,2010). Un paper molto importante e di grande contributo alla letteratura risulta essere quello di Atzori et al. (2010), che contiene i concetti riguardanti la classificazione e l'introduzione delle tecnologie compatibili con l'IoT ed una struttura di applicazioni pertinenti ad esso in grado di suggerire nuove strade per ulteriori ricerche (Atzori et al., 2010). Seguendo un simile approccio, anche lo studio di Li et al. (2014) si preoccupa di dare una visione integrata dell'IoT, affrontandone l'architettura, le tecnologie e le applicazioni in termini prettamente tecnici. Inoltre, vengono affrontati i problemi collegati alla standardizzazione dei processi, sicurezza dei dati e privacy degli utenti (Li et al., 2014). Le tecnologie abilitanti e i problemi di sicurezza dell'IoT sono state le tematiche che hanno coperto per l'80% la letteratura esistente in merito sino al 2014 (Yan et al., 2015).

A seguito di quanto detto emerge un problema evidenziato nello studio di Li et al., ovvero la grande lacuna nella letteratura IoT legata al business. Nessuna delle review svolte sino a quel momento aveva mai fornito un'analisi delle pubblicazioni dell'IoT dal punto di vista del business. Proprio per questo motivo la terza parte di questo capitolo viene interamente dedicata all'applicazione dell'IoT nel mondo del business, a dimostrazione dell'importanza della tematica e attualità della stessa.

Come precedentemente detto esistono molte definizioni in grado di identificare l'Internet of Things, ma quelle maggiormente apprezzate dall'opinione pubblica sono tre. La prima è attribuibile ad Atzori et al. (2010) secondo cui l'IoT è il risultato della convergenza di tre visioni: una visione "orientata alle cose", una "orientata verso Internet" ed una "semantica". L'IoT è stato definito semanticamente come "una rete mondiale di oggetti interconnessi" in grado di esercitare una "presenza pervasiva" nei confronti degli utenti che a loro volta interagiscono con altri oggetti ma anche nei confronti dell'ambiente fisico che li circonda e raggiungere così obbiettivi comuni (Atzori et al., 2010).

La seconda definizione invece è stata presentata da ITU (ITU Strategy and Policy Unit, 2005; ITU-T, Y. 2060, 2012), che ha posto l'accento su come l'IoT sia ogni oggetto del mondo fisico o virtuale "in grado di essere identificato nelle reti di comunicazione".

Infine, quella che può essere considerata una delle definizioni più rappresentative è stata proposta dalla Commissione Europea, secondo cui l'IoT è un'infrastruttura di rete globale dinamica integrata in Internet in cui varie "*things*" hanno identità unica, attributi fisici, personalità virtuale e interfacce intelligenti (Guillemin e Friess, 2009). In altre parole, "l'*Internet of Things* consentirà a persone e cose di essere connessi in qualsiasi momento, in qualsiasi luogo, con qualsiasi cosa e chiunque, idealmente utilizzando qualsiasi percorso/rete o servizio" (Guillemin e Friess, 2009). Il termine "cose" agisce come una nuova dimensione dell'estensione dell'attuale interazione umana e applicativa esistente, consentendo di collegare persone e oggetti, scambiando informazioni in tempo reale attraverso qualsiasi percorso (Baldini et al., 2016; Guillemin e Friess, 2009 ; Man et al., 2015; UK Research Council, 2013).

Per quanto differenti, le definizioni sopra citate hanno vari punti di contatto. Ad esempio, condividono tutte e tre il concetto di rete dinamica, di infrastruttura globale, interconnessione ma soprattutto l'interazione tra esseri umani e cose. Lo scopo dell'IoT è rendere possibile la condivisione efficiente di informazioni in tempo reale tra attori autonomi nella rete (Yang et al., 2013). L'IoT si riferisce alla presenza pervasiva di miliardi di oggetti in grado di comunicare in maniera intelligente, connessi in una struttura simile ad Internet. L'idea finale dell'IoT è quella di considerarlo come l'estensione futura di Internet, ma anche delle città e del mondo stesso, proprio grazie alla sua capacità di comprendere oggetti smart in grado di percepire e reagire a ciò che li circonda (Ng et al., 2015; Rau et al., 2015; Shin , 2014; Stankovic, 2014).

L'architettura globale IoT facilita lo scambio di beni e servizi e l'interazione tra oggetti intelligenti, così da creare delle vere e proprie opportunità di innovazione di servizio. Quello che sostanzialmente l'IoT è in grado di garantire è un'innovazione dei processi standard come oggi li conosciamo. Grazie alle sue caratteristiche ed alla sua architettura, è uno strumento completamente nuovo e con caratteristiche di versatilità ed applicazione uniche (Baldini et al., 2016; Dlodlo et al., 2012; Winter, 2014). Con i *social system* sempre più orientati verso una piena connettività, l'IoT è stato considerato come una vera e propria rivoluzione tecnologica ed un processo di cambiamento sociale (Elmaghraby e Losavio, 2014; Quigley and Burke, 2013; Speed, 2010; Xu, 2012). Bisogna tuttavia tener conto che il mondo sta diventando ricco di dati e ci stiamo avviando verso uno scenario in cui la condivisione e l'esposizione di dati sensibili aumenterà sempre di più, portandoci a ragionare su tematiche quali la tutela della privacy e sulla sicurezza delle informazioni (Brill, 2014; Weinberg et al., 2015).

L'ultima tematica affrontata è uno dei punti chiave su cui verterà la ricerca: la disciplina in merito alla tutela della privacy e la percezione che l'utente ha di questa. Prima di passare ad analizzare questa parte bisogna però soffermarci sulla letteratura relativa alle attività commerciali e le prospettive organizzative. Il motivo per cui affrontiamo questo argomento è che la letteratura che la riguarda questo argomento è una delle meno presenti ma più attuali. Basti considerare che è solo dal 2015 che vengono fatte ricerche di spessore sulle potenziali applicazioni di business dell'IoT (Y. Lu et al., 2018).

3. Privacy Paradox

Nel 2001, uno studio sull'uso di Internet indagava la popolarità dello shopping online e le preoccupazioni dei consumatori/utenti circa la loro privacy e sicurezza dei loro dati (Brown, 2001). Fu Brown per primo, attraverso varie sessioni di *deep interview* ad accorgersi di "un paradosso della privacy". Mentre le persone esprimevano le loro preoccupazioni sulla violazione dei loro dati personali, di fatto si dimostravano disposte a fornire dettagli personali ai rivenditori online in cambio di una *reward*. Gli intervistati hanno dichiarato di temere la raccolta massiva di informazioni sul loro conto, ma ciò non ha di fatto impedito loro di proseguire ad acquistare online. È successivamente emerso che carte fedeltà, sconti e regali offerti hanno avuto la funzione di catalizzatori per attirare i consumatori ad acquistare online. Queste implicazioni sono risultate

coerenti con le ricerche fatte sulle carte fedeltà, le quali avevano dimostrato che gli acquirenti erano disposti a scambiare informazioni sui loro acquisti se in cambio potevano risparmiare al momento dell'emissione dello scontrino. (Savre & Horne, 2000). Nello stesso anno, Spiekermann et al. (2001) hanno presentato i risultati di uno studio volto a rivelare la relazione tra le preferenze sulla privacy e il comportamento reale nel contesto dell'e-commerce. Lo studio consisteva in un esperimento in grado di confrontare le preferenze sulla privacy autoregolate con il comportamento di divulgazione effettiva durante lo shopping online. I partecipanti hanno inizialmente compilato un questionario in grado di catturare e misurare le loro attitudini e preferenze verso la privacy, e seguentemente hanno visitato un negozio online. Durante la fase di visita del sito e shopping online sono stati coinvolti, tramite *chatbot*, in una conversazione finalizzata alla vendita. I partecipanti hanno risposto a gran parte delle domande, nonostante queste fossero strettamente personali. Questo evidenzia come, nonostante gli utenti di Internet affermino che la privacy sia un elemento di massima priorità, nella pratica non si comportano di conseguenza. Un esempio ancor più eclatante sulla dicotomia esistente tra atteggiamento e comportamento è stato fornito dai ricercatori che hanno perseguito la via del comportamento economico. Acquisti (2004) ha affermato che "le persone potrebbero non essere in grado di agire come agenti economicamente razionali quando si tratta di privacy personale". Quello che la precedente frase vuole lasciar intendere è che le decisioni relative alla privacy sono influenzate da informazioni incomplete, razionalità limitata e pregiudizi psicologici, come *bias* di conferma, sconto iperbolico ed altri. Questi *bias* decisionali sono stati ben documentati nella letteratura di economia comportamentale (per esempio Gilovich et al., 2002). Acquisti ha costruito un modello economico in grado di spiegare parte dell'*attitude* verso la privacy e le incoerenze comportamentali. Il modello incorpora il pregiudizio immediato della gratificazione. Gratificazione immediata si riferisce alla tendenza da parte del consumatore di dare maggiore peso ai benefici presenti contro i rischi futuri. Pertanto, la valutazione euristica condotta dalle persone porta a considerare i benefici attuali ricevuti come un valido compromesso alla divulgazione delle informazioni personali ed i rischi futuri ad essi associati (Acquisti, 2004).

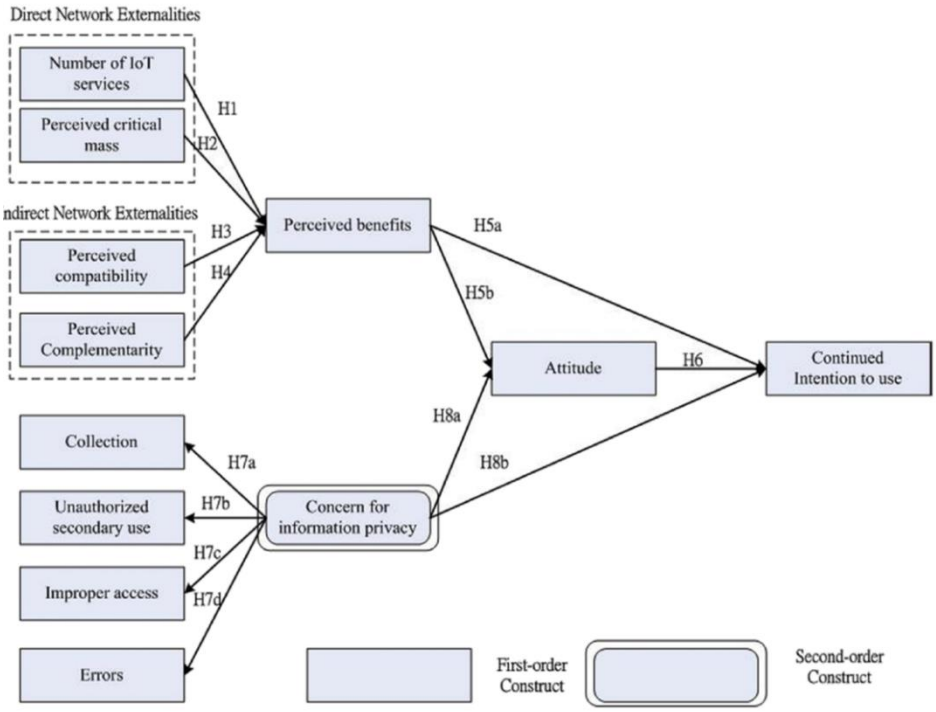
Passando dalla teoria economica alla ricerca empirica, Acquisti e Grossklags (2005) hanno raccolto dei dati in grado di supportare l'ipotesi secondo cui il processo decisionale che avviene sulla privacy sia influenzato da informazioni incomplete, razionalità limitata e pregiudizi psicologici (euristiche e *bias* cognitivi). È stato inoltre provato che sebbene la maggior parte dei soggetti (circa l'89%) abbia dichiarato di essere moderatamente o molto preoccupato per la privacy, oltre il 21% del campione ha ammesso di aver fornito dati strettamente personali in cambio di sconti o servizi. Un altro flusso di ricerca mirava a comprendere il comportamento auto-rivelante tra i giovani nei *social network.* Barnes (2006) usa il termine paradosso della privacy in riferimento al comportamento tenuto dai giovani ne confronti della privacy sui siti di *social networking* (SNS). I giovani tenderebbero a non rendersi conto che gli SNS forniscono uno spazio pubblico gratuito divulgando informazioni sensibili che potrebbero essere soggette ad un utilizzo improprio. Il termine paradosso della privacy inteso per come lo intendiamo oggi è da attribuirsi principalmente a Norberg et al., (2007). Sono stati condotti due studi, ciascuno dei quali composto da due fasi. Nella prima

fase è stato chiesto ad un campione di studenti la disponibilità a rivelare informazioni specifiche. La seconda parte, oltre ad aver avuto luogo svariate settimane dopo la prima, consisteva nel richiedere ai soggetti lo stesso tipo di informazioni ma da parte di un ricercatore di mercato. Questo studio ha il merito di aver confermato l'ipotesi secondo cui gli individui avrebbero effettivamente rivelato una quantità significativamente maggiore di informazioni personali rispetto a quanto era stato indicato nelle intenzioni dichiarate.

4. Theoretical Background

Il modello costruito per l'indagine si ispira a quello teorizzato da Hsu e Lin. Prima di mostrare le variabili in esso presenti, passeremo in rassegna gli elementi più importanti e i principali snodi attraverso i quali il modello si articola e dai quali successivamente svilupperemo quello utile alla nostra domanda di ricerca. Gli elementi originali del modello, trattati nel paragrafo 2.1, riguardano l'IoT, le esternalità di rete e il permesso al trattamento dei dati personali (CFIP). Infine, sarà presente la parte basata sul *Privacy Paradox Phenomenon*. Infatti, nel modello è stata introdotta una variabile a carattere di *reward.* Questa era, secondo letteratura, la causa scatenante del paradosso della privacy. In questa circostanza essa avrà natura di *reward* di servizio andando a giocare il ruolo di moderatore all'interno del modello. Si cercherà pertanto di capire se una *reward* di servizio di tipo sanitario è in grado di innescare lo stesso meccanismo che una *reward* monetaria o di personalizzazione era in grado di innescare nel consumatore. Una volta misurata si osserverà che effetto di moderazione viene esercitato rispettivamente su *attitude*, CFIP e benefici percepiti. Il modello concettuale che andremo ad utilizzare si rifà principalmente a quello utilizzato da Hsu e Lin nel loro lavoro del 2016: "*An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives*". Il modello da loro utilizzato, di cui in Figura 6, dimostrava come l'intenzione all'utilizzo dei sistemi IoT fosse determinata dai benefici percepiti dai consumatori, dalla preoccupazione che essi avevano per il trattamento delle informazioni sulla privacy e dal loro atteggiamento verso questi sistemi. Inoltre, l'atteggiamento media l'impatto dei benefici percepiti e la preoccupazione per la privacy delle informazioni. Il numero di servizi IoT e la massa critica percepita sono considerati esternalità di rete dirette e la compatibilità e complementarità percepite sono definite come esternalità di rete indirette. Questi quattro costrutti sono teorizzati per essere i predittori dei benefici percepiti. La preoccupazione per la riservatezza delle informazioni è trattata come un costrutto di secondo ordine che prende in considerazione la raccolta, l'uso secondario non autorizzato, l'accesso improprio e gli errori.

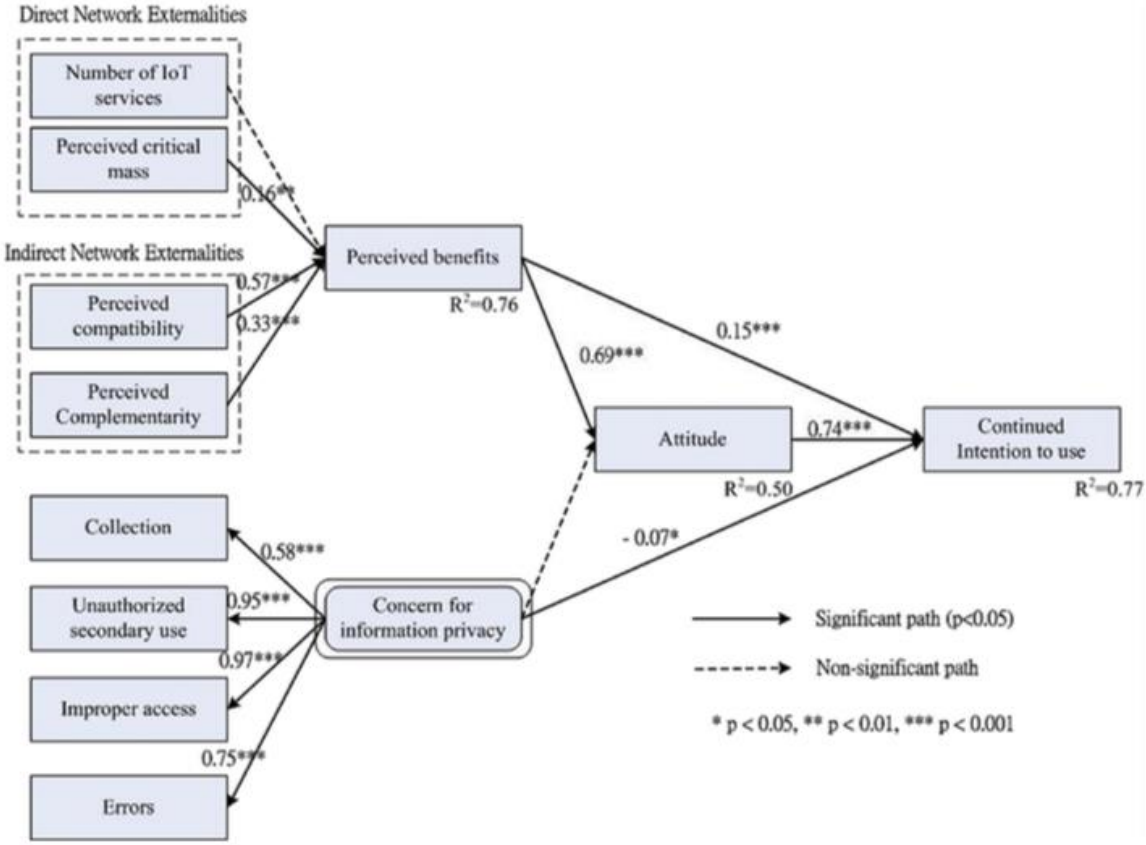
Figura 6 – Framework di riferimento



Sources: Hsu&Lin "An empirical examination of customer adoption of Internet of Things services: network externalities nd concern for information privacy perspectives", 2016

Con questo studio Hsu e Lin hanno contribuito a fornire le seguenti implicazioni teoriche. In primo luogo, a differenza di altri studi precedenti che esaminavano l'effetto delle esternalità di rete sull'adozione e standard di tecnologie informatiche specifiche, come servizi di telefonia mobile (Iimi, 2005), tecnologie di informazione interattiva (Lin & Bhattacherjee, 2008), social network (Chiu et al., 2013; Lin & Lu, 2011), *e-service* (Lin et al., 2011), videogiochi online (Yang & Mai, 2010) e servizi di comunicazione mobile (Kim, Park, & Oh, 2008), pochi studi però hanno esaminato l'effetto delle esternalità di rete sull'utilizzo del servizio IoT. Il loro studio scompone le esternalità di rete e esamina empiricamente la loro influenza sui benefici percepiti. I risultati confermano che la massa critica, la compatibilità e la complementarietà percepite hanno avuto effetti significativi sui benefici percepiti e, a loro volta, influenzano l'atteggiamento verso l'adozione e l'uso continuo dei servizi IoT. Inoltre, le variabili detenevano una vera e propria posizione dominante poiché in grado di spiegare gran parte della varianza nell'atteggiamento verso l'uso dell'IoT, che, a sua volta, era il fattore più influente nel determinare la continua intenzione dell'utente di utilizzare i servizi IoT (Figura 7).

Figura 7 – Framework di riferimento, con beta di regressione

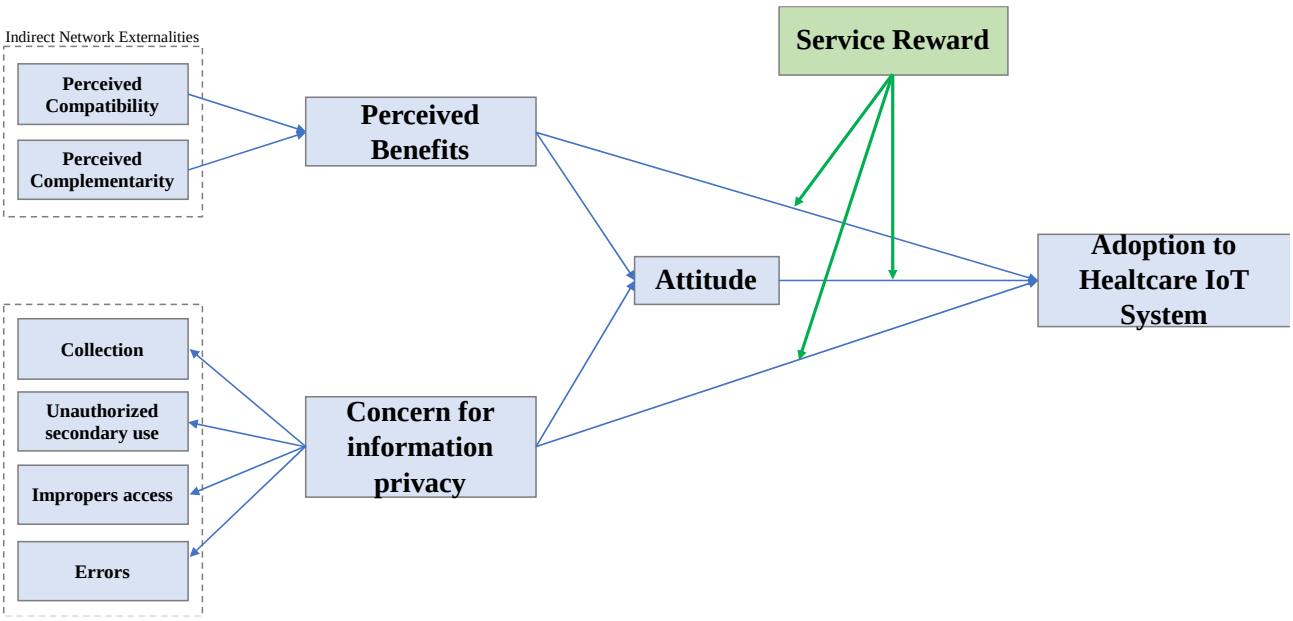


Sources: Hsu&Lin "An empirical examination of customer adoption of Internet of Things services: network externalities nd concern for information privacy perspectives", 2016

Un suggerimento proposto dallo studio riguarderebbe il miglioramento, dal lato dell'offerta, dei servizi IoT in termini di aumento di complementarietà e miglioramento della disponibilità degli stessi piuttosto che aumentarne il numero. In secondo luogo, i precedenti studi indicavano che i problemi di privacy avevano un impatto significativo sull'intenzione degli utenti all'adozione. Hsu e Lin hanno confermato empiricamente il dato, ma con un impatto piuttosto debole. Inoltre, lo studio contribuisce alla letteratura IoT suggerendo anche l'accesso improprio e l'uso secondario non autorizzato ("*improper access*" e "unauthorized *secondary use*") sono entrambi componenti importanti nella disponibilità a concedere informazioni personali CFIP ("*concern for information privacy*"). In conclusione, sono state evidenziate alcune importanti informazioni per i fornitori di servizi IoT. I benefici percepiti, avendo un impatto positivo sull'adozione dei servizi IoT, indicano come gli utenti siano preoccupati dei vantaggi d'uso dell'IoT e del valore che ne scaturisce dall'utilizzo. Inoltre, le esternalità indirette (compatibilità e complementarietà percepite) sono fondamentali per motivare l'adozione tra la maggior parte degli utenti. Quindi i fornitori dovrebbero essere consapevoli della loro importanza, garantendo l'adattamento ai valori e agli stili di vita degli utenti. Come detto precedentemente, i fornitori dovrebbero curare maggiormente l'aspetto della complementarietà dei servizi offerti piuttosto che il numero,

questo perché il complementare percepito è risultato essere un fattore predittivo molto influente nella formazione degli atteggiamenti positivi verso i servizi IoT. Infine, per eliminare i rischi per la privacy, è stato suggerito un aumento dell'offerta verso gli utenti in termini di maggiore concretezza del servizio per quanto riguarda le responsabilità dei provider e i meccanismi di conservazione dei dati. Poiché questo studio si basava su esternalità di rete e CFIP come antecedenti dell'intenzione comportamentale di continuare ad utilizzare i servizi IoT, potrebbero esserci presumibilmente più predittori di adozione come cultura, stile di vita, influenze sociali, personalità e costi. Pertanto, i risultati dello studio di Hsu e Lin non dovrebbero essere generalizzati e applicati all'adozione di IoT basata sull'impresa, come la piattaforma di informazioni logistiche. Proprio su questo spunto finale del loro lavoro sono state gettate le basi per questo studio. L'idea con cui mi sono approcciato all'argomento è stata quella di andare ad indagare quali potessero essere altri agenti in grado di influenzare il processo di adozione dei sistemi IoT da parte dei consumatori. In particolar modo mi sono focalizzato sull'ambito della privacy e trattamento dei dati personali cercando di capire quale fenomeno potesse essere in grado sia di smorzare l'effetto negativo che la CFIP aveva sull'intenzione all'adozione di sistemi IoT sia di incidere positivamente sui benefici percepiti. Per fare questo è stato introdotto un moderatore denominato "*service reward*" ossia "ricompensa di servizio". La variabile moderatrice viene concepita nel momento in cui si va a studiare il fenomeno della privacy *paradox*. L'idea è quella di proporre un servizio come *reward* al fine di modificare l'atteggiamento dei consumatori sia verso l'adozione dei sistemi IoT che verso la CFIP. Inoltre, il *framework* modificato, oltre ad includere la variabile moderatrice, esclude la parte delle esternalità dirette in quanto si erano dimostrate essere molto esplicative della variabile "benefici percepiti" e sarebbe risultato ridondante studiarle nuovamente. Per contro sono state tenute quelle definite come esternalità indirette. La motivazione è da ricercarsi nelle implicazioni che lo studio di Hsu e Lin ha generato. È stato rimarcato più volte quanto la complementarietà e la compatibilità dei servizi IoT dovessero essere implementate in termini di offerta di mercato anziché aumentare il numero di dispositivi/servizi. Da qui la decisione di trattenere solo le esternalità indirette all'interno del *framework* e non quelle dirette. Come riassunto in Figura 8 andremo a misurare come la variabile moderatrice impatta rispettivamente sull'"*attitude*", sulla CFIP e sui "*perceived benefits*" nei confronti dell'"*adoption to healthcare IoT system*". La variabile moderatrice "*service reward*" ha sostanzialmente la funzione di porre in maniera chiara e ben rappresentata l'offerta di servizio che il prodotto IoT è in grado di fornire. La *reward* di servizio in questo caso si identifica nella prevenzione di possibili complicazioni sanitarie ed ha anche la funzione di sensibilizzare ed informare il consumatore rispetto ai dispositivi IoT in ambito *healthcare*. L'effetto di moderazione si compone di un'immagine di un *wearable device* ed una descrizione in cui viene definita in maniera chiara e semplice l'applicazione che ne viene fatta ed i vantaggi/benefici che se ne possono trarre.

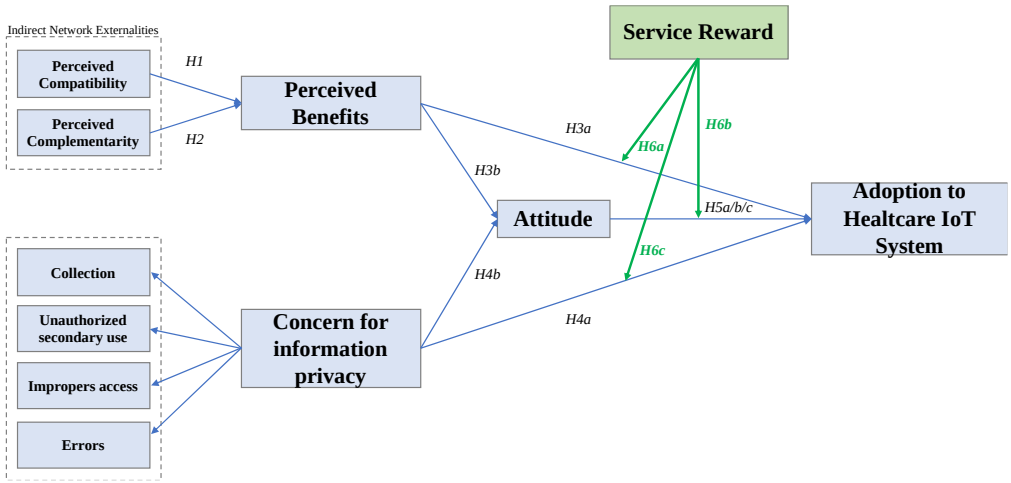
Figura 8– Nuovo Framework di riferimento



5. Ipotesi e modello di ricerca

Come precedentemente detto, l'obbiettivo dello studio consiste nel riproporre il modello concettuale dell'articolo di Hsu & Lin (2016), escludendo le variabili riguardanti le esternalità dirette ma aggiungendo una variabile moderatrice denominata "*service reward*" che andrà ad impattare su *Perceived benefits*, CFIP ed *Attitude*. L'intento è quello di replicare l'esperimento estendendolo anche alla tassonomia di *device* in grado di fornire supporto medico, ma soprattutto quello di verificare se un servizio percepito come *reward* sia in grado di confermare il paradosso della privacy. Riassumendo si vuole verificare se e come un servizio ti tipo sanitario collegato ai sistemi IoT, proposto come *reward* in cambio di accesso ai dati personali degli utenti, riesca a verificare il *privacy paradox*. Di seguito vengono presentate le 14 ipotesi di ricerca che si vogliono studiare (Figura 9).

Figura 9– Nuovo Framework di riferimento con Hp



Le variabili che compongono le fondamenta del modello sono quelle inerenti alle esternalità di rete, che come precedentemente detto, in questo studio, saranno comprensive delle sole esternalità indirette. In linea con quanto affermato dall'autore, le esternalità indirette si compongono di due variabili: compatibilità percepita e complementarità percepita. Queste due variabili incorporano al loro interno i costrutti inerenti all'utilità percepita dall'utente in base alla compatibilità e complementarità che i dispositivi IoT hanno verso *device* di altro genere e natura. La compatibilità percepita è il grado in cui un servizio IoT viene percepito come coerente con i valori esistenti, i bisogni e le esperienze passate dei potenziali utilizzatori. Teoricamente, la teoria della diffusione dell'innovazione ha indicato che la compatibilità è l'elemento chiave nel motivare la maggior parte degli adottanti (Rogers, 1983). Studi precedenti hanno confermato che la compatibilità percepita di un'innovazione ha un'influenza positiva verso l'adozione del servizio IoT (Cooper & Zmud, 1990; Hardgrave et al., 2003; Tan & Teo, 2000). Ciò implica l'importanza della compatibilità percepita come antecedente dell'adozione. La variabile complementarietà percepita è invece definita come la disponibilità di funzioni o applicazioni che servono a compilare o completare i servizi IoT. Quando le esternalità di rete indirette riguardano un prodotto/servizio con prodotti/ servizi una maggiore complementarietà crea ulteriori vantaggi di rete per gli utenti (Lin & Bhattacherjee, 2008). Pertanto, nel contesto dei servizi IoT, ulteriori applicazioni complementari e funzioni quali identificazione, transazioni, accesso di controllo, tessere associative, biglietti elettronici e assistenza sanitaria, aumentano la convivialità della vita degli utenti ed efficienza del lavoro. Entrambe le variabili sono in grado di influenzare positivamente i benefici percepiti del consumatore i quali risultano essere un costrutto fondamentale in grado di influenzare direttamente l'intenzione all'adozione di sistemi IoT in ambito medico/sanitario. Di conseguenza, i costrutti e le ipotesi ad essi associati vengono preservati dal modello originale (H1, H2), e adattati al contesto di questa ricerca:

> ***H1.*** *La compatibilità percepita ha un effetto positivo sui benefici percepiti dall'utilizzo di servizi IoT.*
> ***H2.*** *La complementarità percepita ha un effetto positivo sui benefici percepiti dall'utilizzo di servizi Iot.*

Precedenti studi hanno confermato che i benefici hanno un effetto significativo sull'atteggiamento e l'intenzione comportamentale (Davis, 1989; Lin & Bhattacherjee, 2008; Yen, Wu, Cheng, & Huang, 2010). L'atteggiamento è stato definito come il grado in cui gli utenti provano sentimenti positivi utilizzando dei servizi IoT. L'intenzione di adozione è la misura in cui un utente crede di adottare i servizi IoT. In generale, gli utenti vorrebbero utilizzare i servizi IoT solo se li trovano utili nella vita o nel lavoro. Di conseguenza, ipotizziamo (H3a; H3b; H6):

> ***H3a.*** *I benefici percepiti dei servizi IoT avranno un effetto positivo sull'intenzione all'adozione di servizi IoT*
> ***H3b.*** *I benefici percepiti dei servizi IoT avranno un effetto positivo sull'atteggiamento verso l'adozione dei servizi IoT.*

H5a. *L'atteggiamento verso l'utilizzo dei servizi IoT avrà un effetto positivo sull'adozione di servizi IoT.*

H5b*. I benefici percepiti avranno un effetto positivo sull'atteggiamento verso ed adozione dei servizi IoT in ambito medico-sanitario.*

H5c *La preoccupazione per la privacy delle informazioni dei servizi IoT avrà un effetto negativo sull'atteggiamento verso l'utilizzo ed adozione dei servizi IoT in ambito medico-sanitario.*

Per quel che concerne la CFIP, questa viene presentata sotto diverse sfaccettature: raccolta, uso secondario non autorizzato, accesso improprio ed errori (Smith et., 1996). La "raccolta" riguarda il collezionamento di grandi quantità di informazioni personali da parte dei fornitori di servizi IoT. L'uso secondario non autorizzato è la preoccupazione che le informazioni raccolte per uno scopo possano essere infine utilizzate per altri scopi non autorizzati. L'accesso improprio è definito come la preoccupazione che i dati personali raccolti dai fornitori di servizi IoT siano accessibili alle parti autorizzate. Gli errori comportano la preoccupazione che procedure inadeguate vengano utilizzate per proteggere da errori accidentali o intenzionali nella memorizzazione dei dati personali. In particolare, Stewart e Segars (2002) suggeriscono che il CFIP è più accuratamente modellato come un fattore di secondo ordine piuttosto che quattro fattori correlati del primo ordine. Sostanzialmente, le aziende dovrebbero informare gli utenti su come verranno utilizzate le informazioni raccolte. Tali informazioni consentiranno ai consumatori di formarsi un'idea più accurata sui rischi di divulgazione di dati personali (Harris Interactive & Westin, 1997). Milne e Culnan (2004) hanno suggerito che gli utenti con maggiore preoccupazione per la privacy avranno maggiori probabilità di leggere le informative sulla privacy online rispetto alle persone meno interessate. Ciò suggerisce che il grado di preoccupazione guiderà l'intenzione comportamentale degli utenti. Molti studi hanno verificato empiricamente che il CFIP ha un effetto negativo sull'intenzione comportamentale in una rete nomologica (Angst & Agarwal, 2009; Dinev & Hart, 2006; Malhotra, Kim, & Agarwal, 2004; Zhou & Li, 2014). Di conseguenza, ipotizziamo:

H4a. *La preoccupazione per la privacy delle informazioni dei servizi IoT avrà un effetto negativo sull'intenzione all'adozione verso tali servizi*

H4b. *La preoccupazione per la privacy delle informazioni dei servizi IoT avrà un effetto negativo sull'atteggiamento verso l'utilizzo di tali servizi*

Le relazioni tra la *reward* di servizio su benefici percepiti, atteggiamento e CFIP sono l'aspetto topico dello studio del modello. Queste rappresentano la moderazione inserita all'interno dello studio, elemento caratterizzante di tutta la ricerca. Tramite lo studio della variabile si cercherà di capire se questa ha ed eventualmente in che misura, un effetto positivo sulle variabili sopracitate. Di conseguenza ipotizziamo (H7a; H7b; H7c)

H6a. *L'esposizione alla reward di servizio ha un effetto positivo sui benefici percepiti dall'utilizzo di servizi IoT.*

H6b. *L'esposizione alla reward di servizio ha un effetto positivo sull'atteggiamento verso l'utilizzo di*

servizi IoT.

H6c. *L'esposizione alla reward di servizio ha un effetto positivo sulla concessione alle informazioni personali derivante derivanti dall'utilizzo di servizi IoT.*

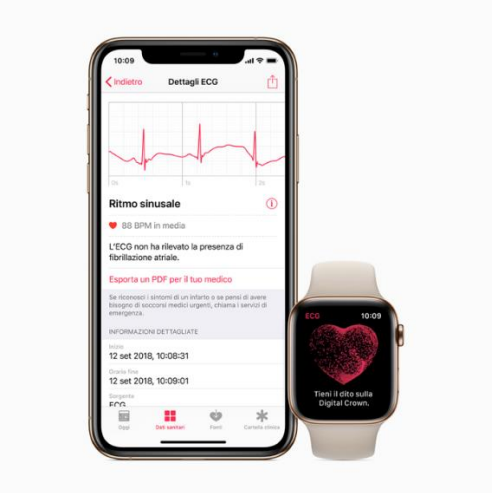
L'impostazione data allo studio permetterà di andare ad esplorare l'effetto di un ulteriore fenomeno all'interno del *framework*. La moderazione inserita sarà in grado di farci capire se una maggiore presa di coscienza del servizio, con una chiara identificazione della sua *utility*, sia un elemento in grado di modificare le scelte del consumatore in merito all'adozione dei sistemi IoT. Ma non solo, rimane molto importante e sentito l'ambito della privacy, dove il moderatore offrendo un servizio "aggiuntivo" ad un dispositivo IoT (ossia la garanzia di prevenzione e monitoraggio sanitario), dovrebbe essere in grado di smorzare se non addirittura invertire l'avversione all'adozione dei sistemi IoT da parte dell'utente. In altre parole, indagherò se, un'esplicitazione chiara della funzione ed utilità associate ad un servizio IoT sanitario, sia in grado di:

- aumentare la propensione a fornire i dati personali da parte dell'utente;
- aumentare i benefici percepiti dal servizio/dispositivo;
- impattare positivamente sull'attitude.

Se così dovesse essere il contributo netto che la ricerca potrebbe dare, sarebbe la dimostrazione che il meccanismo di *reward* della privacy *paradox*, funziona non solo con *reward* di tipo monetario ma anche con *reward* di servizio. Come precedentemente introdotto, partendo dal modello appartenente allo studio di Hsu e Lin (2016), è stata inserita una nuova variabile definita come "*service reward*" con funzione di moderatore. Questa si va a collocare nella parte finale del modello, trovando spazio tra la variabile dipendente "*Adoption to Healtcare IoT System*" e le rispettive variabili indipendenti "*attitude*", CFIP e "*Perceived benefits*". La variabile si compone di due termini chiave che la identificano, tuttavia questi prima di unirsi coniandone il nome, seguono percorsi logici molto differenti tra loro e di diverso contesto. Per chiarire come nascono la variabile ed il suo nome è opportuno partire dalla parola "*reward*". "*Reward*", ossia "ricompensa" è un termine che compare spesso quando si tratta la tematica attinente al paradosso della privacy, infatti la sua provenienza nello studio deriva proprio da quell'ambito. Ci serviamo di questo termine perché la nostra variabile vuole avere questa funzione, ossia quella di ricompensa. Nel paradosso della privacy si parlava di *reward* come lo strumento/mezzo in grado di permettere ai fornitori di servizi IoT di abbattere la barriera di rifiuto verso l'adozione del prodotto, da parte dei consumatori, a causa del trattamento dei dati personali. In parole semplici, il consumatore non vuole che, tramite l'utilizzo del prodotto/servizio, il fornitore ottenga i suoi dati personali, anche se, in cambio di una r*eward* questo si dichiara disposto ad accettare la raccolta e il trattamento dei dati personali. Generalmente negli studi sul paradosso della privacy, la ricompensa in grado di innescare il repentino cambiamento delle preferenze nel consumatore, consisteva in una *reward* prettamente monetaria. Il termine "*reward*" è stato quindi inserito come componente del nome della variabile proprio per via della sua natura funzionale che è esattamente la stessa che vuole avere la variabile moderatrice. Per quel che riguarda invece la parola "*service*" questa fa riferimento al carattere della *reward*. Se come è stato detto precedentemente la *reward* nell'ambito del paradosso della privacy era solita essere di carattere monetario, in

questa circostanza abbiamo voluto cambiare questa sua peculiarità, trasformandola da monetaria a "di servizio". Il motivo per cui la variabile viene caratterizzata in questa maniera è dovuto al fatto che vogliamo andare a capire se un soggetto che non è disponibile a fornire i propri dati personali lo diventa nel momento in cui gli viene fornita una *reward* non più monetaria ma identificata in una garanzia di servizio personalizzato nell'ambito medico/sanitario. Non bisogna dimenticare, infatti, che i dati di cui si parla in questa fase sono quelli strettamente collegati alla sfera della salute di una persona. Quindi la *reward* che l'utente riceve, in cambio dei suoi dati, risulta essere fortemente personalizzata e compatibile. Cosa si intende: a seconda del tipo di problematica che il dispositivo riscontra, l'utente riceverà una *reward* commisurata al problema riscontrato. Avendo quindi così concepito questa variabile, la moderazione è stata inserita nel questionario tramite un'immagine ed una descrizione (Figura 10) ad essa associata in grado di esplicare in maniera chiara e univoca la natura del dispositivo e ponendo l'accento sulle caratteristiche della *reward*.

Figura 10 – Immagine e descrizione con funzione moderatrice



L'immagine raffigura un dispositivo IoT in grado di raccogliere dati in merito alla tua salute e condizione fisica. Adesso immagina che il dispositivo in questione sia in grado di notificare a te ed al tuo medico curante un'anomalia fisica riguardante la patologia maggiormente ti preoccupa, con un preavviso tale da permettere un intervento preventivo in grado di, non solo evitare complicazioni, ma evitare completamente una potenziale situazione critica.

6. Metodologia

Questo studio si basa utilizza come metodologia di ricerca quella denominata: metodo sperimentale. Questo tipo di metodologia si prepone di indagare rapporti di causa-effetto stabilendone la certezza o meno. Il ricercatore deve ricorrere all'ambiente controllato. Il metodo sperimentale permette così di ridurre sensibilmente (se non addirittura eliminare) il rischio che ipotesi alternative minaccino la validità delle conclusioni dell'indagine. Risulta evidente l'implicazione per cui è necessario il completo controllo di un fattore o di una variabile, della quale ne viene supposto il ruolo causale, e il controllo sulla selezione dei soggetti-casi che costituiscono sia il gruppo sperimentale che quello di controllo. Assume, pertanto, la massima importanza selezionare due gruppi identici: il gruppo sperimentale ed il gruppo di controllo. I membri di ciascun gruppo devono verosimilmente essere rappresentativi dello stesso spaccato della popolazione, avere quindi somiglianza rispetto alle variabili conosciute. Il gruppo sperimentale viene sottoposto al "trattamento" ed il gruppo di controllo no. Viene infine monitorato il comportamento e l'effetto che il trattamento ha avuto

sul primo gruppo e confrontato con il comportamento dei componenti del secondo gruppo. I maggiori vantaggi di questo metodo stanno nella capacità di controllo e rigore logico che esso offre.

7. Risultati finali

Il campione di controllo è risultato essere abbastanza equilibrato, nonostante il genere tenda a favore di quello femminile (59,3% femmine e 39,7% maschi), mentre l'età risulta essere fortemente concentrata nelle fasce di età comprese tra 20-24 e 25-29 che, se sommate, coprono il 62,7% del campione. Per quel che concerne la professione, il 42,52% dei rispondenti ha un'occupazione mentre il 45,5% sono studenti, dato che si dimostra in linea con l'età media restituita dal campione (il restante 11,9% rientrano nelle categorie di disoccupati o pensionati). Per quel che riguarda il livello di istruzione del campione il 54,4% ha conseguito almeno una laurea di primo livello, il 33,5% possiede un diploma di istituto superiore e solo il 6,7% non va oltre la terza media. Risulta interessante notare come, nonostante la maggioranza del campione abbia ammesso di non avere familiarità con il concetto di IoT (62,7% no contro il 37,3% si), quasi la totalità si è dichiarata "abbastanza" (29,1%) o "molto" (63,4%) preoccupata in merito alla tutela dei dati personali raggiungendo un totale pari al 92,5% del campione. Sono stati rilevati dati analoghi anche quando la domanda è stata posta in maniera specifica verso la tutela dei dati contenenti informazioni sulla propria salute con una copertura quasi totale del campione (91%) dettata nuovamente da "abbastanza" (23,1%) e "molto" (63,4%). Le patologie che si sono rivelate essere le principali cause di preoccupazioni nei rispondenti vedono in primis le complicazioni di natura cardiovascolare con quasi la metà del campione pari al 41%, seguite da altre complicazioni di varia natura equivalenti al 38%. I rispondenti hanno inoltre messo in luce come le motivazioni di tali preoccupazioni siano dovute alla conoscenza di queste patologie ma senza che ve ne sia mai stato un reale interessamento a livello di storia clinica da parte loro (55,2%). Infine, il 78% dei rispondenti si è dichiarato favorevole a spendere in una fascia compresa tra gli 0 ed i 300€ per usufruire di un servizio IoT a carattere sanitario.

Ipotesi di ricerca		**t1**	**t2**	**Coeff**	**Coeff 2**	**Risultato**
H1:	*Pc -> Pb*	6.32		0.63		Confermato
H2:	*Py -> Pb*	14.20		0.52		Confermato
H3a:	*Pb -> Adopt*	10.16		0.64		Confermato
H3b:	*Pb -> Att*	10.53		0.64		Confermato
H4a:	*CFIP-> Adopt*	-0.94		-0.10		Non Confermato
H4b	*CFIP -> Att*	1.39		0.14		Non Confermato
H5a:	*Att -> Adopt*	11.58		0.61		Confermato
H5b:	*Pb + Att -> Adopt*	5.58	7.18	0.38	0.42	Confermato
H5c:	*CFIP + att -> Adopt*	-2.12	11.71	-0.19	0.62	Non Confermato
H6a:	*Pb + mod -> Adopt*	10.48	3.75	0.65	0.32	Confermato
H6b:	*CFIP + mod -> Adopt*	-1	3.03	-0.1	0.32	Non Confermato
H6c:	*Att + mod -> Adopt*	11.93	3.79	0.61	0.32	Confermato

Giunti alla fine dello studio procediamo con un'analisi complessiva dei risultati ottenuti, sia da un lato prettamente empirico sia da quello economico-manageriale. L'intenzione di questa sezione è pertanto quella di andare a capire cosa si cela oltre il semplice numero, quello che è comunemente noto come *insight*. Verranno

brevemente riproposti gli obbiettivi dello studio e si cercherà di dare, attraverso i dati empirici ottenuti, un significato non solo teorico ma anche realmente applicabile alle dinamiche di mercato. Delle 12 ipotesi formulate, 4 non sono state confermate, tutte riguardanti il ramo inerente alla privacy. Con grande rammarico per questo risultato, non sarà possibile generare alcun tipo di implicazione che riguardi la parte sulla privacy, tanto meno il paradosso della privacy. In linea di massima però, possiamo ritenerci sufficientemente soddisfatti della parte restante del modello studiato. Questo è dovuto al fatto che le altre ipotesi sono state confermate con risultati, in termini di significatività dei modelli, eccellenti. In alcuni casi si è arrivati a registrare dei valori per gli *R-squared* che rasentano il 50%, risultato da ritenersi di spessore statistico. Partendo dal modello originale l'introduzione della variabile moderatrice *service reward* è stata accolta in maniera positiva: 2 delle 3 ipotesi che la riguardavano sono state confermate e l'unica a non esserlo riguardava la privacy. La causa per cui questa non è stata confermata non è da imputarsi al moderatore, che altrimenti non avrebbe funzionato neanche per le altre ipotesi, ma alla mancanza di significatività del *main effect* che andava a moderare. Dopo questo appunto sulla variabile inserita si vuole procedere con ordine andando a commentare le ipotesi alla base del modello. In primis ci interfacciamo con le esternalità di rete indirette composte dalla *perceived compatibility* (*H1*) e *perceived complementarity* (*H2*). Questo blocco delle esternalità di rete non era stato volutamente escluso in quanto risultava essere uno degli aspetti che il modello originale aveva evidenziato come estremamente rilevante per l'influenza esercitata sui benefici percepiti. Per lo studio condotto, le domande utili alla misurazione dei costrutti erano state modificate ad *hoc*, quindi indirizzate a sottintendere una compatibilità e complementarità di servizi IoT a livello medico-sanitario. In base ai risultati conseguiti è possibile affermare che, anche per dispositivi in grado di impattare più o meno direttamente la salute di un utente, la compatibilità e la complementarità dei servizi IoT sono risultati essere elementi molto importanti ai fini dell'aumento dei benefici percepiti. (Appendice 1-2)

Sulla stessa verticale nel modello incontriamo le variabili che andranno a comporre la variabile CFIP "*Concern For Information privacy"*, queste sono: *collection*, *unauthorized secondary use*, *improper access* e *errors*. Per quanto riguarda queste variabili non sono state formulate ipotesi per via del fatto che la costruzione della CFIP attraverso queste variabili risultava essere molto complessa e diversa da qualsiasi altra variabile sin ora studiata; costruzione che di fatto non siamo riusciti a replicare, tematica che verrà approfondita nella sezione seguente 3.7.

Entriamo finalmente nel vivo della ricerca andando a verificare i *main effect* delle variabili *perceived benefits* (*H3a*) e *CFIP* (*H4a*) verso la variabile dipendente *Adoption to Healthcare system* ma anche dell'effetto di mediazione condotto dalla variabile *attitude (H5/a/b/c*), il tutto letto in un'ottima pre e post moderazione. La variabile dei benefici percepiti ha risposto in maniera coerente con quanto ci si aspettasse. Oltre ad essere risultata significativa all'interno del modello, ha dimostrato possedere un effetto positivo sull'adozione dei sistemi IoT sanitari da parte dei consumatori (Appendice 3). Questo effetto si è dimostrato ancora più accentuato a seguito dell'introduzione del moderatore. Infatti, confrontando i beta di regressione del modello senza moderatore con quelli del modello moderato si può notare come la variabile *service reward* sia stata in

grado di aumentare la propensione all'adozione dei servizi IoT in ambito sanitario dei rispondenti (Appendice 10). Questo significa che chi è stato esposto ad uno stimolo informativo maggiore ha risposto positivamente ad esso. Ricordiamo che la variabile moderatrice consisteva sostanzialmente in un'immagine di tipo informativo, con lo scopo di far immedesimare il rispondente in una situazione quanto più realistica e a lui familiare possibile. Visti i risultati si può supporre che quindi una maggiore conoscenza del servizio IoT sanitario possa effettivamente garantire una maggiore propensione all'adozione di questi servizi. La variabile *CFIP*, creata tramite un'analisi fattoriale sulle 4 variabili della privacy del modello, nonostante abbia conseguito ottimi risultati in fase di pre-test, non è risultata essere significativa verso *adoption healthcare IoT system* (Appendice 5). Questo significa che è stato impossibile verificarne alcun tipo di relazione tra la variabile indipendente e quella dipendente (*H4a*). In tal caso non siamo in grado di compiere nessuna assunzione in merito. Ovviamente, data la circostanza, perdiamo anche l'ipotesi moderatrice (*H6c)* andando essa ad agire su una relazione, di fatto, inesistente (Appendice 12). Prima di verificare l'effetto che la variabile *attitude* ha in via esclusiva sulla variabile dipendente (*H5a*) ci occuperemo di commentare le relazioni che questa ha con i benefici percepiti (*H3b*) e la CFIP (*H4b*). Per quel che riguarda la relazione tra *perceived benefits* ed *attitude* possiamo dire che l'ipotesi viene confermata e che quindi la percezione positiva di un servizio IoT di tipo medico si riflette in un aumento dell'atteggiamento che l'utilizzatore ha verso il dispositivo (Appendice 4). Questo risulta essere abbastanza plausibile anche a livello logico, in quanto una maggiore utilità percepita è normale sfoci in un atteggiamento maggiormente positivo dell'utilizzatore verso il prodotto. Anche in questo caso non è stato possibile identificare alcuna relazione statistica significativa tra la variabile *CFIP* ed *attitude* (*H4b*) (Appendice 6). Vista anche la mancata relazione tra queste due variabili risulta inutile soffermarsi sull'ipotesi che vedeva coinvolte la *CFIP* e l'*attitude* in maniera congiunta sull'adozione dei sistemi IoT sanitari (*H5c*), decisione che risulta essere confermata anche dai dati (Appendice 9). Verifichiamo adesso l'effetto della variabile *attitude* direttamente sulla variabile dipendente (*H5a*). Questa è risultata essere confermata dai dati in maniera significativa (Appendice 7). Possiamo quindi asserire che un atteggiamento positivo verso i dispositivi IoT da parte del consumatore è in grado veicolarlo in maniera più efficace verso l'adozione dei servizi. Se confrontiamo i risultati dell'ipotesi appena citata con quelli dell'ipotesi affetta da moderazione (*H6b*) potremo notare come i risultati ottenuti differiscano (Appendice 11). Come era accaduto per la moderazione sul *main effect* "benefici vs adozione" lo stesso si verifica in questa circostanza. Infatti, l'atteggiamento subisce un sostanziale aumento dovuto all'effetto della *service reward*. In questo caso però l'implicazione che ci si sente di fornire non riguarda più solamente l'aumento di utilità percepita dovuta ad una immedesimazione del rispondente in una circostanza ben definita, ma, trattandosi dell'atteggiamento, si potrebbe essere portati a pensare che l'effetto positivo scaturito derivi dalla capacità di comprensione del messaggio grazie alla sua chiarezza ed immediatezza. L'effetto congiunto generato dai *percieved benefits* e *attitude* verso *adoption to healthcare IoT system* è risultato essere significativo è complessivamente positivo. In breve, si è potuto vedere come l'effetto combinato di queste variabili sia in grado di aumentare significativamente l'adozione dei sistemi IoT (Appendice 8). Si può quindi suppore che i benefici percepiti

risultano giocare un ruolo chiave in quanto influenzano, seppure in parte, l'atteggiamento il quale dimostra avere (se preso singolarmente) un coefficiente beta minore rispetto a quello dei benefici sulla variabile dipendente ma anche un *R-squared* maggiore e quindi maggiormente esplicativo della varianza di essa (Appendice 3 vs Appendice 7).

Dopo aver riassunto i risultati con qualche spunto di riflessione, si cercherà di realizzare una visione d'insieme degli elementi, sperando di fornire qualche assunzione di tipo manageriale che possa essere utile nel concreto. Nonostante uno degli obbiettivi principali di questa ricerca non sia stato confermato, ossia la dimostrazione che una *reward* di servizio potesse essere in grado di attenuare l'effetto di rifiuto all'adozione di sistemi IoT a causa dell'eccessiva raccolta di dati, siamo comunque in grado di portare un modello che potenzialmente può ancora dirci qualcosa. Se dividiamo il *framework* di riferimento sull'asse orizzontale potremo analizzarlo in due emisferi, quello superiore, ipotesi confermate, e quello inferiore, ipotesi non confermate. Per questo motivo saremo in grado di analizzare solo la parte superiore. Cercando di inquadrare i risultati ottenuti in un'ottica più generale possibile, possiamo dire che abbiamo individuato un nuovo elemento in grado di favorire l'adozione ai sistemi IoT. Sostanzialmente il modello non è altro che un piccolo frammento della fase definibile come *attraction* all'interno della *customer journey*. Per dirla semplicemente, partendo dal modello di Hsu & Lin 2016, abbiamo studiato quali elementi un servizio IoT deve avere o garantire affinchè questo venga "adottato". Per usare un sinonimo un po' più tecnico si potrebbe dire che questo *framework* mette in mostra come potrebbe essere possibile favorire il *first trial* di un dispositivo IoT dedicato ai servizi medici sanitari da parte di un consumatore. Questo era quello che il modello di base già era in grado di dire. Quello che siamo riusciti ad aggiungere con il nostro moderatore è un tassello che precedentemente non era stato considerato: l'esposizione informativa chiara e immediata. Ricordando nuovamente che il moderatore inserito si configurava come un'immagine a scopo informativo, ne sono stati successivamente misurati gli effetti, che oltre ad esser risultati significativamente statistici hanno messo in mostra come questo tipo di variabile generi un effetto positivo sull'adozione dei sistemi IoT. L'informazione finale che si evince, in un'ottica imprenditoriale, potrebbe riguardare i seguenti aspetti.

Al fine di favorire l'adozione dei servizi IoT nonché il *first trial* e di conseguenza le vendite, il dispositivo/prodotto deve essere compatibile, rispecchiando ciò che il consumatore vuole, risultato ottenibile grazie ad un alto livello di personalizzazione, ma anche complementare, ovvero dispositivi in grado di comunicare tra di loro, abbattendo le eventuali barriere dovute a sistemi operativi diversi. La componente utilitaristica risulta essere fondamentale ed anche la formazione di un atteggiamento da parte del consumatore gioca un ruolo cruciale. Essendo queste due caratteristiche elementi non prettamente tecnici, ossia che non si possono aumentare o decidere in maniera operativa durante il processo in filiera produttiva (e ci si riferisce in particolar modo alla formazione dell'atteggiamento del consumatore verso un prodotto/servizio), ecco che risulta cruciale la variabile *service reward*. Questa potrebbe effettivamente diventare un elemento importante tramite il quale formare l'atteggiamento dei consumatori verso un prodotto. Quindi attraverso l'esposizione

informativa del servizio ed una comunicazione chiara e immediata si può andare a pensare di intaccare in maniera importante la fase di *attraction* dei consumatori.

8. Limiti della ricerca e prospettive future

Il limite principale di questa ricerca riguarda il non esser stati in grado di confermare le ipotesi sulla privacy andando a perdere una parte corposa dello studio. La motivazione principale è da ricercarsi nella creazione della variabile CFIP. Questa è stata definita come una variabile autoriflessiva di secondo ordine, mentre in questo studio è stata generata semplicemente attraverso un'analisi multifattoriale inclusiva delle variabili *collection, unauthorized secondary use, improper access, errors*. Purtroppo, nonostante la fase di pre-test con le alpha di Cronbach dimostrassero una buona *reliability*, questa non è stata sufficiente a far si che la variabile risultasse significativa nel modello per nessuna delle ipotesi formulate (*H4a*, *H4b*, *H5c*). Sicuramente uno spunto per eventuali ricerche future riguarda proprio il prestare maggiore attenzione alla costruzione di questo costrutto, che se ben generato, può effettivamente dare un grande contributo alle implicazioni finali offerte dalla ricerca. Per quando riguarda invece l'evoluzione del modello proponiamo due possibili strade:

- continuare l'arricchimento del *framework* attraverso nuove variabili e cercando di rendere sempre più completo il mosaico che porta all'adozione di sistemi IoT in ambito sanitario.
- Andare oltre lo step dell'*attraction* concentrandosi sulla fase di retention, ossia studiare quali meccanismi siano in grado di far mantenere costante nel tempo l'utilizzo di dispositivi IoT.

La prima strada aiuterebbe lo studio del fenomeno e, se fatta a distanza di anni, a fattori costanti, potrebbe permettere di capire come i bisogni dei consumatori si evolvano nel tempo. La seconda invece, consentirebbe di ottenere, infine, una visione continua del consumatore, intesa come un percorso che si articola nelle fasi basilari di *attraction*, *retention* ed *evolution*.