Dipartimento di Impresa e Management Cattedra: Analisi del Comportamento d'acquisto

Data Privacy nel Marketing: Un' Analisi Esplorativa

RELATORE

Prof.Ssa Romani Simona

CANDIDATO
Viligiardi Tommaso

MATR.
682611

CORRELATORE

PROF. Donato Carmela

ANNO ACCADEMICO 2017 / 2018

INDICE

CAPITOLO 3. LA RICERCA ESPLORATIVA: LA RELAZIONE TRA FATTORI DI COMMUNITY, MOTIVI TECNICI E PREOCCUPAZIONI LEGATE ALLA PRIVACY

INTRODUZIONE

Uno dei temi più caldi nel marketing attuale è quello della self – disclosure dei dati personali. Soprattutto a seguito del recente scandalo che ha coinvolto Facebook ed il suo creatore, mai come oggi il tema in questione è considerato estremamente attuale.
Sempre più individui si dichiarano preoccupati sulla diffusione e soprattutto sugli usi che le aziende fanno dei loro dati, e naturalmente allo stesso tempo i soggetti di business sono sempre più interessanti alla raccolta di questi dati sensibili. I dati sensibili sono quei dati personali che riguardano la sfera più intima dell'individuo e, pertanto, necessitano di una speciale protezione. Nell'era del digitale la tutela della privacy è divenuto uno degli obiettivi più importanti da raggiungere. Riprese in pubblico, fotografie, abbonamenti a riviste, iscrizioni a piattaforme online: tutto viaggia velocemente nella rete, rendendo di dominio pubblico (o quasi) i dati personali. Per porre un argine alla diffusione esagerata delle informazioni, la legge italiana ha previsto che alcune di esse possano essere trattate solamente con il consenso espresso dell'interessato ovvero con l'autorizzazione preventiva del Garante della privacy. Si tratta dei cosiddetti dati sensibili. Questi sono dei particolari dati personali che, per la loro delicatezza, necessitano di una disciplina particolare. Nello specifico con l'espressione "Dati Sensibili", vediamo che questi si inseriscono all'interno dei dati personali, i dati sensibili sono quelli che rivelano l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale. I dati sensibili sono soggetti, per la loro delicatezza, ad un particolare trattamento giuridico.
Come dicevo questi dati vengono bramati sempre di più dalle aziende, in quanto è comunemente riconosciuto che riuscire a raccoglierli in grandi quantità, porta grandi benefici, in quanto permette di ideare e produrre prodotti e servizi fatti su misura per un certo target di consumatori.
Questi benefici non sono solo per le aziende, in quanto ricevendo offerte fatte su misure, anche i consumatori ricevono determinati vantaggi. Proprio per questa ragione, a prescindere dalle preoccupazioni e dai rischi che il rilascio dei dati personali comporta, i consumatori sono spesso portati a passare oltre, decidendo quindi di fornire a terze parti i propri dati.
L'obiettivo di questa ricerca è quindi quelli di indagare a fondo su questo argomento tentando di individuare quali sono quei fattori (Anche detti fattori facilitatori) che spingono gli individui a svelare i propri dati.
Questi fattori saranno indagati tramite un enorme lavoro, volto a capire in primis il contesto di riferimento e tutto ciò che gli ruota intorno, per arrivare al risultato finale di riuscire a formulare una domanda di ricerca che poi andremo ad analizzare ed a verificare o smentire, tramite l'analisi dei dati.
Quindi, dopo un primo capitolo che sarà necessario a dare un'infarinatura generale sul tema, in cui verrà principalmente visto il significato che oggi viene attribuito alla privacy, le normative in vigore ed i soggetti che

sono interessati ai suoi sviluppi, nel secondo capitolo affronteremo nello specifico i temi che sono stati maggiormente toccati negli ultimi anni. Saranno qua enunciate le principali teorie economiche, la dicotomia che esiste tra i gli atteggiamenti dichiarati ed i comportamenti effettivamente messi in atto dai consumatori, ed in particolare vedremo l'analisi costi – benefici che spinge gli individui a prendere determinate decisioni.
Infine, sempre nel secondo capitolo vedremo quali sono quei fattori attualmente riconosciuti dagli esperti, come importanti per la maggior parte degli individui, per negoziare i propri dati sensibili. In particolare i fattori che vedremo sono: fiducia, personalizzazione e controllo.
Infine nell'ultimo capitolo sarà presentata la nostra ricerca: di questa verranno presentati tutti gli step, partendo da come ci siamo avvicinati a questo tema, gli obiettivi che avevamo, la metodologia utilizzata, che vedremo essere formata da due fasi, la raccolta e la lettura dei dati ed, infine, la stesura dei risultati che abbiamo ottenuto in questo lungo percorso

1. IL RUOLO DELLA PRIVACY NELLO SCENARIO ATTUALE

1.1 Overview sulla Privacy

In questo primo capitolo della mia tesi di laurea, voglio andare a presentare a linee generali l'argomento di interesse che ho scelto, il perché, e quindi l'importanza che questo ricopre nello scenario e nell' epoca in cui viviamo, e ultimo, ma non per importanza, quali sono i soggetti che ne sono coinvolti.
Mai come negli ultimi decenni il tema del self – disclosure di dati ed informazioni sensibili è rilevante ed attuale. Con il concetto di "Dati sensibili" intendiamo "categorie speciali di dati che includono dati personali in grado di rivelare le origini raziali, opinioni politiche o religiose, senza dimenticarci di questi dati personali sulla salute, la vita sessuale e sui precedenti criminali di un determinato individuo" (King & Raja., 2012).
Alcuni stati membri dell'Unione Europea hanno recentemente esteso la protezione speciale ad altre categorie di informazioni personali, che vanno a considerare sensibili dati come debiti personali, situazioni finanziarie o il pagamento di certi benefits legati a sistemi di welfare.
In generale le aziende non possono raccogliere, immagazzinare o processare queste categorie speciali di dati dei propri clienti o dei propri impiegati, a meno che questi non abbiano dato un esplicito consenso sul trattamento di queste informazioni.
Le aziende devono anche esplicitare il trattamento preciso che faranno di questi dati che sono stati raccolti.
Il trattamento di dati sulla geo-localizzazione, che sarà uno dei punti focali di questa tesi, è appropriato inserirli all'interno delle categorie speciali (Seppur questo non è ancora stato fatto a livello teorico dal legislatore) in quanto questi sistemi rivelano la location fisica degli users che utilizzano questi sistemi. Questo tema acquista sempre più importanza e causa molte preoccupazioni e timori negli individui in quanto quotidianamente essi convivono con dispositivi che sono facilmente rintracciabili a causa del GPS a di altre tecnologie collegate a questi apparecchi.

In definitiva, almeno per ciò che riguarda la legislazione dell'Unione europea, definire ciò che sono i dati sensibili, va oltre le definizioni di categorie speciali di dati, ma dobbiamo identificare informazioni personali meritevoli di avere la giusta protezione, così da assicurare un giusto grado di debolezza per i cittadini.

Con l'avvento, e soprattutto con l'affermarsi di Internet (e successivamente dei social networks) come strumento sempre più presente nella nostra vita quotidiana, il concetto di privacy è sensibilmente e rapidamente cambiato rispetto al passato.

Ma cos'è la privacy? I significati espressi con questa parola sono molteplici e molto dipende dal contesto di riferimento in cui è collocato. Se ad esempio prendiamo come riferimento il contesto legale, qua la privacy è ampiamente sinonimo di "Il diritto di essere lasciati soli" (Warren e Brandeis 1890).

Nel 1965, la Corte Suprema degli Stati Uniti d'America ha descritto il concetto di privacy come un diritto fondamentale, costituito da due componenti. La prima è l'interesse individuale nell'evitare la concessione di informazioni su questioni personali di interesse. La seconda componente riguardava invece l'interesse individuale sulla possibilità di essere indipendenti nel poter prendere certi tipi di decisioni personali (Griswold, 1965). Nel 1977, la stessa Corte Suprema, descrive l privacy come "includere il diritto degli individui di essere liberi nei propri affari privati dalla sorveglianza e dall'intrusione del Governo ed il diritto di un individuo di far sì che i propri affari non siano resi pubblici dagli enti governativi (Whalen v. Roe, 1977). Quello che però forse ci interessa di più per il nostro scopo, è quello che molti altri studiosi sostengono, ovvero come la privacy sia più semplicemente il diritto di proteggere la disclosure delle informazioni personali. Molti altri ancora, come ad esempio (Parent, 1983) sostiene la tesi che ancora non è emerso un concetto univoco riguardo la privacy. La contestuale natura della privacy è evidente dato il fatto che i concetti possono cambiare a seconda dell'ambiente e dei fattori personali, per cui questo desiderio innato sulla privacy, è un qualcosa estremamente dinamico. Le persone sono continuamente impegnate in un processo di adeguamento in cui i desideri per la privacy sono soppesati dai desideri di divulgazione e comunicazione personale con gli altri (Kimmel, 1996). L'aggiustamento avviene nel contesto di varie forze situazionali, come pressioni da parte di altri, norme sociali e processi di sorveglianza utilizzati per rafforzarle (Kimmel, 1996). Hoffman invece definisce la privacy informativa con tre diritti distinti.

Il primo è il diritto degli individui di determinare quali informazioni su loro stessi possono essere condivisi con gli altri. Il secondo riguarda il diritto ad essere informati cosà è stato raccolto su di loro.

L'ultimo invece riguarda il diritto degli individui di accedere alle informazioni riguardanti i propri dati.

Comunque sia, l'unica cosa certa è sicuramente il fatto che le questioni legate alla privacy sono ritenute estremamente importanti sia per gli individui che per la società moderna, per non parlare del contesto legale, in cui mai come oggi interventi dei legislatori e regolamenti sulla questione sono ben auspicati da tutte le risorse toccate dal tema. Un' enorme quantità di dati ed informazioni vengono rivelati ogni giorno all' interno del mondo digitale, comportando che diversi scenari si aprono a contorno di questo tema, andando a farcire di grandi attenzioni e ricerche degli esperti sulla questione. Come spesso accade, la tecnologia è in qualche modo

un'arma a doppio taglio. Sebbene possa migliorare le nostre vite in molti modi, poiché il nostro mondo diventa una "società dell'informazione", solleva anche nuove preoccupazioni. Per gran parte di queste informazioni si riferisce non solo alle cose ma alle persone. Le informazioni su di noi sono accessibili, archiviate, manipolate, estratte dai dati, condivise, acquistate e vendute, analizzate e potenzialmente perse, rubate o utilizzate da innumerevoli agenzie governative, aziendali, pubbliche e private, spesso senza la nostra conoscenza o il nostro consenso.

Gli sforzi di molti studiosi sono convogliati su questo tema, ed in particolare vediamo come a partire dagli anni ’90 molto materiale è stato prodotto sulla relazione che si è andata a creare sulla self-disclosure ed Internet. Per riportare qualche esempio su ciò che ho appena detto, possiamo prendere in considerazione la ricerca di Parks & Floyd (1996) i quali sono andati ad indagare sulle relazioni che si creano tra gli utenti di Internet. I risultati di questo studio ci dicono che sono stati riscontrati comportamenti di maggiore apertura all’interno dei confini del mondo digitale, piuttosto che nella vita reale.

Ancora di maggiore interesse per quello che poi vedremo sarà il tema focale di indagine della mia tesi di laurea, la ricerca condotta da Chesney (2005) riporta livelli nettamente più alti per ciò che riguarda la self-disclosure di informazioni sensibili. Il 59% dei partecipanti a questo studio, dichiarano che non avrebbero mai rivelato in alcun modo lo stesso tipo di informazioni nella vita reale.

Con riferimento ai 2 studi appena citati, uno degli effetti che causa i maggiori livelli di self – disclosure all’interno di Internet, è senza dubbio l’effetto psicologico dell’anonimato.

Da un punto di vista quindi strettamente psicologico, la capacità che Internet concede a tutti noi, ovvero quello di poter accedere a migliaia di comunità, con la possibilità di nascondere la nostra vera identità, viene spesso considerato come un importante input che spinge gli individui ad una maggiore apertura per ciò che abbraccia la sfera di dati ed informazioni personali.

Nel corso degli anni, allo stesso tempo si sono venuti a creare, come ho accennato in precedenza, un grande numero di temi che sono legati a quello principale dell’apertura di informazioni personali all’interno del mondo virtuale. Uno di quelli che senza ombra di dubbio sembra essere più interessante sia per gli individui che per gli studiosi, è quello che copre i vari aspetti relativi alla sfera del Privacy Concerns e quindi del paradosso che si viene a creare con l’effettivo comportamento di quanto detto fino a questo momento.

Come già è stato verificato da una grande quantità di recenti sul tema del comportamento online, notiamo importanti discrepanze tra l’attitudine degli users ed il loro effettivo comportamento quando si trovano su questo tipo di piattaforme.

Analizzando quanto appena detto più nel dettaglio, vediamo che mentre spesso gli users dichiarano di essere estremamente preoccupati e sensibili circa le questioni inerenti alla loro privacy, gli stessi fanno veramente poco per proteggere i loro dati. Infatti, se ad esempio guardiamo al grande numero di App mobili, che poi saranno anche il punto focale su cui ci concentreremo nel corso di questo studio, vediamo che per le scelte dei consumatori nell’uso di queste App, gli users sono principalmente guidati dalla considerazione di popolarità, la

usability ed il prezzo (Kelly, 2013). Constatiamo quindi che la privacy non è all'interno dei primi 3 driver che guidano il consumatore nel loro comportamento e nelle loro scelte.
Vediamo per prima cosa, il senso che viene dato all'espressione self – disclosure, grazie alle definizioni che sono state definite da alcuni esperti del settore.
"Self – disclosure è la quantità (ampiezza) e la qualità (profondità) delle informazioni personali che un individuo fornisce ad un altro" (Jourard, 1971).
"Sono state condotte numerose ricerche sul tema della "self – disclosure. In generale queste hanno adottato una prospettiva teorica di scambio sociale (Ajzen, 1977), suggerendoci che la self – disclosure, come qualunque altro comportamento interpersonale, viene approcciato ed interpretato in termini di relazione costo – beneficio dagli individui (Moon 2000).
Sappiamo infatti che al giorno d'oggi riscontriamo un'enorme domanda per disseminare e condividere dati specifici su gli individui per nuovi ed eccitanti usi. Come appunto stavo dicendo, con l'ultima rivoluzione tecnologica, la stragrande maggioranza di questi dati sono disponibili elettronicamente. Gli individui sono sempre spinti a condividere il loro capitale sociale grazie alla miriade di innovazioni tecnologiche che sono ancora in atto. La tensione che però esiste tra il desiderio dei consumatori di comunicare onilne e le preoccupazioni che sorgono su come i dati che rilasciano verranno trattati, esisteva già prima del boom dei social network. Basti pensare anche allo scandalo sotto gli occhi di tutti, che ha colpito Facebook, il colosso dei social network. Questi strumenti vengono percepiti dalla società come fornitori di nuovi benefits, ma sono una grande fonte di dati caricati, immagazzinati e condivisi. (Hallam e Zanella, 2017).
I tipi di informazioni più distintivi e chiaramente anche quelli che spesso suscitano maggior interesse, e di conseguenza provocano maggiori negli individui per rilasciarle all'interno del web e non solo) sono ad esempio il a) nome, b) Codice fiscale e c) data di nascita.
Ma perché oggi il tema delle rivelazioni di dati personali e specifici è considerato così importante e centrale dagli esperti? È riconosciuto oramai globalmente, che le compagnie ed organizzazioni hanno un estremo bisogno di collezionare questo tipo di dati per far sì di raggiungere un vantaggio competitivo significativo verso i propri principali competitors e, di conseguenza, per far crescere il proprio business.
Il rilascio di queste informazioni permette a questi players di sfruttare le grandi opportunità che offre il web. Per fare un esempio in merito a quello che sto dicendo, che però non è l'unico, un benefit importantissimo che Internet mette in mano alle aziende, è proprio quello di poter personalizzare le comunicazioni da intraprendere con consumatori individuali. Per far sì che ciò sia possibile dobbiamo proprio ritornare alla nostra questione primaria: il rilascio di informazioni e dati da parte degli individui.
Oltre agli atteggiamenti e alle preoccupazioni sulla privacy, è importante considerare i comportamenti che le persone possono adottare per salvaguardare la loro privacy. Ad esempio, avete mai fornito informazioni personali false o incomplete al momento della registrazione su un sito Web, piuttosto che fornire il vero nome e

indirizzo? Probabilmente la maggior parte delle persone risponderebbe di si. È probabile che ci sia una relazione complessa tra atteggiamento e comportamento in questo contesto.

1.2 Privacy concerns

Come detto, le aziende possono sì effettuare comunicazioni personalizzate, ma prima di questo devono essere sufficientemente abili nel collezionare ed immagazzinare in appositi Database, i bisogni e le preferenze dei singoli individui (Sheehan e Hoy 2000).
Qual è però la difficoltà che le aziende incontrano ad intraprendere questo processo, che permetterebbe loro grandi passi avanti? Facciamo però prima un piccolo passo indietro per capire meglio il contesto in cui ci stiamo muovendo; cosa intendiamo davvero con l'espressione Privacy Concerns? È davvero possibile dare una definizione univoca? Le preoccupazioni e remore che i consumatori hanno circa concedere dati sensibili circa la propria sfera personale ed intima sta crescendo parallelamente alla presa di coscienza (sempre più elevata) che queste informazioni sul loro comportamento online, viene stockato dalle aziende a prescindere dalla conoscenza e, in particolare, il permesso degli stessi individui.
È stato rilevato che esiste un crescente grado di preoccupazione e disagio nella popolazione circa gli usi commerciali dei dati privati. Una politica regolatori disinformata in materia di privacy può causare perdite significative in termini di welfare, quindi il modo in cui le persone valutano la propria privacy è centrale sia a livello economico, sia a livello governativo.
Sono molti gli studi empirici esistenti che portano a tali valutazioni sulla protezione della privacy, che però, suggeriscono risultati molto diversi.
Da un lato, alcuni studi suggeriscono che una vasta maggioranza della popolazione è fortemente preoccupata per i propri dati personali, con fino il 90% dei partecipanti che negano categoricamente la volontà di vendere dati personali per uso commerciale. Inoltre, i partecipanti che sono d'accordo in cambio di un compenso fanno richieste piuttosto elevate (Acquisti e Grossklags, 2005) che sono molto lontane dal valore reale o dal prezzo di mercato di tali dati. Dall'altro lato, alcuni studi sul campo incentivati indicano viceversa che sono molto pochi i partecipanti che sarebbero realmente disposti a pagare anche piccole somme di denaro in cambio di una migliore tutela della privacy, ricevendo così un beneficio dal lato della propria sfera personale (Beresford, 2012).
Come le aziende espandono i loro sforzi per raccogliere ed usare i dati dei consumatori, anche le preoccupazioni di quest'ultimi verso la loro privacy cresce di pari passo.
Quando un soggetto economico raccoglie, immagazzina ed usa delle informazioni personali, cresce il potenziale di danno, e quindi la sensazione di vulnerabilità nei consumatori.

La maggior parte degli effetti negativi dei clienti derivanti dall'uso dei dati derivano quindi dall'ansia dei clienti circa il potenziale di danno o dai sentimenti di violazione, piuttosto che dall'effettivo utilizzo improprio dei dati che ne fanno le aziende o il danno finanziario o di reputazione (Scharf, 2017).
Questo senso di vulnerabilità dei clienti genera risultati negativi per le aziende a causa del comportamento messo in pratica dagli users. Molteplici sono state le misurazioni relative alla privacy che sono state avanzate nel corso degli anni, ed è stato tentato di incrociarle insieme a una varietà di fattori e risultati ritenuti di interesse. Un supporto importante dagli studi è quello che il concetto di privacy è stato classificato come la principale preoccupazione dagli utenti su Internet (Kehoe, 1998). L'81% degli adulti negli Stati Uniti hanno dichiarato recentemente di essere particolarmente preoccupati riguardo la loro privacy online. L'altro lato della medaglia riguarda però il fatto che, nonostante le preoccupazioni sulla protezione della loro privacy, che gli individui dichiarano di avere, queste vanno frequentemente in contraddizione con i comportamenti che mettono in atto e con le aspettative che hanno sulle questioni legate alla privacy. Questo infatti viene comunemente riconosciuto dagli esperti e studio come il concetto di Privacy Paradox. E proprio questo sarà uno dei temi focali nella ricerca che questa tesi intende andare ad investigare, ma lo vedremo principalmente nel capitolo successivo.
Come vediamo, o almeno possiamo intuire da queste prime righe della ricerca, il tema in cui ci stiamo addentrando è molto più ampio di quello che potremmo pensare a prima vista, e soprattutto ricopre una grande importanza nella società in cui viviamo. In più i risvolti che questo comporta sono molteplici, e non è solo un argomento di discussione che interessa le aziende o il mondo del business più in generale, ma come vedremo successivamente, sono molti i soggetti interessati alle dinamiche di rilascio delle informazioni e sulle conseguenze che questa cosa potrebbe portare.
Ritornando però per il momento sul soggetto Azienda, quali sono le azioni che questa potrebbe intraprendere per superare le preoccupazioni degli individui di cui stavamo parlando nei paragrafi precedenti? La maggior parte degli studi realizzati sul tema del Self – disclosure, ci suggeriscono che la disponibilità dei consumatori aumenta in base alla loro personale concezione, e dell'importanza che gli danno, della relazione che esiste tra il concetto di costo e quello di beneficio. Proprio a seguito di questo le aziende che hanno interazioni costanti con i consumatori si trovano a mettere in atto una serie di approcci per alterare la relazione in esame, e quindi incoraggiare il consumatore ad aprirsi nei confronti dell'azienda (o chi per essa).
Per dare qualche esempio reale di ciò che sto dicendo, alcune compagnie aumentano le probabilità di ottenere questi dati ed informazioni di estrema importanza, offrendo in cambio delle ricompense, che di solito si concretizzano in regali, gadgets o coupons. Altre ancora invece prendono esattamente la strada opposta, per andare però ad ottenere lo stesso trade off. Queste aziende giocano sulla leva dei costi invece che su quella dei benefici, andando a rafforzare le proprie policies sulla privacy così da rendere in consumatore più confident nel rilasciare i propri dati (Andrade, Kaltcheva e Weitz, 2002).

Come detto in precedenza, entrambe le strade sono senza dubbio valide. Ciò che pesa di più sulla riuscita di queste iniziative è appunto la concezione e l'importanza che i consumatori assegnano al costo della propria azione, o al beneficio che ricevono in cambio.
Nel contesto della mia ricerca , come potrete constatare voi stessi in seguito, io mi andrò a concentrare principalmente sulla prima strada descritta, ovvero quella di un rewards in cambio delle proprie informazioni personali.
Ciò che mi ha fatto convogliare verso questa strada, e che mi spinge a ritenerla di interesse primario, è proprio il fatto che, se è vero che da una parte il fatto che dare benefici al consumatore per ricevere informazioni in cambio è ormai comunemente appurato, dall'altro lato sono molto limitati gli studi attui ad indagare quali sono i fattori che gli individui considerano di interesse e che li spinge ad andare oltre le proprie preoccupazioni.
Gli studi volti ad indagare questi fattori, come dicevo sono limitati, ma certamente non sono assenti del tutto dal panorama di ricerca.
Andando a vedere lo studio "Self-Disclosure on the Web: the Impact of Privacy Policy, Reward, and Company Reputation", possiamo analizzare alcuni fattori ed alcune variabili interessanti. Alcuni approcci, ci dice Andrade, che le compagnie possono utilizzare per l'analisi costi- benefici riguardo i consumatori, così da favorire la self – disclosure di quest'ultimi, possono essere ad esempio, lo sviluppo di una determinata reputazione aziendale così incrementare il livello di fiducia nei consumatori.
Elevare la reputazione aziendale, come sappiamo bene ha enormi benefici.
Alcuni di questi, come il fatto che una miglior reputazione aziendale porti all'attrazione dei migliori talenti sul mercato, sono ben conosciuti dall'aziende. Però quello che non sapevamo, che coincide anche con l'obiettivo della nostra ricerca, è appunto quanto affermato nel precedente paragrafo, ossia il fatto che migliorare la reputazione ad esempio attraverso azioni richieste dalla maggior parte della società (ex. Ecofriendly) fa sì che i consumatori si sentano più protetti e quindi maggior disponibili verso l'azienda stessa, portando in alcuni casi anche ad una maggior disponibilità a condividere le informazioni personali.
Sicuramente la possibilità di effettuare comunicazioni personalizzate ai consumatori, permettendo così di accrescere il retention rate è una variabile estremamente importante per i consumatori. Ma non è sicuramente l'unico motivo per cui far sentire protetti ed a proprio agio i consumatori e gli users.
Come è ben noto, la reason to be delle aziende, dagli albori dell'economia, è quella di raggiungere un livello di fatturato tale da permettergli di continuare il proprio business.
E quale è oggi il principale strumento che il mondo di Internet ha messo a disposizione delle aziende per raggiungere i propri obiettivi di budget? È oramai riconosciuto a livello mondiale, e lo abbiamo accettato nella nostra vita quotidiana, come l'e – commerce abbia guadagnato fette ampie negli sforzi rivolti dalle aziende per le proprie vendite.
Come è facile intuire, i temi dell' e-commerce e quello della privacy sono strettamente collegati tra di loro. La crescente espansione di questo strumento e l'enorme disponibilità di dispositivi elettronici ha fatto aumentare

le preoccupazioni degli individui per i propri dati, ed ha allo stesso tempo portato le aziende ad interfacciarsi con nuove sfide, che dovranno superare per raggiungere quel famoso vantaggio competitivo nel mercato, che le permetta di distinguersi dal grande numero di proposte che troviamo ogni giorno.

1.3 Customer Data Management

Nuove frontiere nella tecnologia hanno fatto sì che il cosiddetto marketing relazionale sia diventato reale negli ultimi anni, ma soprattutto, queste tecnologie (come Data Warehousing,e data mining) hanno permesso che la gestione delle relazioni con i consumatori sia diventata un'area fertile dove sviluppare un vantaggio competitivo rispetto agli altri players presenti sullo stesso mercato.
In particolare grazie al data mining, ovvero l'estrazione di dati ed informazioni nascoste all'interno di grandi database, le organizzazioni possono identificare clienti interessanti per il loro business, prevedere comportamenti futuri che questi metteranno in atto, e di conseguenza prendere decisioni proattive, guidate da una maggiore conoscenza del mercato. Soprattutto questi strumenti sono in grado di dare risposte ad alcune domande di business che fino a poco tempo era estremamente time consuming e nonostante questo, non sempre si era in grado di arrivare ad una risposta soddisfacente.
Nella realtà attuale in cui viviamo, il concetto di mass production e mass marketing, che si erano venuti a creare durante la rivoluzione industriale, sono stati accantonati per dare invece spazio a nuove idee in cui la relazione con il cliente occupa gli sforzi principali per le aziende (Rygielski, Wang e Yen, 2002)
Quindi riassumendo quanto detto fino a questo momento, l'importanza della gestione delle relazioni con i consumatori è ampiamente riconosciuta dagli esperti, ed è globalmente conosciuta come CRM (Customer Relationship Management). Una prima impressione, errata, potrebbe dirci che lo strumento del CRM sia applicabile solo per sviluppare le relazioni tra imprese e consumatori. In realtà, dopo un esame più attento, ci rendiamo conto che questo strumento è ancora più importante per i cosiddetti business customers. È proprio nel contesto del B2B infatti, che un grandissimo numero di informazioni vengono scambiate regolarmente e quotidianamente in praticamente tutti i mercati. È proprio questo uno dei punti principali che ci aiuta a capire l'importanza che il tema della privacy e self – disclosure (che vanno chiaramente di pari passo con lo sviluppo degli strumenti di CRM) hanno nel contesto economico attuale. Infatti come dicevo, in ogni campo di business è interessato nel prevedere i comportamenti dei propri consumatori attraverso la conoscenza acquisita con il data mining.
Per fare qualche esempio concreto, vediamo di seguito alcuni dei campi prevalentemente interessati:

- Retail: Attraverso l'uso di strumenti come carte di credito brandizzate e sistemi di punti di vendita, i retailers possono tracciare e immagazzinare dati di ogni transazione che avviene al loro interno. Questo li aiuta chiaramente a capire al meglio i vari segmenti di consumatori.

- Banche: anche le banche possono usare questi strumenti per avere un vantaggio nel loro business. Un esempio p quello del data mining che aiuta le banche a predire il valore che ogni cliente avrà nel corso della loro vita e per servire adeguatamente ogni segmento dei propri clienti.
- Telecomunicazioni: le aziende di telecomunicazioni di tutto il mondo si stanno oggi confrontando con una competizione sempre più agguerrita, che le obbliga a spingere su programmi di pricing finalizzati alla retention dei clienti e per attrarne di nuovi. Uno strumento che hanno però, è quello che viene fornito dalla grande quantità di registrazioni telefoniche, molto dettagliate. Identificando segmenti di consumatori che hanno patterns simili, queste compagnie possono sviluppare prezzi attrattivi e promozioni con determinate caratteristiche.

Quindi questi esempi sono volti a far comprendere l'importanza che questi strumenti oggi hanno per i più svariati tipi di business.
Senza dubbio tutti questi aspetti che sono stati esposti all' interno del paragrafo, sono da collegare come avrete già capito, a uno degli aspetti più interessanti che Internet ci ha messo a disposizione: l'E-commerce.
Così come l'ambiente del commercio elettronico diventa progressivamente più interattivo, così le preoccupazioni riguardo la privacy delle proprie informazioni sensibili ricopre sempre di più una posizione centrale nei dibattiti. Il centro della questione è su chi avrà affettivamente accesso alle informazioni che i consumatori divulgano in rete. Il famoso customer data a cui le aziende danno grande e importanza e a cui spesso viene dedicato un dipartimento apposito, per far sì che si sviluppino questi strumenti per le questioni che abbiamo detto precedentemente.
Il concetto di Customer Data Management è fondamentale per comprendere l'importanza che LA gestione delle informazioni degli utenti ricopre per tutti i soggetti interessati in maniera attiva nel business.
Molte imprese sono oggi consapevoli dei problemi legati alle preoccupazioni degli utenti circa la propria privacy, e sanno che sono sfide che dovranno vincere se non vogliono perdere le loro posizioni sul mercato. Per questo vengono pubblicate le polizze aziendali riguardo il trattamento che verrà fatto dei dati degli utenti, così da apparire equi e rassicuranti agli occhi dei consumatori, dando quel senso di protezione che può spingere alla self – disclosure.
Le principali compagnie oggi si trovano a spendere annualmente circa 36 miliardi di dollari per catturare e gestire i dati dei clienti. L'altro lato della medaglia che porta le aziende a produrre questa mole di investimenti , è che molti consulenti del lavoro suggeriscono che le aziende possono utilizzare le informazioni sensibili dei propri clienti per generare incrementi di produttività e di profitto che sono del 6% più alti rispetto alla competition (Wilmott, 2013). Questo circolo generato da questo sforzo, è che aumenti in maniera sensibile anche la vulnerabilità e la suscettibilità degli users, i quali si preoccupano dell'uso che viene fatto dei propri dati. Quindi la raccolta dei dati, in particolare quella che avviene online, può avere una parte oscura, e a causa di questa gli individui spesso esprimono una reazione negativa alle pratiche effettuate sulla propria privacy (Marcus & Davis, 2014). L'idea che viene alla mente dopo un'attenta analisi degli studi effettuati sul tema fino a questo momento, è che nonostante il rilievo del tema, le aziende e le organizzazioni non hanno ancora chiaro e non hanno soprattutto insights a disposizione, che possano prevenire e mitigare gli effetti negativi che le loro

azioni possono portare. Uno strumento importante in tal senso (Karjoth, 2002) è la cosiddetta Platform for Entreprise Privacy Paractices (E-P3P).
Questo strumento definisce la tecnologia capace di migliorare e rendere effettive le promesse fatte ai consumatori, risolvendo gran parte dei problemi che hanno le aziende le quali collezionano ed immagazzinano le informazioni dei propri clienti. A prescindere dal fatto che l'azienda raccolga, immagazzini o processa le informazioni personali, E-P3P può assicurare quel flusso di informazioni e di pratiche che una compagnia compie per rispettare il proprio statuto circa la privacy.
Questo paragrafo, cosi come gli altri di questo capitolo, lo ritengo fondamentale per capire l'ambiente in cui ci stiamo muovendo e quindi in particolare per comprendere l'importanza delle variabili che permettono ai clienti di concedere i propri dati alle aziende, e il perché i soggetti economici rivolgono così tanti sforzi per riuscire ad accaparrarsi queste informazioni a discapito dei competitors.
Tutti questi tentativi delle aziende nel carpire il maggior numero di dati per i propri scopi, porta infatti gli individui ad interfacciarsi con minacce relative alla propria sfera personale.
La sfida principale è dunque quella di guadagnare la fiducia dei clienti assicurando un adeguato livello di privacy e sicurezza per i dati più sensibili.

1.4 Le implicazioni dal punto di vista legale

I cloud dei database descritti in precedenza, hanno enormi benefici potenziali per le compagnie, tra cui evitare di sprecare risorse informative, accrescere l'efficienza dei propri strumenti ed abbattere i costi.
La cosiddetta cloud computing non può essere sottostimata nell'economia globale, in quanto si parla di un giro di 68 miliardi di dollari, con una previsione di crescita di 17 miliardi ogni anno nel futuro.
Per raggiungere questo potenziale è però essenziale assicurare un alto livello di privacy e di sicurezza per le informazioni sensibili dei consumatori, che, come detto in precedenza, rappresenta una difficile sfida per le aziende. È proprio per questo che allo stesso livello dei consumatori e delle aziende, uno dei soggetti maggiormente interessati alla questione di riferimento di questa tesi, è proprio quello legislativo.
Gli individui richiedono sempre di più, dei regolamenti ad hoc in grado di proteggere le proprie informazioni più sensibili, dagli strumenti e dai fini sempre più aggressivi che le imprese mettono in campo.
Per analizzare al meglio questo scenario in un importante studio vengono presi in esame i regolamenti di 2 principali soggetti a livello mondiale: gli Stati Uniti e l'Unione Europea.
Il concetto di privacy, la sicurezza ed altri rischi legali associati alla protezione di informazioni sensibili sono considerati uno dei principali ostacoli nell'uso di questi database di registrazione che usano le aziende per il proprio CRM. I policy makers ed i legislatori devono analizzare la natura delle debolezze legate oggi alla sicurezza. L'attuale stato delle cose ci porta a dichiarare che il livello di protezione è semplicemente troppo basso e spesso inefficiente per i dati sensibili. Vediamo ad oggi quali sono i regolamenti principali per quanto

riguarda gli stati membri dell'Unione Europea. Le leggi europee ad oggi richiedono alti livelli di protezione da parte delle aziende e delle organizzazioni per ciò che riguarda i dati sensibili dei propri clienti. La direttiva sulla protezione dei dati dell'Unione Europea (95/46/EC) dà ai consumatori alcuni diritti di base con rispetto ai loro dati personali, ed allo stesso tempo richiede dei "Data Controllers" che seguono regole e restrizioni nelle operazioni da compiere.

All'interno dell'Unione Europea, i soggetti che fanno business non possono raccogliere, immagazzinare e rilasciare dati personali dei propri consumatori in maniera diversa da quanto specificato dalla Direttiva 95/46/EC e dalle leggi interne dei singoli stati membri (che spesso sono addirittura più rigide). Ciò significa che le informazioni personali possono essere utilizzare finalità specifiche, esplicite e legittime e mai in maniera differente da quanto è stato invece dichiarato.

Inoltre le impresse devono essere in grado di assicurare adeguata protezione in modo tale da prevenire accessi non autorizzati a questi dati. Tutti I soggetti, anche esterni, che operano all'interno dei confini dell'Unione Europea, dovranno obbligatoriamente adattare le proprie Privacy Policies a quelle richieste dalla direttiva nominata in precedenza. La direttiva proibisce in maniera univoca di trasferire i dati personali degli individui dell'UE in paesi che si trovano all'esterno dell'EEA (Area Economica Europea), se questo non ha le leggi necessarie volte ad assicurare un chiaro livello adeguato di protezione delle informazioni in questione.

Ad esempio il trasferimento di questi dati è vietato dall' Unione Europea agli Stati Uniti, a meno che chi li riceve non sia membro del Safe Harbour Agreement.

Il concetto di privacy, come è naturale che sia, ricopre un grande interesse legale a livello globale. Paradossalmente già con il fatto di essere cittadini dell'Unione Europea, dovrebbe farci sentire fortunati rispetto ai cittadini provenienti da altre parti del mondo, cittadini del Stati Uniti d' America compresi.

La direttiva sulla protezione delle informazioni personali dell'Unione Europea, del 2015, rappresenta infatti un set di protezione delle informazioni personali, considerevolmente più estesa rispetto agli sforzi statunitensi.

La direttiva UE impone un unico set di regole di protezione dei dati, che ritengono le società responsabili per i comportamenti rilevanti per la privacy di una singola autorità di regolamentazione.

Fattore da non sottovalutare è infatti il cosiddetto "diritto ad essere dimenticato" o, più tecnicamente, diritto all'oblio, che permette ai consumatori dell'Unione Europea di poter richiedere la rimozione di qualche collegamento sul web che non forniscono più informazioni personali accurate e rilevanti.

Proprio il diritto all'oblio è stato recentemente protagonista di upgrade nello scenario della legislazione europea.

Questo importante diritto, inizialmente riconosciuto esclusivamente a livello giurisprudenziale sia in campo europeo che nazionale, con l'entrata in vigore del nuovo Regolamento Generale sulla Protezione dei Dati Personali (RGPD, Regolamento UE 2016/679) riceve finalmente un'espressa regolamentazione che ne indica portata e limiti.

Il diritto in questione, come anticipato in precedenza, può essere definito come l'interesse di un singolo individuo ad essere dimenticato: la sua esplicazione consiste nella cancellazione dei contenuti, dalle varie pagine web, di precedenti informazioni, spesso pregiudizievoli nei confronti dello stesso individuo, e che non rappresentano più allo stato attuale la vera identità del soggetto in questione.
Oggi è quindi possibili richiedere l'eliminazione di notizie relative a fatti avvenuti in passato in modo da tutelare la riservatezza e l'identità personale attuale di un determinato individuo.
Naturalmente questo atto non può avvenire in modo incondizionato, ed adesso la RGDP (dopo le varie corti nazionali e comunitarie) hanno stabilito quali debbano essere le condizioni necessarie per un corretto esercizio di questo diritto, in particolar modo allo scopo della sua compatibilità con il diritto di informazione che, nei casi in cui le notizie siano attuali e di interesse pubblico, dovrà comunque prevalere sull'interesse del singolo.
Notizia recentissima è l'entrata in vigore del GDPR, nuovo regolamento sulla privacy, che ha valenza in tutti gli stati membri dell'Unione Europea a partire dal 25 Maggio 2018.
Il cosiddetto GDPR è la più grande revisione delle norme sulla privacy online sin dalla nascita di Internet, che darà ai cittadini europei il diritto di sapere quali dati sono memorizzati su di essi e tutelerà il diritto di vederli cancellati.
Le informazioni presenti nella rete sono in continuo movimento, e le connessioni e relazioni tra i diversi Paesi del mondo si fanno sempre più fitte.
I dati su Internet inoltre con questo nuovo regolamento saranno più protetti grazie a nuove restrizioni e all'obbligo di utilizzare un linguaggio chiaro nelle regole relative alla privacy.
Un'importante novità è l'istituzione di una nuova figura, ovvero quella del responsabile della protezione dati di cui dovranno munirsi tutte le realtà, pubbliche e private, che trattano informazioni sensibili.
L'idea che ha ispirato l'introduzione della nuova normativa è quella di permettere che i cittadini europei abbiano un controllo molto maggiore sul modo in cui i singoli, le aziende e gli enti pubblici utilizzano le informazioni, e in particolari i dati sensibili, raccolti dagli utenti.
Come leggiamo sul regolamento: "Per dati sensibili si intendono le informazioni che possono rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale.
L'esigenza da cui è nato il GDPR, è quella di armonizzare e semplificare le norme riguardanti il trasferimento dei dati personali dall'Ue verso altre parti del mondo per far fronte alle sfide date dagli sviluppi tecnologici.
Allo stato attuale, vi è inoltre l'assenza di una reale consapevolezza, da parte dei cittadini, dell'importanza di proteggere tutte le informazioni che comunicano a terzi.
Ma vediamo adesso concretamente cosa andrà a cambiare nello scenario attuale con l'introduzione di questo regolamento. Per tutti i dati sensibili sarà necessario un consenso esplicito dell'interessato. Per quanto riguarda

i minori, il consenso sarà considerato valido a partire dai 16 anni, prima di quell'età il consenso deve essere espresso da un genitore o da chi ne fa le veci.
La normativa esplicita in maniera più chiara rispetto alle precedenti, ciò che deve essere presente all'interno dell'informativa sulla privacy.
Questi elementi sono: la base giuridica del trattamento, l'interesse legittimo, il periodo di conservazione dei dati, l'esposizione del diritto di presentare un reclamo all'autorità di controllo e l'indicazione della logica dei processi decisionali impiegata e le conseguenze per l'interessato, nei soli casi in cui il trattamento concerna processi decisionali automatizzati come, ad esempio, la profilazione.
I diritti di cui gode chi fornisce i propri dati sensibili di ampliano sensibilmente, che in particolare avrà il diritto all'accesso ai dati che ha fornito, gli dovrà essere comunicato il periodo di conservazione dei dati.
Viene inoltre sottolineato e rafforzato il diritto all'oblio, ovvero il diritto di cancellazione dei propri dati.
Tra gli altri diritti previsti dal GDPR, vi è il diritto di limitazione del trattamento, ovvero l'interessato potrà richiedere la cancellazione o la rettifica dei dati nel caso di trattamento illecito e il diritto alla portabilità dei dati, ovvero, la possibilità che il titolare trasferisca i dati portabili ad altro titolare indicato dall'interessato e con il suo consenso. Un'altra importantissima novità introdotta dal regolamento europeo prevedere il venir meno dell'autorizzazione nazionale.
Il trasferimento dei dati a paesi terzi, potrà avvenire anche senza l'autorizzazione nazionale del Garante, a differenza di quanto invece vigeva con il precedente Codice della privacy.
Come anticipato, con il nuovo regolamento sulla privacy UE, il diritto all'oblio riceve finalmente una regolamentazione espressa.
Entrando nello specifico di questo regolamento recente, vediamo che ad esempio secondo l'articolo 17 l'interessato ha diritto di ottenere, senza ingiustificato ritardo ,la cancellazione dei dati che lo riguardano da parte del titolare, quando ricorrono alcune condizioni speciali.
Le condizioni in questione vanno dal fatto che i dati non siano più necessari ai fini del trattamento per il quale sono stati raccolti o diffusi, al caso in cui l'interessato revochi il consenso al trattamento dei dati, il periodo di conservazione degli stessi sia spirato, oppure quando non vi siano altri legittimi motivi per proseguire con il trattamento.
Un'altra condizione che dà la possibilità all'individuo di richiedere la cancellazione dei dati sul web è l'ipotesi che questi dati siano stati trattati illecitamente, o comunque in maniera non conforme con quanto dichiarato al momento della raccolta delle informazioni che l'individuo ha rilasciato a terze parti.
Come detto però questo diritto non trova applicazione quando arriva a confrontarsi con il diritto di cronaca ed il diritto di informazione che sono prevalenti.
La sua applicazione può inoltre venire limitata in quei casi in cui la conservazione sia assolutamente necessaria per adempiere ad obblighi previsti dal diritto comunitario o per motivi di interesse pubblico nel settore della sanità, della ricerca scientifica e storica o a fini statistici.

Da ultimo, il diritto alla cancellazione non trova espressione quando i dati siano necessari per l'accertamento, l'esercizio oppure la difesa di un diritto in qualsiasi tipo e luogo di una sede giudiziaria.
Tornando adesso al paper di Martin & Murphy (2016), vediamo come numerose ricerche di privacy a livello globale è un aspetto estremamente poco sviluppato al giorno di oggi.
Scoperte tutt'ora limitate , ci mostrano che i valori culturali possono influenzare in maniera importante la percezione di privacy da parte degli individui, e questo si rispecchia nel fatto che i paesi con normative sulla privacy più rigorose abbiano meno problemi di privacy (Dolnicar & Jordaan, 2007).
Sulla stessa onda, troviamo il riscontro che su imprese con regolamenti sulla privacy scadenti, i consumatori mostrano una maggiore insoddisfazione e desiderio di interventi governativi relativi appunto alla privacy.
Bisogna dire però, che anche regolamenti troppo stringenti sulla privacy possono portare a conseguenze negative per quelle aziende che li adottano.
In un esperimento che ha confrontato la situazione pre e post politica della direttiva sulla protezione dei dati emessa dall'UE, i ricercatori hanno scoperto che l'efficacia della pubblicità, misurata attraverso l'acquisto dichiarato, era significativamente diminuita nell'UE dopo tale regolamento.
Invece le nazioni non membri dell'UE non hanno nello stesso arco temporale, visto cambiamenti nell'efficacia dell'advertising, mostrando il ruolo delle politiche sulla privacy, sui risultati del marketing nei consumatori. A livello globale, la maggior parte delle conoscenze che oggi abbiamo esaminando somiglianze e differenze tra contesti differenti, sia a livello individuale che a livello delle aziende, è limitata a campioni europei o statunitensi.
Gli europei hanno mostrato un livello sensibilmente più alto di privacy concerns, ed a conseguenza di ciò riscontriamo una regolazione maggiore delle legislazioni europee, rispetto agli USA e non solo.
Un vuoto importante, come era facilmente prevedibile, lo riscontriamo nelle questioni di privacy dell'oriente, in particolare per ciò che riguarda India e Cina.
In generale, la conoscenza che abbiamo sulle questioni legate alla privacy, e gli approcci sia a livello individuale che a quello aziendale tra i cosiddetti paesi del BRIC, cosiccome per quelli in via di sviluppo, è ampiamente carente, per non dire quasi equivalente a zero.
Un altro argomento importante per il contesto generale è quello che riguarda l'eticità della privacy.
Nella famosa "Valutazione etica della privacy", Foxamn a Kilcoyne (1993) ci dicono che i cosiddetti marketers devono impegnarsi attivamente per assumere un atteggiamento etico in questo settore.
Molti egli stakeholder, vale a dire imprese, consumatori, responsabili delle politiche e gruppi di difesa, sono totalmente investite dallo scambio di informazioni, ed hanno quindi interesse alle regole di questo scambio, alle norme di accesso alle informazioni, alla protezione ed all'utilizzo delle informazioni.
Un esempio importante, la teoria del contratto sociale stabilisce che i programmi di condivisione delle informazioni dei consumatori dovrebbero tenere conto dello scopo di scambio, del rischio e dei potenziali danni per il consumatore. La ricerca sul contratto sociale all'interno dello spazio della privacy rivela anche che

i marketer preferiscono andare oltre quando devono determinare le percezioni della felicità negli scambi. È più probabile che i consumatori credano che i professionisti del marketing abbiano soddisfatto la loro parte del contratto sociale che governa lo scambio di informazioni quando percepiscono un maggiore valore di personalizzazione dallo scambio (Chellappa e Sin, 2005), o quando vengono compensati finanziariamente per le loro informazioni (Gabisch e Milne, 2014).
La letteratura sulla privacy dei consumatori considera l'equità come la chiave per l'attitudine del marketing a soddisfare il contratto sociale che disciplina lo scambio di informazioni (Culnan e Bies, 2003).
Ulteriori prospettive etiche mostrano il potenziale per migliorare la comprensione della privacy. Ad esempio, il modello di equilibrio di responsabilità di potere derivato da Murphy et Al. (2005) sostiene una forte connessione che c'è tra potere sociale e responsabilità sociale, dove un partner potente è obbligato a proteggere e promuove l'uguaglianza percepita del partner meno dominante.
La ricerca induce i consumatori a reagire negativamente a squilibri di potere in cui le imprese non riescono a promuovere l'uguaglianza sentita nello scambio di informazioni (Lwin, 2007).
Nel marketing, lo sviluppo e l'analisi di teoria etica per districare ulteriormente le domande contemporanee sulla privacy dei dati, nel tentativo di fornire consigli a chi deve far fronte a tali preoccupazioni. Ad esempio, il modello di decisione etica di Ferrell e Gresham (1985) potrebbe aiutare a comprendere, colmando le preoccupazioni della società sull'uso delle informazioni ponendo in risalto il problema.

1.5 Conclusioni

Come abbiamo visto da questo primo capitolo, i temi che toccano il concetto di self disclosure dei propri dati svariati, e molti sono stati gli studi effettuati dagli studiosi.
Tante però sono anche le lacune sul tema, soprattutto capire quali siano i fattori che fanno superare le preoccupazioni agli individui e gli permettono di condividere con gli altri le informazioni personali.
Nel seguente capitolo andremo proprio ad esplorare il concetto del paradosso della privacy, vedendo la reale relazione tra quanto viene dichiarato dai consumatori ed il comportamento invece effettivo degli stessi individui.
Saranno quindi affrontati i temi di maggior interesse per questa ricerca, in particolare cercando di indagare due aspetti: l'analisi tra costi e benefici che spingono i consumatori a prendere determinate decisioni, e la dicotomia tra gli atteggiamenti che hanno gli individui verso la privacy, ed i comportamenti che invece mettono effettivamente in atto. Inoltre inquadreremo in maniera più preciso il ruolo che il tema riveste nelle dinamiche di marketing.

CAPITOLO 2. LA RELAZIONE TRA CONSUMATORI E PRIVACY

2 Introduzione

Nel primo capitolo abbiamo cercato di vedere il contesto di riferimento in cui questa tesi intende andare a situarsi e nel quale sono stati affrontati determinati fields di interessi come ad esempio il concetto di privacy, l'ampia questione delle privacy concerns e soprattutto i temi legati alla self– disclosure dei dati/informazioni personali ed agli stakeholders ad essa associati, interessati a capirne le dinamiche per poterne trarre vantaggi economici.
Nel secondo capitolo invece l'intenzione è quella di andare maggiormente in profondità per capire al meglio cosa significa la privacy, come questa si lega alla vita quotidiana dei consumatori, ma soprattutto indagare quelle variabili che sono imprescindibili per cambiare o influenzare il comportamento e le attitudini degli individui, e questo verrà fatto grazie al contributo fornitoci dai principali ricercatori ed i loro contributi.
Verranno inquadrati i principali temi che ci permetteranno successivamente di poter creare, analizzare e vedere i risultati delle domande di ricerca che ci siamo posti una volta che abbiamo iniziato a studiare il tema in esame.
Come vedremo, il terzo capitolo sarà la sede in cui saranno chiariti al meglio i temi che affronterà questa tesi di laurea, ma riteniamo che sia estremamente necessario dare spazio alle principali ricerca per poter individuare i gap che ancora sono presenti e di conseguenza tentare di dargli una risposta adeguata.
Dopo questa breve introduzione fatta per mettere i paletti e rendere più chiara la comprensione di ciò che verrà scritto nei paragrafi successivi, andiamo adesso a vedere nel dettaglio i temi più interessanti che la ricerca degli esperti e degli studiosi ha prodotto negli ultimi anni.

2.1 La questione del data privacy nel marketing

Il paragrafo che andremo adesso ad affrontare, lo ritengo meritevole di estrema attenzione, per comprendere al meglio il ruolo che il tema del data privacy ha assunto nel vasto mondo del marketing attuale.
Come abbiamo iniziato a vedere nel primo capitolo, sono molti i soggetti di business interessati ai dati degli individui, per lo più per ragioni e fini di carattere prettamente economiche e demografiche.
Riuscire ad effettuare comunicazioni ed azioni di marketing precisamente personalizzate e targetizzate sarà uno degli obiettivi su cui le aziende concentreranno i maggiori sforzi nei prossimi anni, e proprio le conseguenze naturali del diffuso acceso alle informazioni personali dei consumatori sono evidentemente moltissime (Martin e Murphy, 2016).
Tra le più comuni possiamo riscontrare la vulnerabilità alle truffe online, invasione della propria sfera di privacy, comunicazioni di marketing non desiderate ed estremamente mirate, altre comunicazioni di marketing considerate invasive e che interrompono il ritmo delle attività quotidiane. Una delle questioni principali a cui è

necessario trovare una risposta rapidamente, è come i consumatori possono reagire adesso che le loro informazioni sono ampiamente accessibili e disponibili ad un'ampia categoria di marketers ed altre parti interessate.
Durante un famoso studio sulla privacy, uno dei partecipanti commentò con le seguenti parole:
"condivido i miei dati sensibili ogni giorno, a prescindere dal fatto che io lo voglia o meno. Le informazioni non sono davvero il problema principale. Il problema reale lo sono coloro che vedono queste informazioni e, soprattutto, coloro che le usano. Ma adesso è troppo tardi per far rimettere il genio all'interno della lampada" (Rainie e Duggan 2016).
Nei prossimi paragrafi, per la nostra ricerca sarà quindi necessario tentare di comprendere quali sono le reazioni dei consumatori alle questioni legate alla privacy, e quali sono le azioni che possono modificare la percezione su questi temi, superando così gli ostacoli delle preoccupazioni per la sicurezza dei propri dati.
L'importanza risiede nel fatto che all'interno delle dinamiche di marketing, la protezione e la raccolta dei dati ricoprono un ruolo molto importante.
Di seguito, vedremo come la privacy venga considerata argomento di interesse dagli economisti, spingendoli ad investire risorse ed energie, nella ricerca di teorie che potessero spiegare le dinamiche che si muovono intorno al concetto di privacy.

2.2 La teoria economica della privacy

Andremo adesso ad affrontare le principali teorie economiche emerse negli ultimi decenni, a partire dagli anni 70', che basano i loro assunti e concentrano i loro sforzi sulle questioni legate alla privacy. Avere ben chiare queste teorie ci è utile nel corso di questa ricerca, in quanto contribuiranno a capire l'importanza che la privacy riveste per i soggetti di business, e per capire l'evoluzione che questo tema ha avuto nel corso del tempo per gli economisti.
Comprendere al meglio gli assunti economici, sarà utile anche per la formulazione del questionario attraverso cui verranno indagati i principali items collegati al concetto di privacy, e di altre variabili che però vedremo con maggiore precisione più avanti.
Una prima ondata di ricerca economica è costituita da opere prodotte tra gli anni '70 e i primi anni '80 da studiosi della Scuola di Chicago come George Stigler e Richard Posner. In linea di massima, questa prima ondata di lavoro non consisteva in modelli economici formali, ma piuttosto trattava argomenti economici di portata generale, che si focalizzavano intorno al valore o ai rischi che gli individui e la società possono sostenere quando le informazioni personali sono protette, rendendo informazioni potenzialmente utili, indisponibili al mercato.
All'interno della teoria economica neoclassica di mercati perfettamente competitivi, si parla di informazione "completa", ovvero quella situazione in cui c'è la disponibilità di informazioni rilevanti a tutti i partecipanti al

mercato, porta all'efficienza economica: ad esempio, quando tutti i consumatori conoscono i prezzi ai quali un' azienda vende il proprio prodotto, la concorrenza spingerà tali prezzi al livello più basso possibile, aumentando il benessere dei consumatori (Acquisti, 2010).

Di conseguenza la protezione della privacy crea inefficienze nel mercato, dal momento che nasconde informazioni potenzialmente rilevanti da altri agenti economici (Posner, 1981). Prendiamo il caso in cui un candidato in cerca di lavoro travisi il suo background e la sua esperienza. Ecco, questa protezione delle informazioni personali del richiedente influenzerà negativamente la decisione di assunzione dell'azienda. Pertanto, la tutela della privacy dei primi viene a scapito della redditività di questi ultimi.

Quindi, rimuovendo le informazioni personali degli individui dal mercato attraverso la normativa sulla privacy, si trasferisce il costo delle possibili caratteristiche negative di quella persona su altri attori del mercato. Sempre secondo la scuola di Chicago, l'interferenza governativa nel mercato delle informazioni personali è destinata, nel migliore dei casi, a rimanere inefficace.

Dato che gli individui hanno interesse a divulgare pubblicamente informazioni personali favorevoli e nascondere tratti negativi, coloro che decidono di proteggere le loro informazioni personali (ad esempio, un debitore che non vuole rivelare la sua storia di credito) stanno di fatto segnalando un tratto negativo. In questo caso, gli interventi normativi che bloccano il flusso di informazioni personali sarebbero contrassegnati da carattere redistributivo ed inefficiente, infatti risorse economiche e fattori produttivi finirebbero per essere usati in modo inefficiente o premiati ingiustamente, perché le informazioni sulla loro qualità sono state rimosse dal mercato.

Più recentemente, è stato scoperto che la condivisione senza restrizioni dei dati personali dei consumatori tra due imprese può infatti ridurre le distorsioni del mercato e aumentare il benessere sociale, compresi quello dei consumatori (Calzolari e Pavan, 2006).

Basandosi sull'argomento del cosiddetto teorema di Coase (Noam, 1997) viene comunemente sostenuto che la protezione dei dati di un consumatore non dipende dall'iniziale protezione delle informazioni personali, ma dipende in ultima analisi dalle valutazioni relative delle parti interessate a tali dati.

Tuttavia, ci sono anche limiti e critiche mosse verso il pensiero degli esponenti della scuola di Chicago. ad esempio si afferma che gli agenti economici razionali possono finire per risultare inefficienti se investono troppo nella raccolta di informazioni personali su terze parti e che ipotesi di comportamento razionale alla base dei modelli di privacy della Scuola di Chicago potrebbero non riuscire a cogliere la complessità intrinseca alla base del processo decisionale sulla privacy da parte di individui e organizzazioni. Viene anche mostrato che dati i prezzi di equilibrio, il beneficio privato dell'acquisizione delle informazioni potrebbe superare il suo vantaggio sociale (Hirshleifer, 1996). In un ambiente di scambio puro, l'informazione può non avere alcun valore sociale, perché si traduce solo in una ridistribuzione della ricchezza da agenti ignoranti a informati. Successivamente è stato costruito un modello in cui ogni individuo si preoccupa della sua reputazione, ma le azioni di un individuo generano esternalità, a volte positive e a volte negative (Daughety, 2010); infatti sotto un

regime pubblico, gli individui distorcono le loro azioni per migliorare o preservare la loro reputazione, mentre nell'ambito privato, scelgono il livello individuale ottimale dell'attività. Pertanto, ad esempio, il benessere sia privato che pubblico può essere aumentato quando le informazioni su un singolo controllo in un centro di riabilitazione dalla droga o dall'alcol rimangono private, altrimenti, lo stigma associato a farlo potrebbe impedirgli di cercare un trattamento. Allo stesso modo, se un medico non fosse legato alla riservatezza, un paziente potrebbe non sentirsi a suo agio condividendo tutti i dettagli rilevanti della sua condizione. Un altro esempio è la beneficienza: infatti quando i contributi di beneficenza sono pubblici, gli importi donati possono aumentare, perché il contributo aumenta la reputazione del donatore.

Dopo questa prima ondata di pensieri economici legati alla privacy gli economisti non hanno mostrato ancora un particolare interesse per questo tema per oltre un decennio.

Ciò è cambiato a metà degli anni '90, probabilmente a causa del progresso nelle tecnologie informatiche e digitali su più fronti (la proliferazione di banche dati elettroniche e personal computer, l'avvento di Internet, la diffusione della posta elettronica), che ha portato a un nuova serie di questioni economiche che comportano l'utilizzo di dati personali.

Questa seconda ondata è simile alla prima in termini di preferenza per articolare argomenti economici, piuttosto che modelli formali, tuttavia, è si differenziano non solo temporalmente, ma anche in termini di specificità degli scenari di privacy considerati e dalla consapevolezza emergente del ruolo delle tecnologie dell'informazione digitale.

I lavori prodotti in questa fase hanno iniziato a concentrarsi su questioni come il ruolo delle tecnologie crittografiche che influenzano gli interessi economici dei titolari dei dati e degli interessati, o la creazione di mercati per i dati personali, nonché le implicazioni economiche sugli usi secondari delle informazioni personali. In particolare si osserva che lo sviluppo di tecnologie a basso costo per la manipolazione dei dati genera nuove preoccupazioni per l'elaborazione delle informazioni personali. Tuttavia, i consumatori possono subire dei costi di privacy quando le informazioni personali su di loro sono troppo poco condivise con terze parti (Varian, 1997).

Il consumatore può razionalmente volere che alcune informazioni su di lui siano note ad altre parti (ad esempio, un consumatore potrebbe desiderare che le sue preferenze di vacanza siano conosciute dai venditori telefonici per ricevere offerte da loro che potrebbero effettivamente interessarle), ma lo stesso consumatore, può allo stesso tempo non voler far girare troppe informazioni per essere conosciuto da altri, per ragioni ritenute importanti per lui.

Questa linea di ragionamento richiama gli approcci della Scuola di Chicago ma aggiunge nuove preoccupazioni associate all'uso secondario dei dati personali. Le aziende possono infatti vendere i dati del consumatore a terzi, che possono portare a spam e discriminazioni di prezzo avverse (Odlyzko 2003). Tali esternalità negative non possono essere interiorizzate dal consumatore né dal distributore che distribuisce le informazioni (Swire e Litan 1998).

Un consumatore può decidere di condividere le informazioni personali con un motivo perché si aspetta di ricevere un beneficio netto da tale transazione; tuttavia, ha poca conoscenza o controllo su come e da chi tali dati verranno successivamente utilizzati.
Superato il pensiero di questa seconda fase od andata della ricerca, andiamo adesso a visualizzare ed indagare l'ultima ondata della ricerca economica sulla privacy.
Questa fase nasce a seguito del successo commerciale di Internet e della proliferazione di banche dati contenenti informazioni sui consumatori, che ha portato un aumento importante sulla ricerca sull'economia della privacy all'inizio del XXI secolo.
Poiché così tante transazioni e attività, che una volta erano esclusivamente private, vengono condotte online, oggi aziende, governi, aggregatori di dati e altre parti interessate possono osservare, registrare, strutturare e analizzare i dati sul comportamento dei consumatori a livelli di dettaglio e velocità di calcolo senza precedenti e di conseguenza, l'economia digitale è, in una certa misura, arginata dall'organizzazione di grandi quantità di dati non strutturati per facilitare l'indirizzamento delle offerte di prodotti da parte dei consumatori ai singoli consumatori.
Ad esempio, i motori di ricerca si basano su dati provenienti da ricerche ripetute e passate per migliorare i risultati della ricerca stessa, oppure i venditori si affidano agli acquisti passati e alle attività di navigazione per fare raccomandazioni sui prodotti. Anche i i social network usano questi strumenti affidandosi ai marketer per accedere alle loro vaste basi di utenti al fine di generare ricavi. Questa terza ondata, temporaneamente vicina alla seconda, è differenziata dal fatto che gli studi sono radicati in modelli economici più formali e in analisi empiriche, compresi esperimenti di laboratorio ed è inoltre più direttamente collegata ai nuovi problemi economici portati avanti dagli sviluppi nella tecnologia dell'informazione, inclusi i motori di ricerca, il targeting comportamentale e i social media. Mentre gran parte della terza ondata è focalizzata su questioni che riguardano la privacy a livello di protezione delle informazioni sulle preferenze(quindi un numero significativo di modelli esaminano le relazioni tra privacy e prezzi dinamici), diverse dimensioni della privacy e i compromessi economici possono derivare da diversi angoli degli stessi scenari di privacy.
Di conseguenza, altri flussi di lavoro comprendono lo sviluppo dei mercati per la privacy, il targeting comportamentale, l'analisi economica della sicurezza delle informazioni (personali), e il rapporto tra beni pubblici, riconoscimento sociale e privacy.
Come abbiamo visto quindi in questo paragrafo, il tema della privacy comporta conseguenze economiche non indifferenti, e per questo non trascurabili nella nostra analisi e nella domanda di ricerca.

2.3 Analisi dei costi e dei benefici

Nel paragrafo precedente abbiamo quindi appena visto quali sono quelle teorie economiche che si sono succedute negli ultimi decenni, permettendoci di avere ben definito il contesto di riferimento. Ancora più importante del precedente, è però la sezione che ci accingiamo ad affrontare, dove saranno analizzati i costi ed i benefici, sia per le aziende che per i consumatori, che sono strettamente interconnessi con le dimensioni della privacy.

Nelle situazioni in cui il singolo individuo si trova davanti alla decisione di fornire o meno i propri dati personali ad una terza parte, si innescano dei meccanismi per cui vengono valutati i relativi costi, spesso tenuti ben nascosti dalle aziende, ed i relativi benefici derivanti da iniziative di marketing, i quali a differenza dei costi vengono ampiamente propagandati dalle stesse aziende: capire le dinamiche scatenate da queste leve è fondamentale per la nostra ricerca, in quanto rende possibile comprendere i fattori che più incentivano gli individui a rilasciare le proprie informazioni.

La sempre più sofisticata gestione delle informazioni sensibili dei consumatori grazie agli strumenti di CRM (Customer Relationship Management), permette la realizzazione di offerte di prodotti personalizzate, raccomandazioni, sconti (spesso minimi) sui vari prodotti, l'aggiunta di servizi extra fruibili gratuitamente ed in generale comunicazioni di marketing e contenuti media considerati rilevanti per gli stessi consumatori. Gli addetti e gli operatori di marketing, possono teoricamente offrire anche ulteriori vantaggi ai propri clienti, considerato il fatto che sono in grado di operare in modo sempre più efficiente se hanno a disposizione informazioni più precise e rilevanti.

L' importanza dei costi e benefici per operatori di marketing e per i consumatori (e di conseguenza anche per la nostra ricerca di tesi) sono un aspetto di primaria importanza e giustificano ulteriori indagini che possano assicurare una comprensione più ampia e soprattutto più chiara del fenomeno: proprio per queste ragioni un grande numero di ricerche sul tema sono state affrontate sempre con maggiore frequenza nel contesto accademico.

Le aziende hanno infatti bisogno di queste informazioni per decidere se investire sulle questioni legate alla privacy e quali ricompense offrire ai consumatori per le loro informazioni personali. Anche I governi hanno bisogno di queste informazioni per decidere sulle politiche pubbliche in materia di riservatezza delle informazioni. Per esempio è stato proposto di regolare la privacy attraverso i mercati in informazioni personali, ma la fattibilità economica di tali mercati dipende dal valore percepito della privacy della singola persona (Laudon e Varian, 1997).

Interessante è che molte di queste ricerche ci mostrano che le pratiche di marketing che usano dati ed analisi raccolti dai consumatori sono sempre più avanzate ed affinate, e stanno sempre di più rappresentando uno spazio importante nello scenario economico globale.

Vediamo adesso i benefici che sono legati ai dati rivelati dai consumatori, legati al mondo del business. Oggigiorno siamo in un'epoca nella quale stiamo vivendo una vera e propria rivoluzione commerciale orientata e basata sui dati dei consumatori, in cui gli individui sono allo stesso tempo consumatori e produttori di un bene più prezioso: le loro informazioni personali.

Le imprese possono beneficiare in modo significativo della capacità di apprendere così tanto sui loro attuali o potenziali clienti, infatti ricchi set di dati dei consumatori possono migliorare le capacità di marketing delle imprese, indirizzando ad esempio specifici mercati o clienti target e abbassando i costi pubblicitari (Blattberg e Deighton, 1991).

Le imprese possono inoltre aumentare i ricavi attraverso le offerte mirate (Acquisti e Varian, 2005), strategie innovative di coupon (considerate, ad esempio, il recente successo di iniziative come Groupon.com) e il miglioramento del CRM (Richards Jones, 2008), nonché una maggiore fidelizzazione del consumatore (Ball, 2006). Analizzando una grande quantità di dati sui consumatori, le aziende sono in grado di prevedere i trend aggregati (come le variazioni della domanda dei consumatori) e le preferenze degli individui (Linden, 2003), minimizzando così i rischi di inventario e massimizzando i ritorni sugli investimenti di marketing e possono migliorare la loro capacità di offrire consigli utili ai consumatori (Bennett e Lanning, 2007).

In definitiva, se osserviamo il comportamento individuale, le aziende possono apprendere come migliorare i loro servizi, e di conseguenza riprogettarlo per trarre vantaggio dal comportamento osservato: un esempio di come le informazioni dei consumatori possono essere sfruttate per ottenere maggiori profitti è la pubblicità online.

Come è oramai noto alla maggior parte della popolazione, il mercato del l'e-commerce e la pubblicità online ammontano a $300 miliardi all'anno negli Stati Uniti, fornendo occupazione a 3,1 milioni di americani (Deighton e Quelch, 2009). Gli annunci online possono essere indirizzati a ciascun individuo in base al suo comportamento online (come le sue ricerche, i siti visitati) e grazie ad inferenze fatte attraverso quei dati. Tale capacità di targetizzare così i segmenti di mercato di maggior interesse, implica che le imprese riducono il costo degli annunci sprecati sui consumatori che difficilmente saranno ricettivi nei loro confronti. Inoltre, poiché l'esposizione degli annunci online, il comportamento di click-through e talvolta anche il comportamento online post-esposizione sono spesso misurabili, gli inserzionisti possono monitorare e migliorare l'efficacia della pubblicità online più che in altri canali di marketing. In primo luogo, ciò consente maggiori guadagni per i marketer e i commercianti (il prezzo della pubblicità mirata al comportamento è quasi 3 volte più il prezzo della pubblicità non mirata: vedi Beales (2010)).

Secondariamente, ciò può anche avvantaggiare il consumatore: la pubblicità mirata può fornire ai consumatori informazioni utili, poiché le pubblicità sono adattate agli interessi dei consumatori. Pertanto, tale targeting può ridurre il costo di comunicazione dei produttori con i consumatori e il costo dei consumatori di ottenere informazioni utili (Lenard e Rubin, 2009). A loro volta, i ricavi da pubblicità mirata e non mirata possono

supportare nuovi servizi e modelli di business, contenuti gratuiti o prodotti a basso costo a vantaggio sia dei consumatori che delle aziende.
Un chiaro esempio ci viene fornito dal settore della riscossione dei crediti, il quale ci offre un altro esempio di come la raccolta e l'analisi dei flussi di dati dei consumatori possano migliorare il benessere. In questo settore le informazioni raccolte, analizzate e poi rivendute dalle agenzie di segnalazione del credito sono utilizzate per allocare il credito in modo efficiente tra i potenziali mutuatari, fornendo quindi valore aggiunto al mercato e ai consumatori stessi (Rubin e Leonard, 2001). Anche le organizzazioni traggono benefici indiretti dai dati dei consumatori vendendoli ad altre aziende. Questo può essere il caso anche per le imprese il cui prodotto principale non è dato dai consumatori, ma che tuttavia trovano nei dati dei loro clienti un patrimonio negoziabile di interesse per altre organizzazioni. È il caso più naturale, tuttavia, delle imprese del Web 2.0, come, ad esempio, i social network online: per tali aziende, i dati dei consumatori sono il bene principale e quindi i loro utenti diventano, in effetti, il prodotto. L'aggregazione dei dati dei singoli consumatori può avvantaggiare le imprese anche quando i dati non sono identificati personalmente: se vediamo il caso di aziende come comScore, ad esempio, queste analizzano le tendenze del web combinando osservazioni comportamentali e di indagine di milioni di consumatori online, e quindi forniscono ai propri clienti dati che possono essere successivamente utilizzati per azioni di intelligence competitiva, test di mercato ed analisi della segmentazione.
Vediamo adesso l'altro lato della medaglia, dopo i benefici analizzeremo i costi che derivano dai dati non forniti alle aziende, organizzazioni od altri soggetti interessati dai consumatori.
Infatti i costi di opportunità e le inefficienze possono insorgere quando non si verificano divulgazioni di dati che migliorino il benessere. Ad esempio, le imprese che non hanno accesso ai dati dei consumatori possono incontrare notevoli ostacoli all'ingresso nel marcato e svantaggi competitivi nei confronti delle imprese con più ampie basi di clienti, limitando così il normale svolgimento della concorrenza.
Un altro punto che va in questa direzione sono le politiche sulla privacy di opt-in obbligatorie per determinati tipi di dati, che possono essere costose per le imprese, quando comportano la perdita di dati preziosi (Staten e Cate, 2003). Inoltre, la mancanza di dati sui consumatori potrebbe rendere più difficile per le aziende innovare e offrire nuovi servizi. Per lo stesso motivo, l'incertezza o il timore di possibili ritorsioni legali a seguito della raccolta o del trattamento dei dati dei consumatori potrebbe ostacolare l'innovazione del prodotto. Allo stesso modo, i costi dei dati non divulgati possono essere danneggiati dalla società in generale.
Un altro centro di costo sono quelli derivanti dalla raccolta di informazioni, infatti i benefici dei dati divulgati che abbiamo evidenziato nei paragrafi precedenti, devono essere ponderati rispetto al costo degli investimenti necessari per raccogliere ed elaborare tali dati. Questi costi sono economicamente giustificabili quando le imprese si aspettano di ottenere maggiori vantaggi dall'analisi dei dati dei consumatori, evitando al tempo stesso i costi che potrebbero derivare dai loro abusi. I costi di raccolta e archiviazione dei dati sono stati costantemente ridotti grazie all'evoluzione dei sistemi di ultima generazione; tuttavia, l'implementazione di

sistemi che fanno un uso efficiente di tali dati non è banale. Ad esempio, l'impatto della gestione delle relazioni con i clienti (CRM) sulle prestazioni aziendali rimane un argomento in auge tra i ricercatori anche se recenti scoperte hanno portato alla conclusione che l'implementazione del CRM è associata a un aumento dell'efficienza dei profitti, ma a un calo dell'efficienza dei costi.
In questo paragrafo abbiamo visto che i benefici ed i costi legati al possesso o meno di dati sensibili ai consumatori, possono avere un fortissimo impatto nelle scelte di business delle aziende. Per questo far sentire i consumatori maggiormente protetti, potrebbe risultare fondamentale per i soggetti di business, in quanto ne trarrebbero conseguentemente un vantaggio non indifferente. Per ciò che invece riguarda questo progetto di ricerca, vedere quali sono i principali centri di costo, e quali sono i potenziali benefici derivanti dalla raccolta dei dati, serve a comprendere l'importanza che il tema riveste oggi nella società economica.

2.4 Dichiarazioni e comportamenti dei consumatori: coerenza o irrazionalità?

2.4.1 Dicotomia tra privacy attitude e privacy behavior

Nei prossimi paragrafi indagheremo sulle importanti dicotomie e contraddizioni presenti nello scenario della privacy. Fare questa analisi è utile alla nostra ricerca in quanto capire che nonostante i timori dichiarati dai consumatori, circa la sicurezza e la protezione delle proprie informazioni personali, gli stessi spesso mettono in atto comportamenti contrastanti con le dichiarazioni, e quindi le aziende facendo leva sui giusti fattori, possono influenzare le decisioni degli individui a proprio favore.
Già nel primo capitolo importante fare un'introduzione sul concetto di Privacy Paradox, ovvero quel fenomeno sempre più comune, per cui la maggior parte degli individui, seppur mostrino importanti preoccupazioni inerenti alla protezione dei propri dati (in particolare quando questi vengono usati dalle aziende per scopi commerciali e di marketing), mettono successivamente in pratica comportamenti ed atteggiamenti non coerenti con tali preoccupazioni, rilasciando quindi i propri dati senza ricevere in cambio le giuste rassicurazioni dagli operatori del mercato.
La domanda che agli esperti e non, deve sorgere spontanea è la seguente: "Sono realmente interessate gli individui ai temi legati alla propria privacy o è solo un loro costrutto mentale che non trova poi coerenza pratica?" (Kokoksis, 2015).
Gli individui infatti rivelano informazioni personali e sensibili per "premi"/ricompense relativamente insignificanti o comunque non determinanti, spesso per raggiungere picchi di visibilità negli ambienti online, in particolare nei social network. Evidenze empiriche hanno infatti dimostrato che gli individui sono mediamente disponibili nel trattare e negoziare le proprie informazioni sensibili, nonostante le preoccupazioni dichiarate.
Un esempio in questa direzione

è il fatto che il valore degli users su Internet si aggira intorno ad una cifra di 7 euro, che corrisponde al prezzo di un pasto consumato da McDonald. Continuando però a cavalcare l'onda di questo paradosso legato alla privacy, dall'altre parte ricerche sulle attitudini degli utenti online, mostrano che quest'ultimi sono seriamente preoccupati per la loro privacy e la raccolta ed uso che viene fatto dalle aziende dei loro dati più intimi.
Come dicevo, questa dicotomia tra l'attitudine verso le proprie informazioni di privacy ed il comportamento reale, ha portato a coniare la definizione "Privacy Paradox2 (Norberg, 2007), o per essere più precisi "Information Privacy Paradox".
Questa cosa si ripercuote naturalmente in implicazioni significative per l'E-commerce, E-Government, mondo dei social network, e per i regolamenti statali.
Molti dei più influenti ricercatori hanno tentato di testare ipotesi su questo paradosso, cercando quindi di dare una spiegazione. Sfortunatamente però, molti dei risultati che sono emersi da queste survey sono estremamente contraddittori tra di loro, complicando così il lavoro, e facendo sì che oggi non esista una spiegazione univoca al fenomeno.
In molti degli studi citati, il paradosso si riferisce alla dicotomia detta precedentemente, quella tra privacy attitude e privacy behaviour. Altri invece hanno stretto questa dicotomia al privacy behaviour ed alle privacy concerns. Questi due costrutti è vero che sono molto simili tra di loro, ma hanno importanti differenze. Privacy concerns può essere infatti considerata un costrutto abbastanza generale, e nella maggior parte dei casi, non viene inserita in nessuno specifico costesto. Gli atteggiamenti nei confronti della privacy invece si riferiscono alla valutazione di comportamenti specifici, e quindi sono inquadrabili in un contesto sicuramente più preciso e determinato rispetto alle privacy concerns.
Importante per comprendere al meglio il nostro tema, è fare un'altra distinzione all'interno di questo mondo. Bisogna distinguere infatti tra privacy behaviour and privacy intention (Kokolakis, 2015).
Molti studi e ricerche si sono infatti concentrate sulla privacy intention piuttosto che sul privacy behaviour. Questi studi però lasciano dietro di loro un'importante dinamica che per noi risulta invece fondamentale, ovvero il fatto che molto spesso accade che la privacy intentions non conducono minimamente l'individuo ad adottare un comportamento di protezione nei confronti delle proprie informazioni più sensibili.
Negli ultimo decenni il dibattito legato al paradosso della privacy è sensibilmente cresciuto, andando a ricoprire un ruolo di interesse primario per moltissimi soggetti, come abbiamo già visto precedentemente. Nel 2001 uno studio su internet si concentrò sull'esplorazione del boom di popolarità che stava acquisendo lo shopping online, e sulle preoccupazioni degli utenti del web sulla propria privacy e sulla propria sicurezza (Brown, 2001). In questo studio, attraverso una serie ben programmata di in-depth interviews con utenti che si erano dimostrati shoppers online, si scopre quello che venne definito "una sorta di paradosso della privacy".
Grazie a questa ricerca venne constatato che mentre la maggior parte degli individui mostravano una grande preoccupazione sulla privacy, e paura che questa venisse infranta dalle aziende, erano comunque disponibili a rilasciare i propri dati personali, spesso anche molto dettagliati, ai retailers online, quando questi avevano

qualcosa da concedergli in cambio. Gli intervistati e partecipanti alle interviste dichiaravano infatti di avere sì paura che le loro informazioni venissero raccolte, ma successivamente aggiungevano che questa ragione non li avrebbe di certo fermati nei loro acquisti online, dando quindi un'importanza primaria ai benefit che ricevevano da questa attività di consumo. Una prima motivazione di questo comportamento contraddittorio possiamo incontrarla infatti, nel fatto chei gli users dichiaravano di usare molto di frequente delle carte fedeltà, con sconti e regali anche minimi, che le aziende concedevano in cambio dei loro acquisti online. Questa scoperta era inoltre anche in linea con studi precedenti sulle loyalty cards negli Stati Uniti d'America, che mostravano che gli acquirenti erano aperti a negoziare le proprie informazioni sui loro acquisti in cambio di risparmiare davanti alla cassa (Sayre e Horne, 2000).

Anche i risultati di un altro studio ci rivelano la relazione che esiste tra privacy preferences ed actual behaviour nel vasto mondo dell' e-commerce (Spiekermann , 2008). Questo studio riguardava un esperimento per comparare le preferenze sulla privacy spontaneamente dichiarate, con il comportamento di apertura e divulgazione dei propri dati effettivamente messo in pratica durante alcune delle fasi dello shopping online. Venne chiesto per prima cosa ai partecipanti dell'esperimento di completare un questionario che aveva al suo interno domande per definire l'atteggiamento e le preferenze verso la privacy, e solamente dopo la compilazione completa, dovevano gli stessi partecipanti visitare un classico sito di shopping online. Inoltre durante la loro visita all'interno del negozio virtuale, i partecipanti venivano impegnati in un dialogo di vendita con un bot 3D. Durante la conversazione con il bot, venne rivelato che i partecipanti rispondevano tranquillamente alla maggior parte delle domande, anche se alcune di queste riguardavano aspetti altamente personali. Tutto questo ci indica che anche se gli users di Internet e degi store virtuali dichiarano che la privacy è una questione di primaria importanza, il loro comportamento non conduce alla stessa deduzione.

Altre evidenze fondamentali per la nostra tesi, ce le procura l'approccio al comportamento economico. "Gli individui non sarebbero capaci di attuare come agenti economici razionali quando le questioni riguardano la privacy personale" (Acquisti, 2004). Secondo questo approccio la maggior parte delle decisioni relative alla privacy vengono "sporcate" da informazioni incomplete, limiti della razionalità e biases psicologici (come ad esempio sconti iperbolici e bias confirmatori).

Venne costruito un modello economico che spiega parzialmente l'inconsistenza della relazione tra attitudini e comportamenti verso la privacy, e questo modello incorpora il bias della gratificazione immediata che fa riferimento alla tendenza che moltissimi individui posseggono, di valutare maggiormente i benefici nel presente, piuttosto che i rischi del futuro.

Pertanto, nella valutazione euristica delle persone, i benefici attuali della divulgazione delle informazioni, superano i rischi futuri della privacy. Inoltre, i "sofisticati avvocati della privacy" potrebbero rendersi conto che proteggere se stessi da ogni possibile intrusione sulla privacy non è realistico, perciò potrebbero non essere disposti ad adottare una rigorosa strategia di protezione della privacy, poiché dubitano che alla fine pagherà, in quanto questa strategia potrebbe rivelarsi stancante e non fruttuosa.

Per dare seguito a questi assunti, sono stati raccolti una grande quantità di dati a supporto delle ipotesi del modello, sul fatto che le decisioni sulle questioni legate alla privacy, sono affette dai fattori detti in precedenza, cioè informazioni incomplete, limiti della razionalità e biases psicologici (Acquisti Grossklags, 2005). Il modello in analisi pone l'evidenza sulla dicotomia che interessa per la nostra tesi, cioè quella tra privacy attitude vs. privacy behaviour: infatti nonostante molti dei soggetti dei loro studi (89% dei rispondenti) riportano di essere moderatamente o altamente preoccupati per la loro privacy, il 31% del campione ammette poi di avere rivelato almeno una volta nel passato, il loro numero sociale di sicurezza per ricevere sconti o servizi migliori, e più del 28% hanno dato il loro numero di telefono a commercianti ed altre figure di marketing simili.

Un altro grande gruppo di ricerche negli ultimi anni, è andato a concentrarsi sul capire il comportamento di auto – divulgazione all'interno della marea di social networks online, che sono venuti fuori nell'era digitale, e che hanno riscontrato enorme successo specialmente tra le giovani generazioni. Anche questo tema si introduce all'interno del paradosso della privacy.

Viene usato il termine privacy paradox per riferirsi al comportamento sulla privacy dei giovani nei siti di social networks, i così comunemente denominati dagli esperti con l'acronimo di SNSs (Bernes, 2006). Vediamo che le giovani generazioni tendono a non realizzare a livello mentale, che i SNSs agiscono e si muovono in uno spazio pubblico e rivelano informazioni sensibili e personali che potrebbero essere misurate ed usate.

I principali studi qu questo aspetto sono stati due, ognuno dei quali era composto di due fasi.

Nella prima fase il team di ricercatori sottoponeva delle domande ad il campione di studenti in questione, circa la loro reale disponibilità di rivelare alcune specifiche informazioni personali (Norberg, 2013). La fase numero due di questi studi invece aveva luogo a diverse settimane di distanza dalla fase descritta di sopra, e qua agli stessi soggetti di prima veniva chiesto di fornire proprio lo stesso tipo di informazioni su cui erano stati interrogati. Questo studio conferma le ipotesi che gli individui in realtà rivelano un numero significativo di informazioni estremamente personali e sensibili, rispetto a ciò che loro dichiarano in relazione con questo tema.

Uno dei problemi è che le informazioni personali non sono un qualcosa di coerente e ben definito univocamente, ma esistono diversi tipi di informazioni personali e le persone attribuiscono valutazioni diverse a loro. Dati come posizione, stato di salute, cronologia di navigazione, età e peso sono trattati in modo diverso dalle persone.

Pertanto, non è appropriato confrontare studi che si riferiscono a diversi tipi di informazioni personali. La sensibilità delle informazioni è un moderatore importante che viene spesso trascurato e, come suggeriscono che il paradosso della privacy può derivare da una mancata considerazione della sensibilità delle informazioni (Mothersbaugh, 2012). Allo stesso modo, ci sono diversi tipi di preoccupazioni sulla privacy, come quelle sulle minacce sociali (incluso il bullismo e lo stalking), le minacce organizzative (incluso l'uso secondario da parte

del raccoglitore di dati, l'uso secondario da parte di terzi e il marketing) e l'accesso improprio da parte dei datori di lavoro o il pubblico (Krasnova, 2009).
Il secondo studio del team di Norberg, ha seguito come dicevamo lo stesso iter e le stesse metodologie del precedente, ma questa volta andava a testare l'effetto della percezione di rischio sull'intenzione di rivelare informazioni personali, e l'effetto di percezione di fiducia sul comportamento reale messo in atto verso la propria privacy. Ciò venne evidenziato con questo studio fu l'evidenza a supporto della relazione esistente tra rischio ed intenzione, concetto che però è necessario in futuro esplorare ancora per avere evidenze empiriche inconfutabili.

2.4.2 Il concetto di privacy ed il relativo valore monetario

Adesso andremo a vedere qua di seguito una serie di studi effettuati dagli esperti, che hanno l'obbiettivo di attribuire un valore reale e monetario al concetto di privacy per una determinata segmentazione della popolazione. Molti degli esperti si sono andati a misurare con degli studi che miravano a determinare un reale valore per le informazioni personali, e ciò che questi hanno indicato sono state valutazioni molto basse che non giustificavano gli elevati dubbi sulla privacy espressi dalle persone nei sondaggi e nelle indagini.
Sono stati condotti una serie di aste sperimentali per ottenere il valore che le persone attribuiscono ai loro dati privati. In queste aste i partecipanti hanno indicato un prezzo per i loro dati e la persona che ha richiesto il minimo ha ricevuto il secondo prezzo più basso richiesto (Huberman, 2005). Le informazioni messe all'asta erano il peso e l'età. Il prezzo medio della domanda per età era $ 57,56 contro $ 74,06 per il peso.
L'esperimento ha anche rivelato una tendenza a una valutazione più elevata delle informazioni sul peso quando è percepito come imbarazzante e, come previsto, i giovani erano maggiormente disposti a rivelare la loro età rispetto a ai soggetti più anziani.
In un altro esperimento i soggetti hanno affrontato situazioni di compromesso, dove è stato chiesto loro di scegliere tra protezione della privacy incompleta e vantaggi come la convenienza o le promozioni (Hann, 2007). In questo studio è stato stimato che la protezione dagli errori nei registri personali, l'accesso improprio alle informazioni personali e l'uso secondario di informazioni personali valgono tra $ 30,49 e $ 44,62.
Vediamo ora un altro studio interessante per indagare sul valore reale dato dagli individui alle proprie informazioni personali, con l'obiettivo di determinare il valore monetario di diversi tipi di informazioni personali. (Carrascal, 2013). Utilizzando un plug-in del browser Web, gli studiosi hanno spinto gli utenti a valutare i propri dati personali nel momento e nel luogo in cui sono stati generati. Nella prima fase dell'esperimento, il plug-in aveva l'obiettivo di raccogliere dati sul comportamento di navigazione di ciascun soggetto in questione per la riuscita di questo studio che vi stiamo raccontando. Questi dati sono stati utilizzati successivamente per calibrare il comportamento del plug-in nella seconda fase, nella quale il plug-in visualizzava popup mentre i partecipanti navigavano in Internet. I popup contenevano due tipi di domande:

domande sulla valutazione delle informazioni personali e domande sulle percezioni e sulla conoscenza della privacy dei partecipanti. Le domande di valutazione delle informazioni sono state inquadrate come aste., ad esempio, una domanda era "Qual è l'ammontare minimo di denaro che accetteresti per la vendita di 10 delle foto che hai caricato su questo sito Web a una società privata?".

L'esperimento si è concluso con un questionario post-studio, i cui risultati mostrano valutazioni significativamente basse delle informazioni personali, dove gli utenti valutano la loro cronologia di navigazione in media a 7 euro. Per quanto riguarda invece le informazioni personali offline, come età, indirizzo e stato economico, la valutazione media è di circa 25 euro. Gli utenti hanno fornito valutazioni più elevate dei dati relativi alle interazioni nei social network (12 euro) e nei siti web finanziari (15,5 euro), rispetto ad attività come la ricerca (2 euro) e lo shopping (5 euro).

Sembra dall'analisi di questi studi, che i consumatori siano disposti a pagare un prezzo per la privacy, anche se piccola. Successivamente due esperimenti con utenti di smartphone hanno mostrato che, scegliendo tra applicazioni con funzionalità simili, i partecipanti attenti alla privacy erano disposti a pagare un sovrapprezzo di $ 1,50 su un prezzo iniziale di $ 0,49 (Egelman, 2012).

Tutti gli studi summenzionati forniscono prove che supportano l'ipotesi di una dicotomia paradossale tra atteggiamenti di privacy e comportamento sulla privacy, ma diversi ricercatori hanno fornito prove che sollevano dubbi sull'esistenza di un paradosso della privacy.

Le persone rivelano informazioni personali quando ne traggono beneficio, ma allo stesso tempo sono significativamente influenzate dal modo in cui queste informazioni vengono gestite. Infatti sono seriamente preoccupati per l'uso secondario di dati personali e queste preoccupazioni portano a un comportamento prudente.

Il numero di studi interessati al fenomeno abbiamo visto come sia molto importante e decisamente popolato, per questo riteniamo che il fenomeno sia di estremo interesse nella ricerca che stiamo portando avanti, e soprattutto che siano ancora molti i gaps che potrebbero essere colmati nel futuro prossimo.

Per quanto riguarda le teorie di fondo sebbene il paradosso della privacy sia stato studiato attraverso una varietà di obiettivi teorici, nessun modello teorico ha prevalso, quindi c'è ancora spazio per nuove prospettive teoriche. In particolare, ci sono diverse teorie della scienza comportamentale che potrebbero essere considerate, come la teoria cognitiva sociale e i suoi derivati (Bandura, 2001).

Infine, potremmo notare che il paradosso della privacy è stato studiato isolatamente. Il rapporto tra comportamento della privacy e campagne di sensibilizzazione sulla privacy, con l'ambiente tecnologico e la disponibilità di tecnologie che migliorano la privacy, è stato sottovalutato.

Inoltre, una migliore comprensione del paradosso della privacy può consentire una nuova prospettiva sul quadro giuridico ed etico della riservatezza delle informazioni.

Concludendo, potremmo obiettare che sebbene ci sia stato un ampio volume di ricerche sul paradosso della privacy, rimane un problema decisamente aperto.

2.5 Fattori che facilitano la disclosure dei dati.

2.5.1 La teoria dello scambio e la teoria della decisione

Il mondo del data privacy, cerca in continuazione di esplorare quali sono quelle condizioni o situazioni che rendono i consumatori disponibili, o viceversa, nel rivelare le loro informazioni sensibili.
Queste condizioni, o per meglio definirli, questi fattori hanno un ruolo primario nella ricerca di tesi che stiamo effettuando, in quanto determinare con certezza quali questi siano, faciliterebbe le imprese ed altri soggetti interessati, nella gestione della privacy. Tutto questo perché presentando questi fattori al pubblico, risulterebbe molto più semplice ottenere informazioni personali dei consumatori. Questa tesi cerca di dimostrare proprio come alcuni fattori, in particolare il senso di appartenenza ad una certa community online, superi nella mente dei consumatori le preoccupazioni legate alla privacy, e dichiarare così le proprie informazioni sensibili.
In questo contesto hanno recentemente guadagnato sempre maggior importanza e rispetto la teoria dello scambio e la teoria della decisione, con risultati eccellenti raggiunti nel corso del tempo. A differenza della teoria del contratto sociale, che pone molta enfasi sulle norme che regolano le domande sulla privacy agli stakeholder, queste teorie affrontano invece il tema calcolando razionali sulla relazione costi-benefici che i consumatori calcolano e tengono in considerazione pensando alla loro privacy. In particolare queste teorie ci dicono che gli individui ponderano le conseguenze della divulgazione delle informazioni personali rispetto al valore di ciò che gli viene offerto in cambio dai marketers.
Soprattutto la teoria dello scambio ci dice che i consumatori sono più disponibili a rilasciare informazioni personali quando il beneficio percepito, è maggiore del costo, mentre la teoria delle decisioni, che come sappiamo rientra all'interno della più famosa teoria del prospetto, considera prevalentemente la valutazione del singolo individuo circa le perdite ed i guadagni all'interno delle decisioni di rischio (Gabisch e Milne, 2014).
Per inquadrare al meglio ciò che stiamo dicendo, è importante vedere con attenzione il seguente esempio che riguarda lo scambio di informazioni. Come vediamo da questo studio, i consumatori statunitensi sono realmente disposti a pagare una cifra tra 30 e 45 dollari per proteggere la loro privacy in contesti che essi ritengono di uso secondario (Hann, 2007). Altri segmenti di consumatori invece, erano più pragmatici ed erano disposti a scambiarsi informazioni personali in maniera più smart e conveniente, se in cambio percepivano un beneficio per loro importante.
Un altro esperimento da inserire all'interno dello scambio di informazioni, ci dice che dati sensibili dei consumatori era possibile ottenerli attraverso l'uso di un'interfaccia tecnologica, che agli occhi degli individui si fosse "comportata" secondo le principali norme sociali dell'interazione umana, così da suscitare un senso di reciprocità (Moon, 2000).
Un risultato importante raggiunto dagli esperti ci dice che essere consapevoli di tutti i rischi delle politiche sulla privacy delle organizzazioni, rende i consumatori meno disponibili a rilasciare le proprie informazioni, e

che al contrario la gran parte dei partecipanti era disponibile a rivelare i propri quando credevano che anche gli altri lo avrebbero fatto (Acquisti, 2012).
Vediamo adesso un altro aspetto fondamentale nel processo di disponibilità a rivelare i propri dati personali. Viene riconosciuta dalla maggior parte degli esperti, una propensione del consumatore medio, nel fornire informazioni false, o che comunque possono trarre in inganno in qualche modo, causando così notevoli problemi alle aziende che fanno di questo tema un aspetto fondamentale del loro business.
Nel contesto della privacy delle informazioni, la teoria della reazione può spiegare con precisione la risposta di alcuni consumatori a messaggi di marketing altamente mirati e personalizzati, che credono possano comprometterne la privacy (Tucker, 2014). Le reazioni che riscontriamo nei consumatori alle comunicazioni personali di marketing, possono portare ad un'elusione della comunicazione stessa, alla falsificazione delle informazioni rivelate, ad un passaparola dispregiativo che può causare gravi danni alle aziende, ed altri comportamenti negativi (White, 2008). Queste risposte dei consumatori emergono come azioni contrarie ed involontarie agli appelli di marketing, che invece dovrebbero (o almeno vorrebbero) suscitare sentimenti di ben altro valore e benefici per le azioni di marketing personalizzate (Goldfarband, 2011).
È più probabile che i consumatori abbiano reazioni negative quando percepiscono uno sbilanciamento di poteri relativo alle pratiche sulla privacy che utilizzano le organizzazioni (Lwin, 2007).
Un flusso parallelo di ricerche esamina le intenzioni di acquisto come il risultato principale delle preoccupazioni sulla privacy, piuttosto che della divulgazione delle informazioni. Le dichiarazioni sulla politica sulla privacy aumentano la benevolenza e l'integrità della fiducia dei consumatori, ma vediamo che queste non aumentano la volontà di acquistare.Tuttavia, questa ricerca e il lavoro correlato rilevano che la privacy, la sicurezza e altre informazioni valutate come più pertinenti e vantaggiose per i consumatori migliorano sensibilmente l'intenzione di acquisto positiva (Miyazaki e Fernandez, 2000).
Considerando infatti la misura in cui i marketer possono oggi accedere a enormi quantità di informazioni sui consumatori, indipendentemente dal fatto che tali informazioni siano fornite volontariamente o meno (Nill e Aalberts2014), la disponibilità a rivelare sembra essere in calo, stando al pensiero della maggior parte degli esperti.
Più recentemente, i ricercatori di marketing hanno iniziato a riconoscere che l'acquisto o l'intenzione di acquisto, non è sempre il risultato aziendale rilevante di interesse per le domande sulla privacy dei dati. Per molte aziende (ad es., Facebook e Instagram) che offrono servizi digitali gratuiti, i dati sono le loro principali fonti di valore con cui ricavare introiti e assicurare una performance positiva nel mercato azionario.
Pertanto, la ricerca emergente ha esaminato le questioni relative all'accettazione pubblicitaria e all'utilizzo dei servizi in relazione alle norme sulla privacy.Ad esempio, vediamo come il risultato di una ricerca valuta la misura in cui i consumatori accetteranno varie forme di pubblicità in cambio di un servizio online gratuito (Schumann, 2014).

È importante sottolineare che questo studio è stato uno dei primi a scoprire che i consumatori sono disposti a sopportare con molta più facilità una determinata pubblicità, quando questa è più mirata, essendo di conseguenza maggior disponibili nel cedere parte della loro privacy, come il prezzo giusto a cui sottostare per la personalizzazione delle azioni e delle comunicazioni e per la concessione di servizi gratuiti.

2.5.2 La fiducia

Fondamentale per questo progetto di tesi saranno i prossimi paragrafi, nei quali andremo ad indagare quali sono quei fattori che migliorano la percezione della privacy nei consumatori.
A supporto delle evidenze che qua riporteremo, ci saranno una serie di studi e di paper redatti dai principali esperti del tema, così da poter assicurare una veridicità ed una credibilità maggiori ai nostri assunti. In accordo con quasi la totalità degli esperti di marketing sono principalmente tre i fattori che esercitano una certa influenza positiva nei consumatori, che li portano a rilasciare le proprie informazioni.
Questi fattori di cui sto parlando sono: la fiducia, il controllo e la personalizzazione.
Per prima cosa andiamo a vedere in profondità tutti gli aspetti che sono legati alla "fiducia" dei consumatori, che come vedremo è considerato uno dei primi driver per i consumatori per rivelare i propri dati alle aziende.
In un contesto in cui la privacy è molto importante, la fiducia promuove risultati di marketing molto positivi, incluso la maggior disponibilità dei consumatori nel rilascio delle proprie informazioni, nell'intenzione di acquisto, nel CTR (Click-throug-rate) e nell'accettare con un mood positivo la pubblicità.
Oltre a venire spesso suggerita come antecedente delle preoccupazioni dei consumatori, la fiducia è stata anche spesso esaminata come un meccanismo di mediazione primario per la disponibilità dei consumatori ad impegnarsi con un' azienda o con una determinata organizzazione in una piattaforma online o in una piattaforma mobile (Aiken e Boush, 2006). Questi lavori trascinano letteralmente il concetto della fiducia ad avere un ruolo dominante nelle varie ricerche e studi sulla privacy.
Un esempio lampante e che tutti noi abbiamo quotidianamente sotto gli occhi, è l'uso esagerato da parte delle organizzazioni, di tecnologie che compromettono la privacy, come lo sono i cookie, che stando ai risultati di molti studi, danneggiano la fiducia dei consumatori e riducono sensibilmente le intenzioni di acquisto (Miyazaki, 2008). Gli sforzi che fanno le aziende per migliorare la fiducia nei loro confronti, sono da considerare come meccanismi di promozione, che possono cambiare l'immagine dell'azienda nella mente del consumatore (Wirtz e Lwin, 2009).
Quindi la fiducia abbiamo visto che può promuovere sia la rivelazione dei dati personali e in particolare incoraggiano la formazione della relazione tra le aziende ed i propri clienti, in un contesto rilevante per i discorsi relativi alla privacy. Più di recente è stato notato che la fiducia riveste un ruolo privilegiato per alleviare le preoccupazioni sulla privacy, in un ambiente in cui i retailers hanno sempre di più targetizzato e/o personalizzato i diversi contenuti per i consumatori (Bleier e Eisenbeiss, 2005). Aggiungiamo che anche se

spesso i consumatori sono molto frequentemente vulnerabili sul tema, una variabile che incrementa la fiducia è ovviamente la trasparenza, che regala una maggiore tranquillità agli individui.
Una forte relazione vedremo adesso che esiste all'interno della relazione che si creano tra le politiche sulla privacy delle aziende e la fiducia. Le aziende possono utilizzare diversi modi per costruire la fiducia dei consumatori nei loro siti web, tra cui un sigillo elettronico per le transazioni finanziarie che forniscono la prova della sicurezza dei dati del sito Web.
È stato confermato che una relazione di successo tra acquirente e venditore dipende dal livello di fiducia dell'acquirente che viene mostrato nel loro modello di intimità della privacy (Lu e Yu, 2004); questo modello spiega come la privacy influenza la fiducia e quindi la fiducia influenza a sua volta l'intenzione comportamentale del consumatore per le transazioni online.
Le relazioni tra le dimensioni della privacy e la fiducia sono risultate significative, ma il modello non suggerisce quale tipo di contenuto o quale formato deve avere una politica sulla privacy. Alcuni studi sostengono che per creare fiducia, le politiche sulla privacy dovrebbero essere informative e rassicurare i consumatori sul fatto che divulgare le loro informazioni personali è una proposta a basso rischio (Dinev e Hart, 2006).
È stato inoltre osservato che una politica sulla privacy chiara e credibile aiuta i professionisti del marketing a creare una reputazione positiva con i consumatori (Schoenbachler e Gordon, 2002).
Esistono molte prove che mostrano relazioni significative tra fiducia e preoccupazione per la privacy, indipendentemente dal fatto di fornire informazioni personali online.
Come è facilmente immaginabile, anche l'E-commerce viene toccato da queste problematiche. Molti ricercatori propongono che le preoccupazioni per la riservatezza delle informazioni costituiscono un ostacolo enorme per le imprese che fanno dell'e-commerce il proprio core-business. Gli esperti prevedono che potrebbero essere prodotti più di un trilione di dollari di e-commerce se le preoccupazioni dei clienti per la privacy fossero minori (Odom, 2002).
Completare una transazione senza rivelare alcuni dati personali è molto difficile, anche se questa divulgazione viene fatta a una terza parte fidata, quindi la privacy diventa una preoccupazione necessaria per l'e-commerce (Ackerman, 1999). Senza persone fidate che conservano dati personali che impediscono ad altri di vedere o utilizzare tali dati, crescenti percezioni di fiducia influenzeranno la privacy per consentire al cliente di determinare che i benefici della divulgazione delle informazioni personali superano i rischi (Luo, 2002). Inoltre la fiducia viene vissuta come un precedente di condivisione delle informazioni, che riduce la preoccupazione per la privacy.
Vediamo adesso un modello interessante, che aggiunge alla relazione esistente tra privacy e fiducia, anche la variabile della familiarità. Il modello di calcolo della privacy esteso mostra forti relazioni positive tra fiducia e disponibilità degli utenti a fornire informazioni personali durante le attività di Internet (Dinev e Hart, 2006)

Ci sono molti studi di ricerca condotti che identificano le dimensioni della fiducia in Hyperspace. Alcuni di loro sono familiarità, fiducia negli scambi e fiducia nella riservatezza delle informazioni. la familiarità è una condizione necessaria di fiducia ed esistono forti relazioni positive tra un alto livello di familiarità ed un alto livello di fiducia. (Luhmann, 1979).
In altre ricerche, la familiarità è stata trovata come un antecedente della fiducia (Bhattacherjee, 2002). La riservatezza della privacy delle informazioni viene violata dal tracciamento non autorizzato e dalla diffusione non autorizzata di informazioni e fa riferimento alle responsabilità di protezione della privacy di un sito Web (Hoffman, Novak e Peralta, 1999). In questo modo, la fiducia può essere sviluppata attraverso l'efficace comunicazione di salvaguardie sulla privacy, segnali di mercato che trasmettono efficacemente alta reputazione e credibilità, e precedenti esperienze positive di consumo di valore percepito.
Lo sviluppo della fiducia tra i consumatori diretti e i consumatori riduce il rischio percepito dei consumatori, il che migliora la disponibilità dei consumatori a condividere le loro informazioni personali con i professionisti del marketing.

2.5.3 La personalizzazione

Come dicevamo oltre alla fiducia, ci sono altri due fattori importantissimi, che ripetiamo essere la personalizzazione ed il controllo.
La personalizzazione, che si riferisce alla "capacità di fornire contenuti e servizi che sono personalizzati per gli individui in base alla conoscenza delle loro preferenze e dei loro comportamenti" (Adomavicius e Tuzhilin, 2005), è stata riconosciuta come un concetto importante, che consente agli utenti di essere identificabili in modo univoco in base alla loro identità e alle preferenze associate, nonché alle loro posizioni (Junglas e Watson, 2003).
Dal punto di vista del marketing, la personalizzazione è anche conosciuta come "marketing one-to-one" o "individualizzazione" (Murthi e Sarkar, 2003), e si riferisce a "costruire la fedeltà dei clienti costruendo un significativo relazione one-to-one "(Riecken, 2000).
La personalizzazione dipende principalmente da due fattori, ovvero la capacità delle aziende di acquisire ed elaborare le informazioni dei clienti e la disponibilità dei clienti a condividere informazioni e utilizzare servizi personalizzati (Chellappa e Sin, 2005). Vedendo il punto delle aziende, queste vorrebbero ottenere quante più informazioni possibili sui loro clienti in modo che possano fornire prodotti o servizi personalizzati. I clienti, d'altro canto, vorrebbero ottenere prodotti o servizi personalizzati, ma dando meno informazioni possibili (Murthi e Sarkar, 2003).
Nonostante i vantaggi che la personalizzazione può fornire alle organizzazioni e ai clienti, questo concetto richiede agli utenti di rinunciare ad alcune delle loro informazioni personali a vantaggio del loro fornitore di servizi, il che solleva problemi di privacy (Roussos, 2003) e crea così un paradosso nella relazione tra privacy e

personalizzazione (Awad and Krishnan, 2006), e nonostante il valore che la personalizzazione offre ai consumatori attraverso nuovi messaggi di comunicazione, raccomandazioni di prodotti e servizi e individualizzazione, produce effetti contrastanti sui risultati dei consumatori in relazione alla propria privacy. Una domanda chiave sul trade off delle informazioni sul valore personalizzato si riferisce al fatto di capire se le informazioni siano state fornite in maniera volontaria oppure è stata ottenuto grazie all'uso di qualche escamotage di marketing, visto anche la grande capacità dei commercianti di ottenere i dati in maniera a volte chiara attraverso una varietà di mezzi (Aguirre, 2015).
La personalizzazione può portare ad un coinvolgimento maggiore attraverso il ctr, ma la raccolta di informazioni deve essere resa nota, altrimenti i consumatori potrebbero sentirsi vulnerabili.
Analogamente, l'efficacia della personalizzazione nella promozione del click-through quando i consumatori sono preoccupati per la privacy è legata ai loro sentimenti di fiducia: vediamo quindi come questi fattori, come fiducia e personalizzazione, non sono due linee parallele, ma sono elementi strettamente legati tra di loro.

2.5.4 Il controllo

Come abbiamo visto in questo capitolo, il terzo fattore che andremo ad analizzare è quello del controllo, che si riferisce al potere dei consumatori di decidere cosa viene appreso su di loro, cioè usando le parole che hanno usato gli esperti "che le persone non vengono lette senza che se ne rendano conto". Studi empirici suggeriscono che il controllo delle informazioni è fondamentale per il livello di preoccupazione per la privacy sperimentato dai consumatori.
E' stato inoltre confermato che il controllo delle informazioni sia un fattore primario nella preoccupazione dei consumatori per la privacy in un ambiente online (Sheehan e Hoy, 2009).
Vengono suggeriti due distinti motivi per la perdita della privacy relativa al controllo delle informazioni: il primo è che le persone che perdono il controllo sull'accesso mentre il secondo riguarda la mancanza di controllo sull'uso e la manutenzione delle informazioni una volta che le persone hanno rilasciato i propri dati (Spiekermann, 2011).
I consumatori che percepiscono una perdita di controllo delle informazioni nelle interazioni online personalizzate sono maggiormente suscettibili di sentirsi vulnerabili, e devono dipendere dalla benevolenza esclusivamente delle entità online per utilizzare e proteggere responsabilmente le informazioni personali del consumatore. Per questi consumatori che percepiscono una perdita di controllo delle informazioni, è probabile che la fiducia nelle entità online sia più proficua nel ridurre la preoccupazione per la privacy, rispetto a quei consumatori che percepiscono livelli più elevati di controllo delle informazioni e, pertanto, sono meno vulnerabili alle intenzioni dell'azienda sia online che offline.
In un esperimento che aveva come obiettivo di ricerca quello di misurare l'importanza del controllo, vediamo che le persone hanno rispondevano in maniera più favorevole a pubblicità maggiormente personalizzate e

targetizzate quando avevano una maggiore capacità di controllare le loro impostazioni sulla privacy personale (Tucker, 2014).
Questo risultato richiama le similitudini che suggeriscono che le persone siano più ricettive alle comunicazioni di marketing altamente personalizzate, di cui le aziende sono ora facilmente fautrici, quando hanno un certo livello di controllo sul processo di rivelazione delle informazioni (Norberg e Horne 2014). Il controllo dell'informazione percepito dai consumatori è il meccanismo focale attraverso il quale vari metodi, tra i quali troviamo la protezione da parte degli individui, l'autoregolamentazione del settore.
Il controllo può sopprimere uno spettro di variabili di privacy e anche promuovere la fiducia e ridurre la violazione emotiva in tali contesti. Tuttavia, Brandimarte (2012) i consumatori potrebbero rivelare troppe informazioni, lasciandole vulnerabili, quando percepiscono maggiori controlli (Martin, 2016).
Vediamo una volta in più come questi fattori che stiamo analizzando siano estremamente collegati tra di loro: un'azienda o chi per essa, non può fare affidamento e fare push ad esempio solo sulla fiducia, senza tenere in considerazione il controllo e la personalizzazione che vengono richiesti dai consumatori. Il modo ideale in cui fornire controlli dei consumatori nei contesti di riservatezza delle informazioni rimane una questione aperta, che sfida gli operatori di marketing e gli studiosi per la ricerca futura. Si tratta infatti di un problema alquanto delicato perché la capacità del marketer di creare percezioni di controllo non riflette necessariamente il controllo effettivo.
Poiché la reattività dei consumatori a messaggi di marketing attentamente personalizzati è altamente indesiderata per le aziende che investono in modo sostanziale in questi approcci, le strutture teoriche ed etiche che possono aiutare a illuminare la relazione privacy-controllo rappresentano un campo futuro importante per le ricerche.

2.5.5 Premi e Ricompense

Oltre a questi tre fattori che sono comunemente considerati dagli esperti come i principali motivi che spingono i consumatori a rivelare le proprie informazioni personali, c'è un quarto fattore che sta sempre più ricevendo approvazione nello scenario della privacy e del superamento delle preoccupazioni legate ad essa.
Stiamo parlando del fattore della compensazione, che come visto da un numero consistente di esperimenti, consente ai consumatori di accantonare i timori che hanno nel fornire informazioni private di dati sensibili a soggetti terzi. La cosiddetta ricompensa può essere offerta principalmente in due forme: in contanti o non in contanti.
Quella più comune è quella in denaro, la quale viene generalmente definita come erogazione di una certa somma di valuta corrente, oppure come regali o sconti sugli acquisti futuri.

Ad esempio un recente studio ha usato come ricompensa un mousepad. Questa compensazione in contanti fornisce al consumatore un beneficio esplicito e tangibile che si ritrova a dover tenere in considerazione nel calcolo della privacy (Sheehan e Hoy, 2015).
Viceversa, la compensazione non in contanti è definita come un vantaggio che non ha un valore equivalente in denaro, ma ad esempio si tratta di informazioni, assistenza o personalizzazione della propria offerta. Ad esempio, gli acquirenti online sono apparentemente disposti ad essere osservati nei propri comportamenti sul web se questi vengono utilizzati per personalizzare la propria esperienza di acquisto.
Offrendo al cliente un vantaggio, sotto forma di una ricompensa tangibile o di una ricompensa non monetaria, un'azienda può segnalare la sua benevolenza e quindi un'apertura nei confronti del consumatore. La fiducia "riguarda le aspettative del futuro ed essa matura per individui e organizzazioni a causa delle loro precedenti buone opere e chiare promesse ". Ancora una volta troviamo correlazione tra i diversi fattori o variabili, in questo caso tra fiducia e ricompensa.
Inoltre, la dimensione della fiducia basata sul calcolo suggerisce che i risultati relativi alla fiducia può essere influenzato da un beneficio o una ricompensa.
Ricerche precedenti indicano che i consumatori sono disposti a scambiare la loro privacy per alcuni benefici, ad esempio consentendo alle imprese di recupero crediti di raccogliere e diffondere informazioni in cambio dell'estensione del credito.
La letteratura sull'economia della privacy suggerisce che il processo decisionale sulla privacy è una razionalità limitata, cioè un mix di considerazioni economiche e influenze psicologiche, ed è influenzato da molti fattori ", inclusi gli atteggiamenti personali, la conoscenza dei rischi e la protezione, fiducia in altre parti, fiducia nella capacità di proteggere informazioni e considerazioni monetarie", pertanto la compensazione non influenzerà direttamente il livello di fiducia, ma piuttosto, l'offerta di indennizzo da parte dell'impresa, sia in contanti che immateriale, rafforzerà gli effetti del livello di fiducia generale del consumatore fornendo un esempio di "buona opera" e facendo una promessa implicita di benefici futuri.
In altre parole, anche se la compensazione non riduce di per sé la preoccupazione per la privacy, la presenza di un'offerta di compensazione significa che la fiducia è ancora più importante nel predire la preoccupazione della privacy del consumatore.
Infine per dare un esempio pratico vediamo l'esperimento effettuato da Taylor, Davis e Jillapally, che può donarci una visione più ampia sul tema che stiamo trattando
Consideriamo gli esempi del cliente A e del cliente B. Il cliente A ha un livello relativamente alto di fiducia nei soggetti online, che, a sua volta, riducono il livello di riservatezza durante le transazioni online. Per il cliente A, un'offerta di risarcimento aumenta la capacità della fiducia di ridurre le proprie preoccupazioni per la privacy perché la sua fiducia infonde confidenza e sicurezza che l'offerta in questione sia legittima e programmata in modo benevolo. Al contrario, il cliente B ha un livello relativamente basso di fiducia nelle interazioni online. Quando il cliente B riceve un'offerta di indennizzo personalizzato, può essere scettico sulla

legittimità dell'offerta e sulla motivazione del risarcimento. Ancora una volta, l'offerta di compensazione aumenta l'importanza della fiducia per la sua preoccupazione sulla privacy. Pertanto, in entrambe le situazioni, l'offerta di compensazione potrebbe aumentare l'influenza della fiducia in merito alla privacy.
Come abbiamo visto, questi fattori sono molto importanti, ed andranno estesi ulteriormente nel futuro in mondo da raggiungere obiettivi, tangibili o meno, che siano in linea con le aspettative di aziende ed organizzazioni.

2.6 La privacy nel mondo virtuale dei social network e delle App

2.6.1 La relazione tra utenti e social network

Tutto questo come ho detto, in particolare capire al meglio grazie alla nostra ampia bibliografia, era necessario per riuscire ad inquadrare la nostra indagine, che sarà incentrata sul mondo delle app di tracking, e sui motivi che spingono i propri users a rilasciare i propri dati sensibili, in particolare la propria posizione. In particolare, le principali che verranno studiate ed analizzate, sono quelle legate al concetto di community e quindi se e come prevalgono rispetto alle privacy concerns per i membri delle community, facendo sì che questi sviluppino sentimenti di loyalty e raccomandino le App usate ad altri utenti favorendo così un passaparola positivo.
Proprio per tutti queste ragioni puntualmente elencate, questo ultimo paragrafo è di enorme rilevanza per la nostra domanda di tesi, considerando il fatto che indagheremo sui valori comunicati dalle community online (nel nostro caso specifico quelle delle App) per superare le preoccupazioni ed i problemi legate alla privacy. Tutto questo non solo per fornire i propri dati sensibili, ma anche per controllare se queste variabili hanno un valore nei comportamenti legati alla fedeltà, alle raccomandazioni ad altri utenti, ed all'uso prolungato nel tempo delle applicazioni prese in esame.
Per questo adesso cercheremo di indagare cosa accade nel mondo dei social network, piattaforme che oramai sono entrati a gamba tesa nella nostra realtà quotidiana, e che tutti noi conosciamo benissimo. Un altro flusso di ricerca si è infatti concentrato sui social network online e sulla relazione tra preoccupazioni sulla privacy e divulgazione di informazioni nelle SNS (acronimo che come abbiamo visto sta per "Social Network Sites", e che useremo per comodità all'interno di questo progetto di ricerca).
I social network online e i siti di community sono diventati una forza sociale estremamente popolare.
Fornendo qualche dato utile a comprendere la portata del fenomeno, vediamo che le nuove registrazioni per Facebook hanno una media di 250.000 al giorno dal 2007; il numero di utenti attivi raddoppia ogni 6 mesi e più della metà degli utenti attivi utilizza il sito ogni giorno.
Nel 2009, MySpace ha registrato 130 milioni di utenti attivi, con le comunità virtuali localizzate e tradotte in 20 paesi e lingue diversi.

I social network online non rappresentano semplicemente un fenomeno sociale esplosivo, ma bensì fanno parte di una tendenza che ha grandi potenziali implicazioni per i sistemi aziendali e di informazione. Basti considerare il fatto che esistono oltre 1 milione di sviluppatori e imprenditori che hanno sviluppato più di 350.000 applicazioni commerciali per i 250 milioni di utenti attivi di Facebook.
Questi siti sono sempre più utilizzati come una fonte ideale di ricerca di marketing (Kozinets, 2002), come un modo per migliorare l'impatto del marchio e per aumentare la domanda di prodotti (Miller, 2009) .
Questa opportunità di raccogliere informazioni è particolarmente importante per le ricerche di marketing, poichè nei tradizionali approcci di ricerca di mercato, solo una piccola percentuale di persone rivela le informazioni desiderate (Robertshaw e Marr, 2006).
Inoltre, molti ricercatori di mercato oggi invocano una relazione tra il brand ed il consumatore che può essere notevolmente migliorata attraverso le interazioni online attraverso i principi dell'interazione interpersonale che possono essere creati dai siti Web.
Nel frattempo, recenti ricerche in materia di economia strategica mostrano che la partecipazione delle imprese nelle comunità online può aumentare la domanda di prodotti delle aziende (Miller, 2009). Altri usi innovativi della self-disclosure nelle comunità online includono la creazione di programmi di ambasciatori del brand e forum di supporto, la scoperta dei clienti più entusiasti e la loro promozione, la motivazione dei clienti, ecc. (Bernoff e Li, 2008).
Uno sviluppo recente correlato in cui i siti di social network e le comunità online possono cambiare drasticamente il panorama del business fa parte di quella che viene definita la "rivoluzione dei contributi", in cui le aziende creano siti di contribuzione per le parti interessate ad un particolare business; questi spesso fungono da difensori del business (Cook, 2008). Questi siti sono oggi sfruttati dalle aziende leader per ottenere vantaggi in termini di costi e persino vantaggi strategici rispetto ai concorrenti, poiché i volontari hanno letteralmente contribuito personalmente alle imprese (Cook, 2008). Le ragioni per cui questi siti sono stati utilizzati sono l’acquisizione di materie prime in maniera gratuita, la creazione di forum di assistenza clienti attraverso la partecipazione dei membri della comunità online o sviluppare azioni ed iniziative di marketing direttamente da volontari sui social network.
Ciò che è condiviso tra gli aspetti sociali delle comunità online e le comunità online più orientate al business è la desiderabilità di una self-disclosure aperta, che promuova le relazioni sociali e / o accresca le relazioni commerciali con persone che condividono un'affinità per un marchio o un'azienda. Pertanto, un contributo importante che la ricerca può dare alle comunità online è spiegare perché gli utenti della comunità online rivelano o nascondono informazioni. Nei sistemi utilitari, le intenzioni di usare e, soprattutto di continuare ad usare, un sistema sono principalmente basate sull'utilità percepita del software e, in misura minore, sulla facilità d'uso percepita (Davis, 1989); tuttavia, la ricerca ha dimostrato che le ragioni per l'utilizzo e la rivelazione di dati nelle comunità online sono completamente diverse.

Nello specifico, le persone utilizzano i siti di social network per formare e promuovere relazioni e per divulgare e condividere informazioni su sè stessi con gli altri (Chiu, 2006).
La ricerca sul rilascio delle informazioni personali all'interno delle comunità online sta appena iniziando a emergere. Uno studio saliente ha applicato la teoria cognitiva sociale e la teoria del capitale sociale per predire i fattori che incoraggerebbero la condivisione delle conoscenze nelle comunità online (Chiu, 2006). Un altro studio ha rilevato che una maggiore apertura degli individui, dal punto di vista delle informazioni personali aumenta le percezioni positive delle recensioni e l'aumento delle vendite nei mercati elettronici online (Forman, 2008).
A supporto di ciò che stiamo dicendo, vediamo i risultati di un questionario che puntava a studiare il comportamento di apertura degli studenti all'interno degli SNS (Tufekci, 2006).
Lo studio ha rilevato una relazione minima o nulla tra preoccupazioni sulla privacy online e divulgazione di informazioni.
Un altro risultato interessante è che gli studenti gestiscono le loro preoccupazioni sul pubblico indesiderato regolando la visibilità delle informazioni, ma non regolando i livelli di divulgazione.
Basandosi su un questionario e un esame dei profili Facebook dei partecipanti di un suo esperimento, è stato notato che una dichiarazione generale di preoccupazione dell'utente non è un indicatore valido del comportamento della privacy all'interno della rete. Tuttavia, è stato successivamente messo in forte dubbio l'adeguatezza dei sondaggi come strumenti per studiare il paradosso della privacy (Hughes-Roberts (2013).
La relazione tra preoccupazioni sulla privacy e relativa apertura dei propri dati è moderata da varie variabili, in particolare, la rilevanza sociale percepita e il numero di altre applicazioni di social web utilizzate hanno un forte effetto moderatore. In uno studio la rilevanza sociale si riferisce principalmente al comportamento divulgativo dei partner di comunicazione che indica che la divulgazione procede in modo proporzionale, cioè "me lo dici e te lo dico".
Un altro esperimento, che ci conferma anche quanto riportato nel paragrafo due ci conferma l'esistenza di una dicotomia tra atteggiamento contro comportamento. Lo studio consisteva nel condurre una serie di interviste approfondite semi-strutturate e un esperimento per valutare l'influenza del beneficio atteso e del rischio atteso sull'intenzione degli utenti di condividere le informazioni personali. Le conclusioni e le evidenze mostrate, sono state che gli utenti condividono attivamente le informazioni personali nonostante le loro preoccupazioni, in quanto non considerano solo il rischio, ma anche il beneficio atteso della condivisione (Lee, 2013)
Sono stati poi esaminati a fondo i dati relativi all'ubicazione, che sono una forma di informazioni personali sempre più utilizzate dalle applicazioni mobili. La loro indagine ha anche trovato prove che supportano l'esistenza del paradosso della privacy per i dati di localizzazione (Zafeiropoulou, 2013). Questo studio è molto importante per la nostra ricerca, in quanto le applicazioni che esaminiamo sfruttano come elemento principale quello della geolocalizzazione dei dispositivi mobili.

Un altro flusso di ricerche in questo campo riguarda lo studio della percezione del rischio di privacy in relazione all'uso di tecnologie che migliorano la privacy (Oomen e Leenes, 2008).

I dati di questa indagine indicano che un'elevata percezione del rischio di privacy è una motivazione non sufficiente per le persone ad adottare strategie di protezione della privacy, pur sapendo che esistono.

Nel campo dei social network online diversi studi mettono in discussione l'assunto comune secondo il quale i giovani non proteggono le loro informazioni private. I giovani usano una varietà di strategie di protezione, come l'uso di pseudonimi e false informazioni (Miltgen e Peyrat-Guillard, 2014), limitando l'accesso ai loro profili e regolando le loro impostazioni sulla privacy (Boyd e Hargittai, 2010), limitando le richieste di amicizia, e eliminazione di tag e foto (Young e Quan-Haase, 2013).

La divulgazione delle informazioni e il controllo delle informazioni nei social network online non sono strettamente correlati, ma al contrario la divulgazione è guidata dalla necessità di popolarità, il che spiega perché i giovani tendono a rivelare informazioni personali.

D'altra parte, bassi livelli di fiducia portano a strategie di controllo, come la negazione delle richieste di amicizia al fine di controllare chi ha accesso ai profili personali (Christofides, 2009).

Gli utenti interessati alla privacy possono utilizzare varie risposte di protezione della privacy.

Esiste infatti una tassonomia delle risposte di protezione della privacy delle informazioni che include le seguenti tipologie: rifiuto (ovvero negarsi di fornire informazioni), travisamento (cioè gli utenti forniscono false informazioni), rimozione di informazioni da database di aziende online, passaparola negativo, lamentarsi direttamente alle società online e lamentarsi indirettamente a organizzazioni di terze parti (Son e Kim, 2008).

Inoltre, gli studi mostrano una correlazione positiva tra preoccupazioni sulla privacy e comportamenti di protezione. Vediamo ad esempio una ricerca condotta tramite un sondaggio telefonico in Svizzera utilizzando un questionario che copriva diversi costrutti relativi alla privacy. (Lutz e Strathoff, 2014). Questo sondaggio ha confermato un'influenza debole ma statisticamente significativa delle preoccupazioni sulla privacy sul comportamento di protezione.

Recenti indagini mostrano che i problemi di privacy innescano risposte protettive, come la disinstallazione di applicazioni mobili. Un sondaggio tra gli utenti di smartphone del Pew Internet Project (Boyles, 2012) ha rivelato che il 54% degli utenti di applicazioni mobili ha deciso di non installare un'applicazione per telefoni cellulari quando hanno scoperto la quantità di informazioni personali che avrebbero dovuto condividere per utilizzarlo e il 30% degli utenti di applicazioni per cellulari ha disinstallato un'applicazione che era già sul proprio telefono cellulare perché ha appreso che stava raccogliendo informazioni personali che non desiderava condividere.

D'altra parte, solo il 19% dei possessori di telefoni cellulari ha disattivato la funzione di localizzazione sul proprio telefono cellulare. Per la nostra ricerca quindi sarà fondamentale capire perché gli utenti hanno comunque scaricato le applicazioni di tracking, pur avendo preoccupazioni relative alla propria privacy.

Vediamo quindi che questo mondo è di fondamentale importanza per il concetto di privacy e negli anni a seguire saranno necessari ulteriori studi per comprenderne il totale funzionamento.

2.6.2 La relazione tra utenti e social network. Il concetto di reciprocità.

Affrontiamo adesso il tema della relazione che come sappiamo esiste tra gli utenti del web ed i social network in cui questi agiscono. Questo aspetto serve ai fini della nostra ricerca per capire come i soggetti si muovono ed agiscono all'interno di questi siti ed applicazioni: tutto questo è utile anche per comprendere quali sono le ragioni che spingono gli utenti ad assumere determinati comportamenti, in modo da poter proporre ipotesi che spiegano al meglio questo contesto.
Come sappiamo infatti, Internet è stato spesso collegato sia agli aumenti che alla diminuzione del capitale sociale. Un esempio chiaro è la comune critica che sostiene che l'uso di Internet riduce il tempo passato faccia a faccia con gli altri, diminuendo di conseguenza il capitale sociale di un individuo (Nie, 2001).
Tuttavia, questa prospettiva ha ricevuto forti critiche, alcuni ricercatori sostengono infatti che le interazioni online possono integrare o sostituire interazioni di persona, mitigando qualsiasi perdita dal tempo trascorso online (Wellman, 2001). Altri studi sulle comunità fisiche, supportati da reti online, hanno concluso che le interazioni mediate dal computer hanno avuto effetti positivi sull'interazione della comunità, sul coinvolgimento e sul capitale sociale (Hampton & Wellman, 2003).
Recentemente, i ricercatori hanno sottolineato l'importanza dei collegamenti basati su Internet per la formazione di legami deboli, che fungono da fondamento del capitale sociale a ponte. Il bridging del capitale sociale potrebbe essere aumentato da tali siti, che supportano i legami sociali, consentendo agli utenti di creare e mantenere reti di relazioni più ampie e diffuse dalle quali potrebbero potenzialmente attingere risorse (Donath e Boyd, 2004). SI ipotizza che questi social network potrebbero aumentare notevolmente i legami deboli che si potrebbero formare e mantenere, perché la tecnologia è adatta a mantenere tali legami in modo economico e facile.
Importante anche per capire al meglio queste relazioni che si sviluppano è quindi il tema della reciprocità, ovvero quella forma di influenza sociale che fornisce il vantaggio chiave per la rivelazione dei dati personali. La reciprocità, chiamata anche effetto diadico, può essere meglio spiegata come comunicazione quid pro quo, sinonimo di mentalità 'mi dici e ti dirò' (Jourard, 1971)
I sentimenti di reciprocità segnalano a un individuo che i suoi partner relazionali sono disposti ad accettare un certo livello di vulnerabilità per continuare la relazione, aumentando così la valutazione dell'individuo sul valore della relazione e sulla necessità di mantenerlo attraverso le rivelazioni future. Questo segnale di relazione è un messaggio molto positivo che promuove il legame sociale e l'intimità che può donare molta soddisfazione agli utenti e favorire molti benefici percepiti (Ko e Kuo, 2009), incluso un maggiore benessere dovuto ad un maggiore legame con il capitale sociale.

Questa reciproca “doppia rivelazione di informazioni” può costituire il nocciolo della costruzione di relazioni intime che sono considerate estremamente gratificanti e che addirittura migliorano il contatto sociale, la soddisfazione e la qualità complessiva della vita.
La reciprocità non è solo un vantaggio, ma aumentando il valore percepito di un'interazione, un soggetto sarà probabilmente più disponibile a rivelare un numero maggiore di informazioni personali per massimizzare il beneficio dell'interazione (Kankanhalli, 2005).
Ad esempio, poiché i destinatari della divulgazione acquisiscono nel tempo le informazioni personali dei loro partner relazionali, i destinatari si sentono in debito di rispondere ai messaggi ricevuti con un livello simile di intimità. Questa comunicazione reciproca consente agli individui di testare con successo strati sempre più profondi di partner per estrarre le informazioni che si trovano nel nucleo centrale (Derlega, 1993) spingendo ulteriormente il cuneo di comunicazione (Altman e Taylor, 1973).
Nella comunicazione, "ci sono prove sostanziali che le persone si impegneranno in un'intima rivelazione di sé, anche con i relativi estranei, se prima divengono i destinatari di tale rivelazione dai loro compagni di conversazione" (Moon, 2000).
Ciò è stato dimostrato nella self-disclosure della comunità online in cui, essenzialmente, attraverso la divulgazione, si crea la norma della divulgazione e la frequenza dell'auto-divulgazione aumenta nel tempo (Dietz-Uhler, 2005), specialmente quando le rivelazioni sono molto personali e comportano un supporto emotivo (Barak e Gluck-Ofri, 2007).

2.7 Conclusioni

Come detto all’inizio di questo capitolo, i temi affrontati sono tanti ed erano tutti quanti necessari per inquadrare in maniera chiara e precisi i precisi in cui si andrà ad inserire la domanda di ricerca di questa tesi. Abbiamo visto che il comportamento degli utenti viene in gran parte viziato da fattori esterni, che però potrebbero essere controllati dalle imprese e dalle organizzazioni per migliorare la propria relazione con i consumatori. Le implicazioni manageriali di questo tema sono infatti molte, e potrebbero essere in grado di portare benefici enormi a chi sarò in grado di giocarsi al meglio le proprie carte in questo campo di gioco. Altro tema importante toccato nella ricerca è il mondo virtuale, che sempre più ha un ruolo primario nella quotidianità di tutti noi.
In questo scenario gli scambi di informazioni, sia Business – to – consumer che Business – to – business, sono miliardi ogni giorno, e riuscire a capire le modalità per incentivarle e per far sentire protetti e sicuri i consumatori è uno dei punti principali su cui le aziende stanno concentrando i loro sforzi. Dopo aver analizzato lo scenario di riferimento andremo, nel prossimo capitolo, nello specifico degli obiettivi della mia tesi, nell’ analisi e nella visione dei risultati, potendo così trarre le nostre conclusioni.

CAPITOLO 3. LA RICERCA ESPLORATIVA: LA RELAZIONE TRA FATTORI DI COMMUNITY, MOTIVI TECNICI E PREOCCUPAZIONI LEGATE ALLA PRIVACY

3.1 INTRODUZIONE

Andremo adesso, nel corso di questo terzo ed ultimo capitolo, a visualizzare la sezione relativa al nostro studio, a cui siamo arrivati grazie ad accurate ricerche, di tipo sia qualitativo che quantitativo, che vedremo nei paragrafi seguenti.

Prima di entrare nello specifico, è utile fare una breve sintesi, con cui vediamo come siamo arrivati fino a questo punto, e per capire cosa ci ha spinto ad indagare proprio questo fenomeno, ovvero la self – disclosure delle informazioni personali degli individui, per questo progetto di tesi magistrale. Quindi, come abbiamo visto, il primo capitolo è stato necessario per inquadrare il tema nel migliore dei modi: nello specifico è stato presentato il concetto di Privacy, vedendo la sua evoluzione, come questa è cambiata nel corso degli anni e l'importanza che questa è andata piano piano ad assumere per gli individui e, soprattutto, per la società moderna, sempre più attenta a temi legati alla privacy. Proseguendo sono stati indagati tutti quei temi legati al concetto di "privacy concern", quindi tutte le preoccupazioni che assalgono i consumatori ogni qualvolta che questi si trovano a prendere decisioni in questa direzioni. Per seguire il filo logico e dare un quadro il più chiaro possibile, abbiamo mostrato nell'ordine: le normative sulla privacy, quindi la loro evoluzione e come i legislatori oggi tentano di proteggere i dati dei consumatori, il paradosso della privacy, e quindi quel fenomeno per cui i consumatori spesso dichiarano determinate cose, in questo caso la preoccupazione verso i propri dati, ma poi in realtà si comportano in maniera decisamente incoerente con quanto dichiarato. Infine in questo capitolo sono stati esplorati tutti gli stakeholder, che hanno interessi legati alla privacy.

Nel secondo capitolo abbiamo invece indagato a fondo tra le ricerche prodotte, principalmente tra le più recenti temporalmente, sul tema della privacy, vedendo le principali teorie economiche, i costi e benefici che spingono consumatori ed aziende a comportarsi in un certo modo e soprattutto i fattori che incentivano la self – disclosure dei dati. Al giorno d'oggi infatti i consumatori si dichiarano sempre più preoccupati per le proprie informazioni personali, e per questo ci pensano spesso due volte a rilasciarli a terze parti. Allo stesso tempo però sappiamo che i soggetti di business sono ogni giorno più interessati alla raccolta dei dati sensibili dei consumatori, tentando con ogni mezzo lecito o meno (Vedi il caso Facebook). Ritengo, per tutti questi motivi, che indagare su questo tema, cercando un gap (che presenteremo successivamente) nelle ricerche prodotte fino a questo momento, e tentare tramite le analisi svolte di dare una risposta efficace a questo gap, che possa avere anche ulteriori sbocchi nella ricerca futura.

Nei prossimi paragrafi vedremo quindi gli obiettivi che questa ricerca si è preposta, le domande di ricerca sorte in seguito all'analisi esplorativa, la metodologia utilizzata, le analisi svolte, sia qualitativa che quantitativa ed infine i risultati ed i limiti di questa ricerca.

3.2 OBIETTIVI DELLA RICERCA

In questo paragrafo verranno definiti in maniera precisa e puntuale gli obiettivi di questa ricerca di tesi. Vedendo le varie ricerche, l'interesse è ricaduto principalmente sul concetto di self-disclosure, ovvero il fenomeno per cui i consumatori rivelano le proprie informazioni alle aziende o ad altri soggetti interessati. Volendo fare un elaborato incentrato su temi legati al business attuale, ritengo che questo sia uno dei più interessanti da indagare, in quanto sempre più sforzi vengono profusi dalle aziende per migliorare le loro dinamiche in questo contesto. La self - disclosure è il racconto di ciò che prima era sconosciuto, in modo tale da diventare conoscenza condivisa: è il processo per far conoscere se stessi agli altri.

Questa conoscenza condivisa potrebbe esistere tra coppie di persone, all'interno di gruppi o tra un individuo e un'organizzazione. Ha una varietà di scopi, in parte dipende dal contesto in cui avviene la divulgazione. Per esempio, all'interno delle coppie, relazioni particolarmente romantiche, serve ad accrescere la comprensione reciproca e crea fiducia rendendo il divulgatore sempre più vulnerabile (emotivamente o meno) all'altra persona. Poiché la self - disclosure viene spesso ricambiata, spesso serve a rafforzare i legami che legano le persone a relazioni romantiche o basate sull'amicizia

Come già abbiamo visto la self - disclosure tra un individuo e un'organizzazione può servire a scopi di autenticazione, ad esempio per stabilire identità, e consentire a un'organizzazione di riconoscerti in futuro al fine di personalizzare le sue offerte. Le organizzazioni potrebbero anche chiedere informazioni personali per scopi di marketing, ad esempio quando si registra per accedere a un sito Web o per entrare a far parte di una comunità online. Naturalmente, le organizzazioni, sotto forma di ricercatori, potrebbero anche chiedere informazioni personali in nome della ricerca accademica.

Le nuove tecnologie, e in particolare Internet, potrebbero cambiare le richieste alle persone di divulgare informazioni personali, nonché le possibili implicazioni di tale divulgazione. Ad esempio, la divulgazione di informazioni personali a un'altra persona online potrebbe non implicare l'aumento della vulnerabilità che di solito segue la self - disclosure di informazioni personali offline (Ben-Ze'ev, 2003). Le organizzazioni potrebbero anche richiedere maggiori informazioni nel nome dell'autenticazione (anche se questo non deve sempre essere un'informazione personale).

Inoltre, la nuova tecnologia modifica la portata delle informazioni personali che possono essere divulgate o raccolte. Ad esempio, lo sviluppo di dispositivi ambientali e onnipresenti, come i gli smartphone, rende probabile che le informazioni sulla propria posizione, i movimenti e le interazioni sociali possano essere raccolte in futuro in modi ancora sconosciuti. Il modo in cui negoziare la divulgazione di tali informazioni è un problema critico, altrettanto importante quanto il modo in cui i sistemi sono progettati per ridurre al minimo le violazioni della privacy fornendo al tempo stesso livelli adeguati di funzionalità.

Come abbiamo visto i campi di applicazione della self – disclosure sono molti, ma l'obiettivo di questa ricerca è concentrarsi su temi legati al business.

Andando finalmente nello specifico abbiamo individuato alcune aree in cui poteva essere interessante sviluppare certi ragionamenti, colmando dei gap attualmente presenti nella ricerca accademica.
Vediamo quali sono queste aree. Per prima cosa abbiamo visto che gran parte delle ricerche che affrontavano temi di privacy attuali, si concentravano sui social network, in particolare sui più famosi, come ad esempio Facebook, Twitter ed Instagram.
Abbiamo cercato di diversificare la presente ricerca cambiando lo scenario di riferimento, e proprio per questo abbiamo individuato nelle applicazioni questo ambiente da analizzare.
Il mercato delle App è infatti oggi uno dei mercati maggiormente in crescita, contando nel solo 2017 175 miliardi di applicazioni scaricate di dispositivi mobili, per un valore totale di circa 85 miliardi di dollari. Il mondo delle applicazioni come però sappiamo è un mondo estremamente variegato, e spazia dai giochi, applicazioni sulla finanza, applicazioni sul turismo, eccetera.
Per differenziare ulteriormente questo elaborato, è stato deciso di restringere ulteriormente il campo, tentando di individuare determinate da App, che fossero fortemente collegate ai concetti di privacy e che quindi potessero avere un certo rilievo per la nostra analisi.
Abbiamo individuato queste caratteristiche che stavamo cercando nelle cosiddette Applicazioni di tracking, che come è noto tracciano tramite appositi sistemi la posizione dei propri utenti. Le Applicazioni di tracking che useremo sono quelle legate al mondo del fitness, che sono di grande moda tra gli sportivi.
Queste Applicazioni permettono di programmare i propri allenamenti e di renderli noti anche ad altri utenti (non solo utenti dell'applicazione, infatti possono essere condivisi i propri allenamenti con la relativa posizione anche sui vari social network). Ci siamo quindi incuriositi per capire cosa spingesse gli utenti di queste applicazioni, ad usarle nonostante la quantità di informazioni personali, come appunto la propria posizione tramite la geo-localizzazione, che dovevano divulgare all'applicazione. Le principali applicazioni che abbiamo individuato sono le seguenti: "Strava", "Runtustic", "Runkeeper", "Endomondo", "Sworkit" e "Map My Run".
L'epoca che stiamo vivendo ci insegna che gli utenti online agiscono in un contesto sociale caratterizzato dalla presenza sempre maggiore della tecnologia, modificando le relazioni stesse tra gli stessi individui. È noto ormai anche il fatto che le persone utilizzano sempre più spesso queste nuove tecnologie con il fine di sentirsi parte di qualcosa, di un gruppo. La condivisione delle informazioni personali rappresenta uno strumento attraverso cui migliorare il proprio io all'interno delle comunità.
La ricerca vediamo che aveva bisogno di essere suddivisa in due fasi, una prima indagine esplorativa in cui indagare sul web i comportamenti degli utenti, alla ricerca di atteggiamenti codificabili, che potessero aiutarci nella nostra ricerca. Una volta conclusa questa fase, si renderà necessario la fase di raccolta e di analisi dei dati.

3.3 METODOLOGIA

3.3.1 RICERCA QUALITATIVA

Come abbiamo visto, dato che la nostra ricerca rappresenta in un certo modo una novità, e che quindi non potevamo appoggiarci su variabili, dati o scale già esistenti nel mondo accademico. Per questo si è reso necessario per prima cosa svolgere un'analisi esplorativa (ricerca qualitativa), che ci porterà a defiinire le dimensioni e le modalità su cui baseremo la nostra raccolta dei dati. Un'analisi esplorativa ha l'obiettivo di fornire una migliore comprensione del problema di ricerca, che nel nostro caso è quello di capire le ragioni per cui gli individui sono disposti a negoziare e fornire le proprie informazioni personali a soggetti terzi. L'analisi esplorativa si rende necessaria quando si hanno basi ridotte dell'argomento da affrontare ed è impossibile formulare ipotesi senza qualche ricerca esplorativa. In definitiva la ricerca esplorativa deve aiutare nella formulazione di un problema ricercabile e di ipotesi testabili.
Come già spiegato, nel nostro per prima cosa abbiamo fatto uno studio dei principali paper di ricerca accademica per individuare l temi della app di tracking che si lega con quelli di privacy. Una volta individuati questi temi, abbiamo deciso di procedere con un'analisi netnografica del web. La Netnografia è un metodo di ricerca di matrice etnografica che permette di entrare nelle esperienze di consumo autentiche degli utenti online al fine di orientare, potenziare e ottimizzare le strategie di business. L'analisi netnografica si dimostra particolarmente funzionale in ambito social media, ambiente in cui diventa possibile monitorare le conversazioni spontanee espresse online e capitalizzare tutti gli insight emersi dallo studio delle stesse conversazioni. La Netnografia si configura come un metodo di ricerca qualitativa precipuo allo studio della cultura di consumo online sia per finalità sociologiche che di marketing. Con l'avvento del Web 2.0, Internet è divenuto il luogo preferito dai consumatori per scambiarsi informazioni su marchi e prodotti esprimendo valutazioni, critiche, modifiche d'uso, possibili miglioramenti e innovazioni per i brand e per i prodotti. In tale contesto, la metodologia di ricerca netnografica riesce ad imporre tecniche di osservazione dirette e non intrusive delle conversazioni, in generale di tutto il passaparola generato online dall'utenza rispetto ad un argomento specifico, ad un brand o ad un prodotto. Obiettivo principale dell'analisi netnografica è quello di definire contorni netti attorno agli ambienti della rete in cui le web tribe si esprimono, al fine di raccogliere basi di dati e insight qualitativi e oggettivi da tradurre in soluzioni utili a potenziare la propria offerta commerciale, applicabili in asset strategici come: Brand Reputation, Product Innovation, Communication Design, Customer Satisfaction, Crowdsourcing, Trend Watching, Cool Hunting e Community Building, Location-based Insights e Social Innovation.
Quindi nel nostro studio, abbiamo usato gli strumenti che ci permettono di effettuare questa analisi sul web, in particolare è stato utilizzato "Social Mention" per indagare sui social network, le keywords più frequenti collegate alle app di tracking ed al concetto di privacy.

Sono stati esplorati anche i forum dove gli utenti si scambiavano opinioni circa le applicazioni in questione. Oltre alle keywords, sempre grazie a "Social Mention" abbiamo indagato i "sentiment", andando quindi a vedere quali erano i feelings degli utenti nei confronti di queste applicazioni.
Una volta completata questa esplorazione sul web, è stato creato un documento di 100 pagine in cui sono stati raccolti i principali commenti, su cui abbiamo costruito la nostra ipotesi di costrutti e le relative sub – scales, che sono elencati con le relative spiegazioni ed esempi di commenti incontrati sul web.

3.3.2 COME GLI INDIVIDUI NEGOZIANO I PROPRI DATI SENSIBILI PER I TEMI LEGATI ALLA COMMUNITY

Dopo che abbiamo inquadrato il tema di interessa di questa tesi, grazie al grande lavoro di analisi esplorativa che abbiamo effettuato, dovevamo individuare dei fattori per i quali gli individui erano disposti a negoziare i propri dati sensibili in cambio di altri benefici. Come abbiamo visto, grazie al lavoro di analisi netnografica, sono stati raccolte 100 pagine di pagine word, con i commenti degli utenti delle applicazioni.
Questi commenti sono stati analizzati uno ad uno: grazie a questo lavoro di osservazione dei sentiment sul web, abbiamo definito delle di interesse che a nostro avviso potevano essere interessanti per il nostro obiettivo. Il primo tema di interesse, ed anche il più importante, è quello che si lega al concetto di community 2.0. Abbiamo visto infatti all'interno dei tantissimi gruppi (sia pubblici che privati) che i temi inerenti alle dinamiche delle community che si creano nell'ambiente online, sono considerati molto importanti per gli utenti di queste applicazioni.
Per capire al meglio le dinamiche delle applicazioni in questione, abbiamo scaricato sui nostri dispositivi le principali, così da avere una visione a 360 gradi delle funzioni che queste hanno: abbiamo constatato che molte di queste permettono di creare ad esempio nuovi percorsi di allenamento, che poi gli individui possono condividerli con gli altri utenti. È proprio questo continuo scambio di informazioni che gli individui apprezzano, in quanto possono aiutarsi e sostenersi a vicenda.
Vediamo anche che gli utenti all'interno dei forum o dei gruppi sui vari social network sono soliti postare e condividere le proprie esperienze, accompagnate da foto. Sono condivisi anche i materiali ed i tempi dei propri allenamenti. Di solito questi post vengono seguiti da commenti degli altri utenti che si congratulano o donano supporto (nei casi ad esempio in cui ad esempio chi ha scritto il post ha avuto un'esperienza negativa) all'autore del post.
Ciò che si evince una volta entrati in questi gruppi è il grande senso di solidarietà che si crea tra i membri di queste community online: si nota proprio il desiderio di condivisione, sia delle proprie esperienze che dei propri dubbi che dei propri problemi. Quei membri che ad esempio vengono da una performance negativa, si rifugiano spesso nel supporto emozionale degli altri utenti.

Un altro aspetto importante da sottolineare è che spesso gli utenti dichiarano di avere scaricato sui propri dispositivi queste applicazioni, pagando sia in termini monetari che in termini di rilascio delle proprie informazioni personali, per il motivo di incontrare altri utenti con cui condividere i propri allenamenti.
È proprio il senso di aggregazione sociale, di supporto morale in situazioni difficili, di cercare persone simili a te e che condividono gli stessi valori, che rendono gli utenti a rilasciare i propri dati sensibili (tra cui ricordiamo la propria posizione): spesso infatti per questi individui rilasciare le proprie informazioni vale ben la pena, se in cambio possono essere parte di queste community online.

3.3.3 Come Gli Individui Negoziano I Propri Dati Sensibili Per I Temi Legati Ai Motivi Tecnici Delle Applicazioni

Dopo aver indagato i temi indagato i temi legati alla community, vediamo qua l'altro tema di interesse che spinge gli individui a negoziare le proprie informazioni sensibili, e che abbiamo individuato grazie al lavoro di analisi netnografica. Un altro aspetto che è emerso dall'analisi esplorativa del web è infatti proprio questo, ovvero il fatto dello scambio di informazioni tecniche che avviene tra gli utenti della community.
Potersi scambiare questi dati, trucchi o semplicemente dei consigli per migliorare la propria esperienza personale di usability dell'applicazione, rende le persone più disponibili a rinunciare più facilmente ai propri dati sensibili, e quindi superare le preoccupazioni legate alla privacy.
Grazie a questo atteggiamento, gli utenti spesso evitano di utilizzare il classico supporto tecnico che viene fornito dalle aziende, spesso ritenuto inefficiente e lacunoso, in particolare quando si parla di applicazioni per i dispositivi mobili. Si parla in questo caso di fattori legati alla knowledge dei utenti: i membri della community infatti per superare problemi legati ai fattori tecnici delle applicazioni, si affidano ad altri utenti, in quanto tra i membri spesso si creano sentimenti di trust, che spingono gli individui a fidarsi maggiormente dei propri simili, piuttosto che invece, ad esempio, ai servizi clienti delle aziende o delle applicazioni.

3.4 Le Domande Di Ricerca

Quindi terminata questa prima fase di esplorazione del web, che possiamo sintetizzare grazie alla tabella 1, adesso prima di partire con l'analisi quantitativa è stato necessario formulare quella che è la nostra vera e propria domanda di ricerca.

MACRO-AREA	COSTRUTTO	DESCRIZIONE
COMMUNITY	• Community identity	• Ci si identifica con quanto esprime la comunità con la quale mi relaziono.
	• Affiliation	• Si partecipa alle attività della comunità per il bisogno sociale di sentirsi parte di un gruppo
	• Technical Support and Tips	• La comunità diviene una fonte di informazioni tecniche e funzionali dell'app (con Tips intendiamo "pillole" che gli utenti condividono spontaneamente e gratuitamente).
	• Motivational Support	• Gli user superano i propri limiti grazie ad un supporto a livello emozionale delgi altri membri
	• Sharing Experience and Feelings	• Condivisione delle emozioni ed esperienze memorabili vissute.
PRIVACY	• Low Privacy level	• Privacy policies non sufficientemente per la giusta tutela dei dati sensibili (si potrebbe splittare in 2 ulteriori costrutti→low privacy/security need)
	• High Privacy level	• Privacy policies troppo stringente per gli user che vedono limitato il potenziale dell'app
	• Exposition to Marketing	• Gli utenti percepiscono la propria esposizione alle dinamiche aziendali
APP FEATURES	• Price issues	• Valutazioni riguardanti il prezzo del servizio
	• Technical Features	• Indicazioni tecniche sull'app

Tab. 1 Fonte: prodotta dall'autore della tesi

Una volta che abbiamo indentificato i costrutti, che poi tramite le nostre analisi diventeranno le nostre variabili indipendenti (Privacy, Community e Technical Motives), è stato opportuno decidere quali sono le dimensioni finali che vogliamo analizzare, quindi capire quali saranno le nostre variabili dipendenti, su cui effettuare le regressioni. Sempre grazie allo studio dei paper ed all'analisi esplorativa del web, che vedremo nello specifico nel corso del prossimo paragrafo, siamo riusciti ad individuare due tipi di "comportamento finale" dei consumatori, estremamente interessanti per i fini del nostro studio.

Queste due dimensioni le abbiamo definite come "Loyalty and Recommendation" e "Partecipation Mode". Con Loyalty e Recommendation intendiamo quegli atteggiamenti per cui gli individui utilizzano un prodotto in maniera prolungata nel tempo, mentre con Recommendation, vogliamo includere tutte quelle dinamiche di passaparola positivo verso altri soggetti. È noto che saper fidelizzare i propri clienti e far sì che questi parlino bene dei tuoi prodotti con i propri conoscenti, è una delle sfide più difficili per le aziende, ma sono anche due tra i benefici che porterebbero ricavi potenziali eccezionali.

L’altra dimensione è quella della partecipazione, che nel nostro caso consideriamo la partecipazione sulle pagine, ufficiali e non, riferite all’applicazione. Abbiamo splittato questo costrutto in due variabili, che sono la partecipazione attiva e la partecipazione passiva: la prima si riferisce a quelle persone che postano messaggi e partecipano a discussioni sulle pagine delle applicazioni, mentre la seconda si riferisce a quelle persone che non scrivono messaggi ma leggono ciò che viene scritto all’interno di pagine.
Le applicazioni, avendo come fine primario quello del business, e considerando che per certi versi sono considerati veri e propri prodotti, sono estremamente interessate a questi temi, e quindi abbiamo deciso di incrociare questi temi con le nostre variabili indipendenti.
Considerando che, come dicevo nelle prime pagine di questo capitolo, questo scenario di ricerca è ancora carente, abbiamo deciso di non formulare ipotesi, ma bensì una domanda di ricerca.
Dopo un accurato studio ed una riflessione è stata prodotta la seguente domanda di ricerca:

Domanda di ricerca: “I motivi tecnici legati alla usability dell’applicazione, ed i temi legati alla community tra gli users dell’applicazione, sono elementi validi con cui gli individui sono disposti a negoziare i propri dati sensibili?”

Come descritto all’inizio di questo paragrafo, saranno utilizzati gli atteggiamenti degli utenti circa la Loyalty e Recommendation, e gli atteggiamenti di Partecipation sulle pagine dell’applicazione, per determinare e soprattutto dare una risposta significativa alla nostra domanda di ricerca.

3.5 Il Questionario

Una volta effettuata la nostra analisi esplorativa che ci ha portato alla produzione della domanda di ricerca che abbiamo esplicitato nel paragrafo precedente, è giunta la fase in cui devono essere raccolti i dati per dare una risposta a questa domanda. La raccolta è avvenuta attraverso un questionario creato su Qualtrics, il cui obiettivo era quello di raccogliere rispondenti e quindi dati utili per verificare le domande di ricerca.

Quindi una volta terminata questa analisi descrittiva andavano individuate le scale, utili per il questionario che vediamo nella tabella 2.

CONSTRUCTS		
TECHNICAL MOTIVES	1. Getting reliable information from the app functionality 2. Getting tips, recommendations and objective information from other users 3. Possibly receiving rewards and incentives (e.g., discounts, cyber money and gadget) 4. Obtaining price information to compare your fees 5. Obtaining technical information	1. Wang e Fesenmaier 2001 (riadattata secondo la nostra ricerca) 2. Goldsmith and Horowitz 2006 Hennig-Thurau et al. 2004 3. Hennig-Thurau et al. 2004 Sung et al. 2010 4. Form our netnography 5. F Wang and Fesenmaier 2004 (riadattata secondo la nostra ricerca)
CORPORATE IDENTIFICATION MOTIVES	1. Finding partners to train togheter 2. Interacting whit people like me (meeting people with similar interests) 3. I enjoy to be part of the online app community 4. Getting answers from the company on the brand page 5. I identify myself with the community's values 6. Express my satisfaction about a good travel service provider 7. Sharing my experiences and photos with others users 8. Sharing my feelings and photos with others users 9. I am a member of group on FB/Twitter relatively to the app	1. From our netnography 2. Hennig-Thurau et al. 2004 Sung et al. 2010 Jhane and Kunz 2012 3. From our netnography 4. Sung et al. 2010 Jhane and Kunz 2012 5. From our netnograpy 6. Hennig-Thurau et al. 2004 Gretzel and Yoo 2008 7. From our netnography 8. From our netnography 9. From our netnography
PRIVACY ISSUES	1. Privacy concerns 2. Collection	1. Mani, Z., Chouk, I. (2017). Drivers of consumers' resistance to smart products. Journal of Marketing Management, 33 (1-2), 76-97 2. Hsu, C. L., Lin, C. C. (2016). An empirical examination of consumer adoption of Internet of Things services: Network

	3. 3. Intrusiveness	externalities and concern for information privacy perspectives. Computers in Human Behavior, 62, 516–527 3. Mani, Z., Chouk, I. (2017). Drivers of consumers' resistance to smart products. Journal of Marketing Management, 33 (1-2), 76-97
PARTECIPATION MODES	1. How often do you visit the app you mentioned before 2. How often do you use the app regurarly (per week)? 3. How often do you visit the app's social network (and blogs) pages (per month)? 4. In general, I am highly motivated to actively participate in this kind of communities 5. I usually contribute my knowledge and stimulate discussions on the community pages 6. I mostly prefer to read what other people write/comment on community pages 7. In general, I love to frequently post messages and responses on this community pages	1. From our netnography 2. From our netnography 3. From our netnography 4. Casaló, Flavián, and Guinaliu 2010a 5. Casaló, Flavián, and Guinaliu 2010 6. Michal Ben-Shaul1 and Arie Reichel1 7. Casaló, Flavián, and Guinaliu 2010
LOYALTY AND RECCOMENDATION INTENTIONS	1. I intend to reuse the app in the future 2. I intend to revisit the community forums of the app 3. I often reccomend to use the app to other people 4. I will recommend the community forums on social network to other people	1. Casaló, Flavián, and Guinaliu 2010 Jhane and Kunz 2012 (riadattata secondo la nostra ricerca) 2. Sung et al. 2010 (riadattata secondo la nostra ricerca) 3. Jhane and Kunz 2012 4. Casaló, Flavián, and Guinaliu 2010 Sung et al. 2010

Tab. 2 – Fonte: Prodotta dall'autore della tesi

La survey che si è formata contava 52 domande al proprio interno, che seguivano il seguente ordine dei temi trattatati: uso dell'applicazione, domande sulle nostre variabili indipendenti, quindi Technical Motives

Community, e le domande legate alla privacy ed infine le nostre variabili dipendenti "Partecipation Mode" e "Loyalty and Recommendation". Ogni domanda all'interno del questionario venivano misurate a da scale Likert da 1 a 7, dove nella maggior parte dei casi 1=Strongly Disagree e 7=Strongly Agree.
Un aspetto importante che va sottolineato per capire la funzionalità del questionario, è che come prima domanda è stato inserito un filtro per dividere coloro che utilizzano applicazioni di tracking da coloro che invece non utilizzano questo tipo di applicazioni. La domanda era così formulata: "Usi App di tracking?". Se la risposta a questa domanda era "SI", i rispondenti proseguivano con la compilazione del questionario, se invece la risposta era "NO" il questionario terminava immediatamente. Questo filtro è stato inserito per raccogliere risposte quanto più veritiere, dato che avere risposte di persone che effettivamente non usano questo genere di applicazioni, poteva creare un bias sui nostri rispondenti.
Il questionario è stato prodotto in due lingue: Italiano ed Inglese. Questo è stato fatto perché, come vedremo successivamente nella parte relativa al campione, i nostri rispondenti sono stati individui sia italiani che non.
Una volta deciso il flusso del questionario, e le domande esatte da inserire e da somministrare ai risponde, il passo successivo da effettuare è stato quello di decidere il nostro campione di riferimento.
Per prima cosa è stata decisa la dimensione del campione che sarebbe dovuta essere di 200/250 individui. Non sono stati messi limiti su variabili demografici, quindi potevano rispondere al questionario soggetti di tutte le età, sesso e posizione geografica. È stato invece fatto un lavoro di ricerca del campione, in modo di essere certi, che coloro a cui venisse inviato avrebbero effettivamente risposto, riducendo così la timing su questo aspetto.
Nello specifico ho richiesto l'accesso sulla piattaforma di Facebook a svariati gruppi e community relative a queste applicazioni, sia a gruppi locali che internazionali. Una volta che venivo accettato all'interno di questi gruppi, veniva pubblicato un post da parte mia in cui chiedevo di rispondere al questionario, specificandone i fini e gli utilizzi. Oltre a questi gruppi presenti su Facebook, ho inserito il link del questionario anche all'interno di alcuni Forum presenti sul web, dove gli utenti producevano discussioni relative a queste applicazioni.
Infine il questionario è stato inviato ad amici e conoscenti che sapevo in maniera certa che utilizzano queste Applicazioni, in quanto postano i risultati dei loro allenamenti sui vari Social Network. A questi soggetti è stato quindi inviato il link del questionario tramite la chat di Facebook/Instagram.
Una volta effettuato l'invio, abbiamo aspettato di ricevere un numero sufficiente di risposte, secondo le nostre aspettative, monitorando nel frattempo Qualtrics quotidianamente Alla fine sono state raggiunte 240 risposte valide che, dopo aver pulito il data set, abbiamo importato su Stata per iniziare la parte di analisi quantitativa che è riportata di seguito.

3.6 Analisi Dei Dati E Verifica Dei Risultati

Nei seguenti paragrafi andiamo a vedere i risultati che la nostra analisi ha prodotto. Per prima cosa è stata verificata la validity di ogni scala non precedentemente validata attraverso analisi fattoriali per ogni item. Oltre alla validity, per ogni scala è stata verificata la reliability. Quando validate e ritenute affidabili il valore medio delle scale è stato utilizzato per calcolare i coefficienti di regressione utili a determinare le relazioni esistenti tra le varie dimensioni.
Nel prossimo paragrafo approfondiremo l'analisi dei risultati di queste analisi statistiche.

3.6.1 Valori Medi ed Analisi Fattoriale

Dopo aver esportato le risposte del questionario, in cui sono stati raggiunti 240 rispondenti, il data set è stato ripulito da quelli che contenevano i cosiddetti missing values, per arrivare ad un totale di 172 risposte valide su cui poter svolgere l'analisi su stata. Di seguito sono riportati i risultati dell'analisi fattoriale che è stata svolta su Stata, con i relativi commenti. La seguente Factor Analysis, si è concentrata sul costrutto che avevamo individuato come "Technical Motives", contenenti i seguenti Item:

Technical support and tips	- Q10 → Getting reliable information from his functionalities - Q11 → Getting tips, recommendations and objective information from other use
Technical features	- Q12 → Obtaining technical information
Price issues	- Q13 → Getting rewards and incentives (e.g., discounts, cybermoney and gadget) - Q14 → Comparing price information in order to understand the fee differences among the various apps before my decision.

Qual è la posizione media del macro-costrutto techinical motives per ogni item?
,

```
. summ Q10 Q11 Q12

    Variable |        Obs        Mean    Std. Dev.       Min        Max
-------------+---------------------------------------------------------
         Q10 |        170    4.964706    1.455022          1          7
         Q11 |        170    5.088235    1.474992          1          7
         Q12 |        170    4.988235    1.418342          1          7

. summ Q13 Q14

    Variable |        Obs        Mean    Std. Dev.       Min        Max
-------------+---------------------------------------------------------
         Q13 |        170    4.611765    1.584646          1          7
         Q14 |        170    4.558824    1.507205          1          7
```

Per prima cosa vediamo il valore medio (In una scala che va da 1 a 7) di ogni item: I valori medi leggermente sono per gli item "Technical Features" e "Technical Support and Tips", mentre valori medi di poco più bassi vengono rilevati per l'item "Price Issues".
Dedotto questo è necessario ora ottenere la matrice di correlazione dei diversi item.

```
. pwcorr Q10 Q11 Q12 Q13 Q14

             |      Q10      Q11      Q12      Q13      Q14
-------------+---------------------------------------------
         Q10 |   1.0000
         Q11 |   0.2110   1.0000
         Q12 |   0.5331   0.3003   1.0000
         Q13 |   0.2532   0.2907   0.2981   1.0000
         Q14 |   0.3409   0.1959   0.3546   0.6860   1.0000
```

Con la seconda tabella vediamo invece la pairwise correlation. La correlazione tra gli item indica una relazione positiva tra tutti gli item perché in ogni caso il p-value è maggiore di 0,05. L'associazione positiva con il valore maggiore è tra "Techincal features" e "Technical support and tips" (Q12-Q10), mentre la più bassa è tra "Price issues e Techical support and tips" (Q14-Q11).

Conduciamo adesso l'analisi fattoriale per validare gli item (fattori) considerati. Dopo aver lanciato i fattori, ruotiamo quelli caricati in modo da avere uno schema chiaro.
È necessario condurre la factor analysis in quanto alcune delle scale sono scale non validate, perciò si rende necessario creare nuovi costrutti validati per poter procedere ai prossimi step dell'analisi.

```
.
. * Technical motives
. factor Q10 Q11 Q12 Q13 Q14 , pcf
(obs=170)

Factor analysis/correlation                      Number of obs    =        170
    Method: principal-component factors          Retained factors =          1
    Rotation: (unrotated)                        Number of params =          5

    ------------------------------------------------------------------------------
        Factor  |   Eigenvalue   Difference        Proportion   Cumulative
    ------------+-----------------------------------------------------------------
        Factor1 |      2.41396      1.42093            0.4828       0.4828
        Factor2 |      0.99303      0.15384            0.1986       0.6814
        Factor3 |      0.83919      0.38185            0.1678       0.8492
        Factor4 |      0.45735      0.16088            0.0915       0.9407
        Factor5 |      0.29647            .            0.0593       1.0000
    ------------------------------------------------------------------------------
    LR test: independent vs. saturated:  chi2(10) =  217.61 Prob>chi2 = 0.0000

Factor loadings (pattern matrix) and unique variances

    -------------------------------------
        Variable |  Factor1 |   Uniqueness
    -------------+----------+--------------
             Q10 |   0.6714 |      0.5493
             Q11 |   0.5163 |      0.7334
             Q12 |   0.7180 |      0.4845
             Q13 |   0.7564 |      0.4279
             Q14 |   0.7804 |      0.3909
    -------------------------------------

. screeplot , yline(1)

. graph export ScreePlot_TechM.png , replace
(file ScreePlot_TechM.png written in PNG format)

. rotate

Factor analysis/correlation                      Number of obs    =        170
    Method: principal-component factors          Retained factors =          1
    Rotation: orthogonal varimax (Kaiser off)    Number of params =          5

    ------------------------------------------------------------------------------
        Factor  |     Variance   Difference        Proportion   Cumulative
    ------------+-----------------------------------------------------------------
        Factor1 |      2.41396            .            0.4828       0.4828
    ------------------------------------------------------------------------------
    LR test: independent vs. saturated:  chi2(10) =  217.61 Prob>chi2 = 0.0000

Rotated factor loadings (pattern matrix) and unique variances

    -------------------------------------
        Variable |  Factor1 |   Uniqueness
    -------------+----------+--------------
             Q10 |   0.6714 |      0.5493
             Q11 |   0.5163 |      0.7334
             Q12 |   0.7180 |      0.4845
             Q13 |   0.7564 |      0.4279
             Q14 |   0.7804 |      0.3909
    -------------------------------------
```

Come sappiamo, la somma degli eigenvalue risulta uguale al numero totale delle variabili, la cui proporzione indica il peso relativo di ognuno di questi fattori nella varianza totale. Nel nostro caso specifico il Fattore 1 (2,41) spiega il 48% della varianza totale. Se facciamo la cumulativa con il Fattore 2, vediamo che viene grazie a questi due fattori viene spiegato il 68% della varianza totale. In questo caso l'unico fattore che viene mantenuto per le seguenti analisi è il Fattore 1 in quanto il valore dell' eigenvalue è maggiore ad 1.
La Sub-dimension del macro-costrutto è quindi solo una e, attraverso il calcolo di coefficienti di regressione, andiamo a individuare le nuove variabili che la definiscono.

```
. predict Factor1
(regression scoring assumed)

Scoring coefficients (method = regression; based on varimax rotated factors)
```

Variable	Factor1
Q10	0.27812
Q11	0.21389
Q12	0.29742
Q13	0.31333
Q14	0.32330

```
. rename Factor1 TechnicalMotives
```

In ragione dei coefficienti individuati, le variabili Q10, Q11, Q12, Q13, Q14 definiscono il Factor1 e possono essere aggregate in modo da individuare la nuova sub-dimension chiamata "All Technical features".
Di seguito verrà analizzato il costrutto " Community" tramite la Factor Analysis.
Le sub - dimension che sono state utilizzate nel questionario, è che appartenevano a questo costrutto sono: "Affiliation", "Community Identitity", "Sharing Experience and Feelings" e "Motivational support.
Per prima cosa, grazie alla tabella sottostante, andiamo ad analizzare il valore medio di ogni dimensione del costrutto. Grazie a ciò possiamo vedere quali dimensioni hanno ricevuto valori più alti alle risposte del questionario

```
. summ Q23 Q24 Q25 Q26

    Variable |        Obs        Mean    Std. Dev.       Min        Max
-------------+---------------------------------------------------------
         Q23 |        172    5.226744    1.679176         1          7
         Q24 |        172    5.203488    1.600215         1          7
         Q25 |        172     5.02907    1.791557         1          7
         Q26 |        172    4.790698    1.710759         1          7

. summ Q27 Q28

    Variable |        Obs        Mean    Std. Dev.       Min        Max
-------------+---------------------------------------------------------
         Q27 |        172    4.901163    1.698503         1          7
         Q28 |        172    4.802326    1.584425         1          7

. summ Q29 Q30 Q31

    Variable |        Obs        Mean    Std. Dev.       Min        Max
-------------+---------------------------------------------------------
         Q29 |        172    4.930233    1.715364         1          7
         Q30 |        172    4.831395    1.790342         1          7
         Q31 |        172    4.936047    1.710471         1          7

. summ Q32 Q33

    Variable |        Obs        Mean    Std. Dev.       Min        Max
-------------+---------------------------------------------------------
         Q32 |        172    5.052326    1.771326         1          7
         Q33 |        172    4.552326    2.038416         1          7
```

Questa tabella indica la media di ogni item sul costrutto, considerano che è stata utilizzata una scala da 1 a 7, dove 1=Strongly Disagree e 7= Strongly Disagree.

Possiamo vedere che tutti quesiti hanno riscontrato valori mediamente elevati, che vanno da un minimo di 4.55 ad un massimo di 5.22.

I valori più alti vengono mediamente per la dimensione “Affiliation” (Q23=5.22; Q24=5,20; Q25=5,02)

```
.
. * (a) affiliation
. alpha Q23 Q24 Q25 Q26

Test scale = mean(unstandardized items)

Average interitem covariance:     1.999462
Number of items in the scale:            4
Scale reliability coefficient:      0.9009

. * (b) community identity
. alpha Q27 Q28

Test scale = mean(unstandardized items)

Average interitem covariance:     1.208418
Number of items in the scale:            2
Scale reliability coefficient:      0.6187

. * (c) sharing experience
. alpha Q29 Q30 Q31

Test scale = mean(unstandardized items)

Average interitem covariance:      2.11765
Number of items in the scale:            3
Scale reliability coefficient:      0.8751

. * (d) motivational support
. alpha Q32 Q33

Test scale = mean(unstandardized items)

Average interitem covariance:     .6960764
Number of items in the scale:            2
Scale reliability coefficient:      0.3206

. * all community motives
. alpha Q23 Q24 Q25 Q26 Q27 Q28 Q29 Q30 Q31 Q32 Q33

Test scale = mean(unstandardized items)

Average interitem covariance:     1.622975
Number of items in the scale:           11
Scale reliability coefficient:      0.9272

. pwcorr Q23 Q24 Q25 Q26 Q27 Q28 Q29 Q30 Q31 Q32 Q33
```

	Q23	Q24	Q25	Q26	Q27	Q28	Q29
Q23	1.0000						
Q24	0.6879	1.0000					
Q25	0.6373	0.7323	1.0000				
Q26	0.6395	0.6992	0.7767	1.0000			
Q27	0.6517	0.6680	0.7216	0.8160	1.0000		
Q28	0.3972	0.4011	0.3234	0.4917	0.4490	1.0000	
Q29	0.6329	0.6486	0.5715	0.6048	0.5757	0.4898	1.0000
Q30	0.6158	0.7101	0.6214	0.6376	0.6099	0.4623	0.8397
Q31	0.5589	0.6436	0.6952	0.7029	0.7607	0.4053	0.6183
Q32	0.5937	0.6667	0.6187	0.6675	0.6315	0.3996	0.6960
Q33	0.1631	0.1823	0.1989	0.2312	0.3706	0.3617	0.1984

	Q30	Q31	Q32	Q33
Q30	1.0000			
Q31	0.6400	1.0000		
Q32	0.7035	0.6709	1.0000	
Q33	0.2115	0.2282	0.1928	1.0000

Dopo i valori medi andiamo a vedere adesso la reliability.

Si comprende facilmente che per tutti i valori superiori a 0,6 gli Item sono da considerare reliable. Nel nostro caso abbiamo: Affiliation=0,90, Community Identity=0,62, Sharing Experience and Feelings=0,88. L’unico Item non reliable è Motivational Support= 0,32.

Vediamo adesso la Pairwise correlation. In questo caso vediamo che tra tutti gli item esiste una relazione lineare positiva, e nessuna negativa, in quanto non sono presenti valori negativi.
Conduciamo adesso l'analisi fattoriale per validare gli item (fattori) considerati. Dopo aver lanciato i fattori, ruotiamo quelli caricati in modo da avere uno schema chiaro.

```
. factor Q23 Q24 Q25 Q26 Q27 Q28 Q29 Q30 Q31 Q32 Q33, pcf
(obs=172)

Factor analysis/correlation                      Number of obs    =        172
    Method: principal-component factors          Retained factors =          2
    Rotation: (unrotated)                        Number of params =         21
```

Factor	Eigenvalue	Difference	Proportion	Cumulative
Factor1	6.71062	5.63387	0.6101	0.6101
Factor2	1.07675	0.31159	0.0979	0.7079
Factor3	0.76516	0.21301	0.0696	0.7775
Factor4	0.55214	0.07961	0.0502	0.8277
Factor5	0.47253	0.13642	0.0430	0.8707
Factor6	0.33611	0.02244	0.0306	0.9012
Factor7	0.31368	0.04401	0.0285	0.9297
Factor8	0.26966	0.04663	0.0245	0.9542
Factor9	0.22303	0.07561	0.0203	0.9745
Factor10	0.14742	0.01452	0.0134	0.9879
Factor11	0.13290	.	0.0121	1.0000

```
LR test: independent vs. saturated:  chi2(55) = 1445.03 Prob>chi2 = 0.0000
```

Rotated factor loadings (pattern matrix) and unique variances

Variable	Factor1	Factor2	Uniqueness
Q23	0.7936	0.1016	0.3599
Q24	0.8566	0.0967	0.2568
Q25	0.8408	0.0951	0.2840
Q26	0.8374	0.2362	0.2429
Q27	0.7888	0.3565	0.2506
Q28	0.4077	0.6420	0.4216
Q29	0.8028	0.1803	0.3229
Q30	0.8302	0.1697	0.2820
Q31	0.8060	0.2002	0.3103
Q32	0.8185	0.1301	0.3131
Q33	0.0602	0.9099	0.1684

Factor rotation matrix

	Factor1	Factor2
Factor1	0.9552	0.2959
Factor2	-0.2959	0.9552

Come sappiamo dalla teoria, la somma degli "Eigenvalue" è quel valore uguale al numero totale delle variabili, la cui proporzione indica il peso relativo di ognuno di questi fattori nella varianza totale. Nel nostro caso specifico il Fattore 1=6,71 ed il Fattore 2= 1,07, se sommati insieme spiegano il 70,8%della varianza totale. Per questa ragione i fattori 1 e 2 sono gli unici mantenuti in quanto hanno eigenvalue > 1.
Il macro-costrutto, quindi, è definito da 2 sub-dimension che andiamo a definire attraverso il calcolo di coefficienti di regressione.

```
. predict CommunityValues
(regression scoring assumed)

Scoring coefficients (method = regression; based on varimax rotated factors)
```

Variable	Factor1	Factor2
Q23	0.15005	-0.08746
Q24	0.16482	-0.10557
Q25	0.16173	-0.10344
Q26	0.12991	0.01868
Q27	0.09284	0.13289
Q28	-0.05292	0.46258
Q29	0.13470	-0.02177
Q30	0.14300	-0.03696
Q31	0.13102	-0.00538
Q32	0.14919	-0.06847
Q33	-0.18747	0.76968

Tramite la funzione "Predict", sono stati creati i due nuovi fattori, per cui il fattore 1 è definito dalle variabili Q23, Q24, Q25 e Q26, capaci così di individuare il nuovo fattore che prende il nome di "Affiliation Need", ed il fattore 2 viene invece definito dalle variabili Q26, Q27 e Q28, che vanno a definire il nuovo fatto che è stato denominato "Community Identity"
Di seguito sarà analizzato il costrutto Loyalty and Recommendations.

```
. summ Q50 Q51 Q52 Q53

    Variable |        Obs        Mean    Std. Dev.       Min        Max
-------------+---------------------------------------------------------
         Q50 |        172    5.505814    1.290981         1          7
         Q51 |        172    5.273256    1.560021         1          7
         Q52 |        172     5.27907    1.440039         1          7
         Q53 |        172    5.244186    1.799519         1          7
```

Vediamo che i valori medi di queste variabili sono mediamente alti, in una scala da 1 a 7 in cui 1=Strongly Disagree e 7=Strongly Agree.
Nello specifico abbiamo Q50=5,50; Q51=5,27; Q52=5,27; Q53=5,24.

```
. * loyalty & recommendation
. alpha Q50 Q51 Q52 Q53

Test scale = mean(unstandardized items)

Average interitem covariance:      1.24307
Number of items in the scale:            4
Scale reliability coefficient:      0.8175
```

```
. pwcorr Q50 Q51 Q52 Q53, sig
```

	Q50	Q51	Q52	Q53
Q50	1.0000			
Q51	0.4072	1.0000		
	0.0000			
Q52	0.5874	0.4188	1.0000	
	0.0000	0.0000		
Q53	0.4827	0.6094	0.6844	1.0000
	0.0000	0.0000	0.0000	

Dopo i valori medi andiamo a vedere adesso la reliability. Per un valore del coefficiente di reliability di 0,81, possiamo affermare che la dimensione è reliable.

Vediamo adesso la Pairwise correlation. In questo caso vediamo che tra tutti gli item esiste una relazione lineare positiva, e nessuna negativa, in quanto non sono presenti valori negativi.

Conduciamo adesso l'analisi fattoriale per validare i fattori considerati. Dopo aver lanciato i fattori, ruotiamo quelli caricati in modo da avere uno schema chiaro.

```
. factor Q50 Q51 Q52 Q53, pcf
(obs=172)

Factor analysis/correlation                      Number of obs    =        172
    Method: principal-component factors          Retained factors =          1
    Rotation: (unrotated)                        Number of params =          4
```

Factor	Eigenvalue	Difference	Proportion	Cumulative
Factor1	2.60447	1.94399	0.6511	0.6511
Factor2	0.66048	0.17425	0.1651	0.8162
Factor3	0.48623	0.23742	0.1216	0.9378
Factor4	0.24881	.	0.0622	1.0000

```
    LR test: independent vs. saturated:  chi2(6)  =  266.58 Prob>chi2 = 0.0000

Factor loadings (pattern matrix) and unique variances
```

Variable	Factor1	Uniqueness
Q50	0.7602	0.4221
Q51	0.7443	0.4460
Q52	0.8444	0.2871
Q53	0.8716	0.2404

```
Factor rotation matrix
```

	Factor1
Factor1	1.0000

```
. predict positive wom
(regression scoring assumed)
(excess variables dropped)

Scoring coefficients (method = regression; based on varimax rotated factors)
```

Variable	Factor1
Q50	0.29188
Q51	0.28579
Q52	0.32419
Q53	0.33464

Come sappiamo dalla teoria, la somma degli eigenvalue è quel valore uguale al numero totale delle variabili, la cui proporzione indica il peso relativo di ognuno di questi fattori nella varianza totale. Nel nostro caso specifico il Fattore 1=6,51 e quindi spiega il 65% %della varianza totale.

Per questa ragione il fattore 1 è l' unico mantenuto in quanto hanno eigenvalue > 1.

Il macro-costrutto, quindi, è definito da 2 sub-dimension che andiamo a definire attraverso il calcolo di coefficienti di regressione.

Successivamente Tramite la funzione "Predict", è stato creato un nuovo fattoree, che è definito dalle variabili Q52 e Q53 capaci così di individuare il nuovo fattore che prende il nome di "Positive Wom".

Di seguito sarà analizzato la dimensione della “privacy”. Nella fase di esplorazione erano state ipotizzate 3 subscales riferite a questa dimensione: “Privacy Concerns”, “Collection” e . Grazie alle seguenti possiamo individuare quali dimensioni saranno effettivamente utili per la nostra analisi.

```
summ Q34 Q35

    Variable |        Obs        Mean    Std. Dev.       Min        Max
-------------+---------------------------------------------------------
         Q34 |        172    5.017442    1.677069          1          7
         Q35 |        172    5.139535    1.626986          1          7

summ Q36 Q37 Q38 Q39

    Variable |        Obs        Mean    Std. Dev.       Min        Max
-------------+---------------------------------------------------------
         Q36 |        172    4.976744    1.733581          1          7
         Q37 |        171    5.105263    1.662927          1          7
         Q38 |        170         5.1    1.687581          1          7
         Q39 |        170    5.235294     1.61463          1          7

summ Q40 Q41 Q42 Q43 Q44

    Variable |        Obs        Mean    Std. Dev.       Min        Max
-------------+---------------------------------------------------------
         Q40 |        171    4.280702    1.928923          1          7
         Q41 |        171    4.298246    2.017263          1          7
         Q42 |        170    4.288235    2.033559          1          7
         Q43 |        170    3.594118    1.857329          1          7
         Q44 |        171    3.690058    2.030029          1          7
```

Vediamo che i valori medi di queste variabili sono mediamente alti, in una scala da 1 a 7 in cui 1=Strongly Disagree e 7=Strongly Agree. I valori più alti li riscontriamo per la subdimension “Privacy Concern”, che registra valori superiori al 5.

I valori più bassi sono invece per la dimensione “Intrusiveness” (Q40=4,28; Q41=4,29; Q42=4,28; Q43=3,59; Q44=3,69).

```
. * privacy concern
. alpha Q34 Q35

Test scale = mean(unstandardized items)

Average interitem covariance:      1.48878
Number of items in the scale:            2
Scale reliability coefficient:      0.7058

. * collection
. alpha Q36 Q37 Q38 Q39

Test scale = mean(unstandardized items)

Average interitem covariance:     1.862468
Number of items in the scale:            4
Scale reliability coefficient:      0.8875

. * intrusiveness
. alpha Q40 Q41 Q42 Q43 Q44

Test scale = mean(unstandardized items)

Average interitem covariance:     2.689704
Number of items in the scale:            5
Scale reliability coefficient:      0.9175

. * all
. alpha Q34 Q35 Q36 Q37 Q38 Q39 Q40 Q41 Q42 Q43 Q44

Test scale = mean(unstandardized items)

Average interitem covariance:     1.524769
Number of items in the scale:           11
Scale reliability coefficient:      0.9048
```

```
. pwcorr Q35 Q36 Q37 Q38 Q39 Q40 Q41 Q42 Q43 Q44, sig
```

	Q35	Q36	Q37	Q38	Q39	Q40	Q41
Q35	1.0000						
Q36	0.4552	1.0000					
	0.0000						
Q37	0.6130	0.6796	1.0000				
	0.0000	0.0000					
Q38	0.5139	0.6678	0.6973	1.0000			
	0.0000	0.0000	0.0000				
Q39	0.4949	0.6508	0.6203	0.6819	1.0000		
	0.0000	0.0000	0.0000	0.0000			
Q40	0.2792	0.3003	0.3012	0.4049	0.3233	1.0000	
	0.0002	0.0001	0.0001	0.0000	0.0000		
Q41	0.3093	0.3344	0.3884	0.3749	0.2981	0.6586	1.0000
	0.0000	0.0000	0.0000	0.0000	0.0001	0.0000	
Q42	0.3391	0.2986	0.3685	0.3985	0.3270	0.7754	0.6914
	0.0000	0.0001	0.0000	0.0000	0.0000	0.0000	0.0000

	Q42	Q43	Q44
Q42	1.0000		
Q43	0.6468 0.0000	1.0000	
Q44	0.7027 0.0000	0.7249 0.0000	1.0000

Sempre riferendoci al costrutto della privacy, andiamo adesso ad analizzare reliability e pairwise correlation. Vediamo che tutte le subdimension sono reliable in quanto hanno tutte valori superiori allo 0,6. Nello specifico abbiamo: Privacy concern=0,70, Collection=0,88, Intrusiveness =0,91.
Il valore della reliability tra tutti gli Items è di 0,90.
Vediamo adesso la Pairwise correlation. In questo caso vediamo che tra tutti gli item esiste una relazione lineare positiva, e nessuna negativa, in quanto non sono presenti valori negativi.
Di seguito sarà analizzato la dimensione della Partecipation mode. Nella fase di esplorazione erano state ipotizzate 2 subscales riferite a questa dimensione: "Active Contribution" e "Passive Contribution. Grazie alle seguenti possiamo individuare quali dimensioni saranno effettivamente utili per la nostra analisi.

```
. summ Q47 Q48 Q49

    Variable |        Obs        Mean    Std. Dev.       Min        Max
-------------+---------------------------------------------------------
         Q47 |        172    4.616279    1.693942          1          7
         Q48 |        172    4.802326    1.524227          1          7
         Q49 |        172    4.581395    1.910054          1          7
```

Vediamo che i valori medi di queste variabili sono mediamente alti, in una scala da 1 a 7 in cui 1=Strongly Disagree e 7=Strongly Agree. Nello specifico vediamo che Q47=4,61, Q48=4,80 e Q49=4,58.

```
.
. ** Privacy (community)
. * participation modes
. alpha Q47 Q48 Q49

Test scale = mean(unstandardized items)

Average interitem covariance:     1.442676
Number of items in the scale:            3
Scale reliability coefficient:      0.7421
```

```
. pwcorr Q47 Q48 Q49, sig
```

	Q47	Q48	Q49
Q47	1.0000		
Q48	0.4189	1.0000	
	0.0000		
Q49	0.7128	0.3229	1.0000
	0.0000	0.0000	

Sempre riferendoci al costrutto Partecipation Mode, andiamo adesso ad analizzare reliability e pairwise correlation.

Vediamo che tutte le subdimension sono reliable in quanto il coefficiente di reliability è di 0,74.

Vediamo adesso la Pairwise correlation. In questo caso vediamo che tra tutti gli item esiste una relazione lineare positiva, e nessuna negativa, in quanto non sono presenti valori negativi.

3.6.2 Creazione degli Item

In questa seconda ed ultima parte dell'analisi, per prima cosa sono stati creati gli item, in accordo con i risultati che derivanti dalle nostre analisi fattoriali.

```
. alpha  Q36 Q37 Q38 Q39, detail generate(Collection) item

Test scale = mean(unstandardized items)
```

Item	Obs	Sign	item-test correlation	item-rest correlation	average interitem covariance	alpha
Q36	172	+	0.8708	0.7450	1.825711	0.8569
Q37	171	+	0.8644	0.7438	1.869161	0.8549
Q38	170	+	0.8793	0.7772	1.807292	0.8461
Q39	170	+	0.8482	0.7324	1.947648	0.8633
Test scale					1.862468	0.8875

Il cronbach alpha della scala della "Collection", è pari a 0.8875, che è più grande del cutoff 0,60. Guardando alla colonna "alpha", vediamo che eliminando un qualsiasi elemento della scala non cresce di molto. Quindi possiamo affermare che la scala della "Collection" è affidabile e può essere utilizzata per le future analisi calcolando la media del costrutto.

```
. alpha  Q23 Q24 Q25 Q26 Q27 Q29 Q30 Q31 Q32, detail generate(CommunityIdentity) item

Test scale = mean(unstandardized items)
```

Item	Obs	Sign	item-test correlation	item-rest correlation	average interitem covariance	alpha
Q23	172	+	0.7957	0.7399	2.009519	0.9434
Q24	172	+	0.8532	0.8136	1.986778	0.9397
Q25	172	+	0.8456	0.7983	1.940609	0.9404
Q26	172	+	0.8671	0.8279	1.945133	0.9387
Q27	172	+	0.8521	0.8093	1.960375	0.9397
Q29	172	+	0.8210	0.7698	1.980498	0.9418
Q30	172	+	0.8469	0.7999	1.939902	0.9403
Q31	172	+	0.8339	0.7861	1.971524	0.9410
Q32	172	+	0.8297	0.7788	1.959046	0.9414
Test scale					1.965931	0.9470

```
Interitem covariances (obs=172 in all pairs)

       Q23     Q24     Q25     Q26     Q27     Q29     Q30     Q31     Q32
Q23  2.8196
Q24  1.8483  2.5607
Q25  1.9173  2.0993  3.2097
Q26  1.8372  1.9142  2.3804  2.9267
Q27  1.8588  1.8156  2.1959  2.3710  2.8849
Q29  1.8229  1.7804  1.7564  1.7748  1.6773  2.9425
Q30  1.8513  2.0345  1.9932  1.9528  1.8546  2.5788  3.2053
Q31  1.6052  1.7616  2.1305  2.0567  2.2100  1.8142  1.9599  2.9257
Q32  1.7658  1.8899  1.9634  2.0227  1.8999  2.1148  2.2311  2.0326  3.1376
```

Il cronbach alpha della scala della "Community Identity", è pari a 0.9470, che è più grande del cutoff 0,60. Guardando alla colonna "alpha", vediamo che eliminando un qualsiasi elemento della scala non cresce di molto. Quindi possiamo affermare che la scala della "Community Identity" è affidabile e può essere utilizzata per le future analisi calcolando la media del costrutto.

```
. alpha Q34 Q35, detail generate(PrivacyConcerns) item

Test scale = mean(unstandardized items)

Average interitem covariance:      1.48878
Number of items in the scale:            2
Scale reliability coefficient:      0.7058

Interitem covariances (obs=172 in all pairs)

        Q34     Q35
Q34  2.8126
Q35  1.4888  2.6471
```

La reliability (è stata usata la reliability invece che il cronbach alpha in quanto sono presenti solo due elementi a spiegare la variabile) della scala della "Privacy concerns", è pari a 0.7085, che è più grande del cutoff 0,60. Quindi possiamo affermare che la scala della "Privacy concerns" è affidabile e può essere utilizzata per le future analisi calcolando la media del costrutto.

```
. alpha  Q50 Q51 Q52 Q53, detail generate(LoyaltyRecommendation) item

Test scale = mean(unstandardized items)
```

Item	Obs	Sign	item-test correlation	item-rest correlation	average interitem covariance	alpha
Q50	172	+	0.7381	0.5768	1.475022	0.7999
Q51	172	+	0.7674	0.5755	1.328959	0.7999
Q52	172	+	0.8278	0.6908	1.21736	0.7482
Q53	172	+	0.8837	0.7426	.9509384	0.7204
Test scale					1.24307	0.8175

```
Interitem covariances (obs=172 in all pairs)

       Q50      Q51      Q52      Q53
Q50  1.6666
Q51  0.8200   2.4337
Q52  1.0919   0.9408   2.0737
Q53  1.1214   1.7107   1.7736   3.2383
```

Il cronbach alpha della scala della "Loyalty&recommention", è pari a 0.8175, che è più grande del cutoff 0,60. Guardando alla colonna "alpha", vediamo che eliminando un qualsiasi elemento della scala non cresce di molto. Quindi possiamo affermare che la scala della "Loyalty&recommendation" è affidabile e può essere utilizzata per le future analisi calcolando la media del costrutto.

```
. alpha  Q47 Q49, detail generate(ActivePartecipation) item

Test scale = mean(unstandardized items)

Average interitem covariance:      2.30627
Number of items in the scale:            2
Scale reliability coefficient:      0.8288

Interitem covariances (obs=172 in all pairs)

        Q47      Q49
Q47  2.8694
Q49  2.3063   3.6483
```

La reliability (è stata usata la reliability invece che il cronbach alpha in quanto sono presenti solo due elementi a spiegare la variabile) della scala della "Active Partecipation", è pari a 0.8288, che è più grande del cutoff 0,60. Quindi possiamo affermare che la scala della "Active Partecipation" è affidabile e può essere utilizzata per le future analisi calcolando la media del costrutto.

```
. alpha  Q12 Q13 Q14, detail generate(TechnicalMotive) item

Test scale = mean(unstandardized items)
```

Item	Obs	Sign	item-test correlation	item-rest correlation	average interitem covariance	alpha
Q12	170	+	0.6745	0.3547	1.638357	0.8131
Q13	170	+	0.8459	0.6049	.7580926	0.5229
Q14	170	+	0.8614	0.6567	.6699617	0.4571
Test scale					1.022137	0.7116

```
Interitem covariances (obs=170 in all pairs)

        Q12      Q13      Q14
Q12  2.0117
Q13  0.6700   2.5111
Q14  0.7581   1.6384   2.2717
```

Il cronbach alpha della scala della "Technical Motives", è pari a 0.7116, che è più grande del cutoff 0,60. Guardando alla colonna "alpha", vediamo che eliminando due Item la scala crescerebbe. Quindi possiamo affermare che la scala della "Technical Motives" è affidabile e può essere utilizzata per le future analisi calcolando la media del costrutto.

3.6.3 Regressioni

Adesso andiamo ad effettuare il test della regressione, per capire l'impatto che le nostre variabili indipendenti hanno sulle variabili dipendenti. Per prima cosa vediamo le regressioni generali, comprensive di tutte le nostra variabili indipendenti (Technical Motives, Community Identity, Affiliation Need, Collection e Privacy Concerns). In seguito entreremo nel dettaglio, separando le variabili indipendenti legate ai temi della community (Community Identity ed Affiliation Need), dai Technical Motives.

```
. regress PassiveParteciпation AffiliationNeed CommunityIdentity TechnicalMotive PrivacyConcerns Collection
```

Source	SS	df	MS		
Model	106.61638	5	21.3232759	Number of obs	= 170
Residual	289.360091	164	1.7643908	F(5, 164)	= 12.09
				Prob > F	= 0.0000
				R-squared	= 0.2692
				Adj R-squared	= 0.2470
Total	395.976471	169	2.34305604	Root MSE	= 1.3283

PassiveParteciр~n	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
AffiliationNeed	.1348062	.0587239	2.30	0.023	.0188539	.2507585
CommunityIdentity	.3114084	.0763351	4.08	0.000	.1606822	.4621347
TechnicalMotive	.1888581	.1039988	1.82	0.071	-.016491	.3942073
PrivacyConcerns	-.0886368	.1037523	-0.85	0.394	-.2934993	.1162257
Collection	.2050605	.0992876	2.07	0.040	.0090136	.4011073
_cons	1.154805	.5255009	2.20	0.029	.1171851	2.192424

Esaminiamo adesso il significato generale dei coefficienti di regressione e andiamo ad interpretare i risultati.

H0: il coefficiente di regression delle variabili esplicative X1= Affiliation Need, X2=Community Identity, X3= Technical Motives, X4= Privacy Concerns e X5=Collection sono uguali per le variabili indipendenti non hanno effetti sulla variabile dipendente Passive Partecipation.
H1: il coefficiente di regressione delle variabili esplicative esplicative X1= Affiliation Need, X2=Community Identity, X3= Technical Motives, X4= Privacy Concerns e X5=Collection sono uguali per le variabili indipendenti hanno effetti sulla variabile dipendente Passive Partecipation.
Statisticamente:
H0: $\beta1=\beta2=\beta3=\beta4=0$
H1: $\beta i \neq 0$ (almeno una β differisce)
F(5, 164)=12,09, rigettiamo H0. (Prob > F = 0.0000) è minore del livello significativo $\alpha=0.05$, per cui è significante. Quindi rigettiamo H0. Almeno una dei coefficienti di regressione parziali è diverso da 0. Solo le variabili indipendenti "Technical Motives" e "Privacy Concerns" non è significativa in quanto è maggiore di $\alpha=0.05$. Il modello ha quindi un effetto esplicativo sulla DV Passive Partecipation.
Considerando adesso il valore di r-squared vediamo che in questo caso le variabili indipendenti spiegano la varianza della variabile dipendente per il 27%.

```
. regress ActivePartecipation AffiliationNeed CommunityIdentity TechnicalMotive PrivacyConcerns Collection
```

Source	SS	df	MS		
Model	298.58914	5	59.7178281	Number of obs	= 170
Residual	176.859389	164	1.07841091	F(5, 164)	= 55.38
				Prob > F	= 0.0000
				R-squared	= 0.6280
				Adj R-squared	= 0.6167
Total	475.448529	169	2.81330491	Root MSE	= 1.0385

ActivePartecipa~n	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
AffiliationNeed	-.0736151	.0459102	-1.60	0.111	-.1642664	.0170363
CommunityIdentity	.8356692	.0596786	14.00	0.000	.7178317	.9535067
TechnicalMotive	.2909975	.0813061	3.58	0.000	.1304559	.4515392
PrivacyConcerns	.0897708	.0811134	1.11	0.270	-.0703904	.2499319
Collection	-.0601612	.0776229	-0.78	0.439	-.2134303	.0931079
_cons	-.756612	.4108357	-1.84	0.067	-1.567821	.0545973

Esaminiamo adesso il significato generale dei coefficienti di regressione e andiamo ad interpretare i risultati.
H0: il coefficiente di regressione delle variabili esplicative X1= Affiliation Need, X2=Community Identity, X3= Technical Motives, X4= Privacy Concerns e X5=Collection sono uguali per le variabili indipendenti non hanno effetti sulla variabile dipendente Active Partecipation.
H1: il coefficiente di regressione delle variabili esplicative X1= Affiliation Need, X2=Community Identity, X3=Technical Motives, X4= Privacy Concerns e X5=Collection sono uguali per le variabili indipendenti hanno effetti sulla variabile dipendente Active Partecipation.
Statisticamente:

H0: β1=β2=β3= β4=0

H1: βi≠0 (almeno una β differisce)

F(5, 164)=55,38, rigettiamo H0. (Prob > F = 0.0000) è minore del livello significativo α=0.05, per cui è significante. Quindi rigettiamo H0. Almeno una dei coefficienti di regressione parziali è diverso da 0. Solo le variabili indipendenti "Collection" e "Privacy Concerns" non sono significative in quanto è maggiore di α=0.05. Il modello ha quindi un effetto esplicativo sulla DV Active Partecipation.

Considerando adesso il valore di r-squared vediamo che in questo caso le variabili indipendenti spiegano la varianza della variabile dipendente per il 63%.

```
. regress LoyaltyRecommendation AffiliationNeed CommunityIdentity TechnicalMotive PrivacyConcerns Collection
```

Source	SS	df	MS		
Model	145.760365	5	29.152073	Number of obs	= 170
Residual	112.87787	164	.688279696	F(5, 164)	= 42.35
				Prob > F	= 0.0000
Total	258.638235	169	1.53040376	R-squared	= 0.5636
				Adj R-squared	= 0.5503
				Root MSE	= .82963

LoyaltyRecommen~n	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
AffiliationNeed	-.0469523	.0366775	-1.28	0.202	-.1193734	.0254687
CommunityIdentity	.6452709	.047677	13.53	0.000	.5511309	.7394108
TechnicalMotive	-.0073189	.0649551	-0.11	0.910	-.135575	.1209372
PrivacyConcerns	-.059536	.0648012	-0.92	0.360	-.1874882	.0684161
Collection	.1169226	.0620126	1.89	0.061	-.0055235	.2393687
_cons	2.065289	.3282151	6.29	0.000	1.417217	2.713361

Esaminiamo adesso il significato generale dei coefficienti di regressione e andiamo ad interpretare i risultati.

H0: il coefficiente di regressione delle variabili esplicative X1= Affiliation Need, X2=Community Identity, X3= Technical Motives, X4= Privacy Concerns e X5=Collection sono uguali per le variabili indipendenti non hanno effetti sulla variabile dipendente Loyalty e Recommendation.

H1: il coefficiente di regressione delle variabili esplicative X1= Affiliation Need, X2=Community Identity, X3=Technical Motives, X4= Privacy Concerns e X5=Collection sono uguali per le variabili indipendenti hanno effetti sulla variabile dipendente Loyalty e Recommendation.

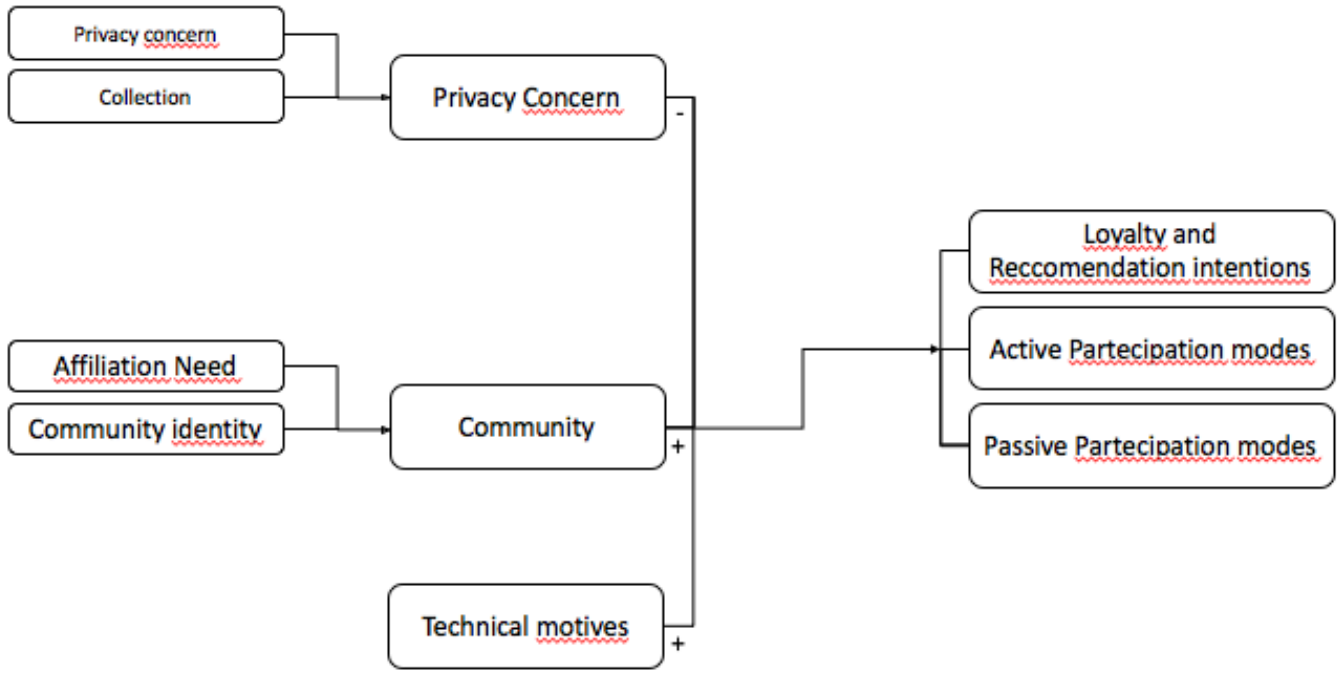
Statisticamente:

H0: β1=β2=β3= β4=0

H1: βi≠0 (almeno una β differisce)

F(5, 164)=42,35, rigettiamo H0. (Prob > F = 0.0000) è minore del livello significativo α=0.05, per cui è significante. Quindi rigettiamo H0. Almeno una dei coefficienti di regressione parziali è diverso da 0. Le variabili indipendenti "Technical Motives" e "Privacy Concerns", "Affiliation Need" e "Collection" non sono significative in quanto sono maggiore di α=0.05. Il modello ha quindi un effetto esplicativo sulla DV Active Partecipation.

Considerando adesso il valore di r-squared vediamo che in questo caso le variabili indipendenti spiegano la varianza della variabile dipendente per il 56%.
Di seguito vediamo il modello riassuntivo, comprensivo delle nostre variabili indipendenti e delle nostre variabili dipendenti.



tab. 3. Fonte: prodotta dall'autore della tesi

Andiamo adesso a leggere cosa queste analisi di regressione ci hanno detto. Per prima cosa possiamo senza dubbio vedere che tutte e 3 le analisi che sono state condotte, mostrano un'influenza positiva delle nostre variabili indipendenti sulle variabili dipendenti che abbiamo ipotizzato, e che ricordiamo essere "Passive Partecipation", "Active Partecipation" e "Loyalty e Recommendation". Questo primo, ma importante risultato, sta a significare che le nostre supposizioni erano corrette e che quindi queste variabili sono utili per gli individui nella negoziazione dei loro dati sensibili.
Andando nello specifico di queste analisi, possiamo vedere che le variabili che maggiormente risentono dell'influenza delle nostre variabili indipendenti, sono "Active Partecipation" e "Loyalty e Recommendation". Rispettivamente, le nostre IV spiegano il 63% della varianza della partecipazione attiva degli utenti ed il 56% dei comportamenti di Loyalty e Recommendation.
Molto più debole è invece l'influenza che le IV hanno sulla variabile dipendente "Passive Partecipation": solo il 27% della varianza di questa variabile è attribuibile ai fattori di Community, Technical Motives e Privacy.
Questi risultati sono estremamente importanti per la nostra analisi, in quanto vediamo che la nostra analisi esplorativa, ha portato effettivamente dei risultati empirici, lasciando un segno nella ricerca di questo, che successivamente dovrà essere maggiormente indagata per poter esprimere tutto il suo potenziale.

Principalmente, quello che queste analisi ci dicono, è che molto spesso le variabili "Community Identity", "Affiliation Need" e "Technical Motives", sono utili per un numero significativo di soggetti, per superare le preoccupazioni che questi hanno circa la loro sfera personali e, nello specifico, sui loro dati sensibili.
La condivisione, anche legata a consigli tecnici, potranno quindi essere armi importanti per le imprese che vorranno investire tempo e risorse in questo ambito.
Tra le IV, vediamo che maggior peso lo ricoprono le variabili legate alla community (Community Identity ed Affiliation Need) rispetto ai Technical Motives,; quindi sempre con riferimento al mondo del business, vediamo che se le aziende riuscissero ad incentivare la formazione di queste community, di cui i consumatori desiderano essere parte, i vantaggi ne deriverebbe non sono da sottovalutare.

3.4 Implicazioni Manageriali

Come abbiamo visto dall'analisi dei dati, le variabili che abbiamo deciso di indagare in questo progetto di tesi sono risultati efficaci, e ci dimostrano che sia le variabili legate al concetto di community, sia quelli legate ai motivi tecnici e sia quelle legate ai concetti di privacy, hanno un impatto importante per le aziende, in quanto grazie ad una buona gestione di questi temi, possono migliorare la fidelizzazione dei clienti, conseguendo inoltre l'importante risultato che questi parlino bene dell'azienda in questione. Inoltre abbiamo anche confutato che queste variabili hanno anche un impatto sui livelli di partecipazione degli utenti sulle pagine e sulla vita in generale di queste applicazioni.
Partendo dal concetto di Loyalty, sappiamo bene come questo possa portare vantaggi tangibili alle aziende. Conseguenza naturale del riuscire a fidelizzare i clienti è il riacquisto, quindi uno degli obiettivi principali delle aziende. Inoltre riuscire a fidelizzare i clienti, aumenta awareness e reputazione del brand tra i consumatori.
Lo stesso passaparola, che noi abbiamo visto come Recommentations, può portare grandi vantaggi alle aziende, facendo sì che un'esperienza positiva di un singolo, spinga altri individui a provare il tuo prodotto, aumentando quindi i ricavi dell'azienda. Da non dimenticare il fatto che in questa ricerca abbiamo appurato che la dimensione della community ha un impatto sia sulla loyalty e sulla recommendation, quindi se consideriamo la community come luogo dove i membri si scambiano opinioni costantemente, capiamo ancora meglio come un passaparola può portare grandissimi benefici alle aziende che riusciranno a sfruttare al meglio questa leva.
Passando invece al concetto di privacy, che è stato il punto focale di tutta questa tesi di laurea, abbiamo visto grazie alla nostra analisi, che una errata gestione di questo aspetto può portare gravi conseguenze alle aziende. Al contrario allocare risorse sula creazione e sullo sviluppo di un buon sistema di Customer Relationship Management, può creare fiducia e sicurezza nei consumatori, che di conseguenza creerà il terreno per interessanti sviluppi manageriali per i soggetti di business.

3.8 Limiti Della Ricerca

Il primo limite di questa ricerca è il fatto che il tema che abbiamo indagato era molto carente di ricerche che includessero le nostre variabili indipendenti, ovvero le community delle Applicazioni ed i motivi tecnici sempre legati a queste applicazioni. Mancando quindi un supporto di fondo siamo stati costretti a creare degli item tramite l'analisi dei dati, che se da una parte è vero che ci hanno validato i nostri costrutti, è anche vero che in alcune regressioni l'impatto sulla variabile (che è positivo in tutte le analisi fatte) è estremamente debole (ad esempio nella domanda di ricerca 5 vediamo che solo il 7% della varianza della variabile dipendente è spiegato dalle variabili indipendenti.
Inoltre anche il mondo delle applicazioni, seppur in grande espansione, è ancora poco studiato sotto questi punti di vista, e per questa ragione, come per il discorso precedente, il flusso di ricerche su cui fare affidamento per il nostro studio è stato abbastanza ristretto.
Un altro limite della ricerca risiede nel fatto che non avendo risorse a disposizione, il campione su cui sono stati fatti i test è abbastanza ristretto. Abbiamo visto infatti che solo 172 partecipanti hanno prodotto risposte valide per il nostro questionario, e quindi per indagare le nostre variabili.

3.9 DISCUSSIONE DEI RISULTATI E CONCLUSIONI

Arrivati alla fine del nostro percorso di tesi, vediamo quali sono state le evidenze che sono venute fuori dai nostri studi, cercando di capire quali possono essere gli sviluppi futuri che vedranno coinvolti questi flussi di ricerche. Il contributo principale che questo elaborato porta, è senza dubbio l'enorme lavoro che è stato fatto, che come abbiamo visto si divide in due fasi principali: la fase dell'analisi qualitativa e la fase dell'analisi quantitativa. L'analisi qualitativa, o esplorativa che dir si voglia, è stata necessaria in quanto data l'importanza del tema, e la mancanza di solide ricerche alle spalle: questo lavoro ha richiesto un grande ammontare di lavoro di ricerca e selezione dei commenti rilevanti.
Come abbiamo visto invece dal fulcro della nostra ricerca, l'analisi dei dati, i risultati ottenuti sono stati importanti, seppur sarà necessario indagare ancora nel futuro, per arrivare ad una visione completa del fenomeno. La metodologia scientifica applicata per legger i dati che abbiamo raccolto grazie alla nostra survey ci ha permesso di dare un senso ai nostri dubbi ed avere a disposizione dei risultati, che andranno poi implementati nel futuro. Le analisi sul coefficiente di regressione hanno dimostrato l'effetto positivo del bilanciamento dei driver sulle variabili dipendenti relative al comportamento degli utenti.
Questi risultati ci dicono infatti che la negoziazione degli individui tra Privacy Concern e i fattori positivi Technical Motive ed i fattori legati al concetto di Community porta spesso a risultati positivi soprattutto per le variabili dipendenti di Loyalty e Recommendation Intention e Active Partecipation. Possiamo dedurre

quindi che i benefits derivanti dalle dimensioni in questione sono importanti per superare le preoccupazioni circa la propria privacy.
In aggiunta i coefficienti di regressione che indagano separatamente i fattori positivi ci hanno dimostrato che le variabili "Affiliation Need" e "Community Identity" sono ritenuti più importanti dei Technical Motives per spiegare il fenomeno indagato.

I driver che abbiamo utilizzato si sono rivelati coerenti per descrivere il comportamento di quegli individui che rilasciano i propri dati personali in fase di acquisto dell'applicazione. Indagando maggiormente sui driver che abbiamo selezionato può portare ai soggetti di business benefici importanti: abbiamo visto che il flusso di ricerche presenti sul tema della self – disclosure è ancora in divenire e probabilmente non ha ancora prodotto il potenziale di quello che per il momento si può solamente intravedere.
Riallacciandoci al tema del paradosso della privacy, le nostre regressioni hanno confermato i nostri sospetti, ovvero che seppur gli individui dichiarano di essere preoccupati per quanto riguarda i propri dati, sono in realtà propensi a negoziare questi stessi dati, in primis con benefici legati all'inclusione che essere parte di una community ti dona, e successivamente anche con le informazioni sulla funzionalità delle applicazioni, che comunque va inquadrato in un'ottica di community dato che questi scambi hanno luogo all'interno di gruppi, forum o blog.
Il cosiddetto marketing relazionale non è sicuramente una novità, infatti è ormai noto che il beneficio legato alla creazione di una community di brand porta grandi vantaggi ai soggetti di business, basti pensare ai casi Ducati o Disney. Quello che però ancora non si sapeva, e che dovrà essere implementato in futuro con altre ricerche degli esperti, era che il senso di appartenenza ad una comunità potrebbe avere effetti positivi come fattore di negoziazione per il rilascio di dati sensibili, allo stesso pari di altri fattori, come ad esempio la personalizzazione e la fiducia che abbiamo visto nel secondo capitolo.
Sarebbe interessante in futuro sviluppare uno studio approfondito di questo fenomeno, magari collegato con altri studi, che permetta di avere una visione più ampia del tema in questione dando dati empirici da utilizzare per migliorare il business.

BIBLIOGRAFIA

1. Acquisti A. John L. (2013) What Is Privacy Worth?. Journal Of Legal Studies: 34 - 41
2. Acquisti A. John L. Loewenstein G. (2012) The Impact of Relative Standards on the Propensity to Disclose. Journal of Marketing Research 49: 160 - 174
3. Andrade, E., Kaltcheva, V., Weitz, B., (2002) Self-disclosure on the web: The impact of privacy policy, reward, and company reputation. Advances in Consumer Research 29: 350 – 353
4. Barth S., De Jong M. (2017) The privacy paradox - Investigating discrepancies between expressed privacy concerns and actual online behavior - A systematic literature review. Telematics and Informatics 34: 1038 – 1058
5. Benamati, J., Zafer, O., Smith, J., (2017) Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. Journal of information science 43: 583 - 600
6. Blank, G., Lutz C., (2018) Benefits and harms from Internet use: A differentiated analysis of Great Britain. New Media & Society 20: 618 – 640
7. Chen D. Fraiberger S. Moakler R. Provost F. (2017) Enhancing Transparency and Control When Drawing Data-Driven Inferences About Individuals. Big data 5: 56 – 87
8. Christofides, E., Muise A. Desmarais S., (2009) Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes? CYBERPSYCHOLOGY & BEHAVIOR 12: 441 - 445
9. Demmers, J., Van Dolen, M., Weltevreden, J., (2018) Handling Consumer Messages on Social Networking Sites: Customer Service or Privacy Infringement? International Journal of Electronic Commerce 22: 8-35
10. Ginosar A. Ariel Y. (2017) An analytical framework for online privacy research: What is missing? Information & Management 54: 948 – 957
11. Gross, G., Acquisti, A., (2005) Information Revelation and Privacy in Online Social Networks (The Facebook case).Workshop on Privacy in the Electronic Society
12. Grossklads, J., Acquisti, A., (2005) Privacy and Rationality in Individual Decision Making. Security & Privacy: 24 – 30
13. Guragai B. Hunt N. Neri M. Taylor E. (2017) "Accounting Information Systems and Ethics Research: Review, Synthesis, and the Future. Journal Of Information Systems 31: 65 – 81
14. Hallam, C., Zanella, G., (2017) Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. Computer in Human Behavior 68: 217 - 227
15. Hsin-Yi, H., (2016) Examining the beneficial effects of individual's self-disclosure on the social network site. Computer in Human Behavior 57: 122 – 132

16. Jordaan, Y., Van Heerden, G., (2017) Online privacy-related predictors of Facebook usage intensity. Computer in Human Behavior 70: 90 – 96
17. Junglas, I., Johnson N., Spitzmu ̈ller, C., (2008) Personality traits and concern for privacy: an empirical study in the context of location-based services. European Journal of Information Systems 17: 387
18. Kokolakis, S., (2017) Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security 64: 122 – 134
19. Krafft, M., Arden, C., Verhoef, P., (2017) Permission Marketing and Privacy Concerns - Why Do Customers (Not) Grant Permissions? Journal of Interactive Marketing 39: 39 - 54
20. Krishnan M. (2006) The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. MIS Quarterly 30: 13 - 28
21. Krishen, A., Raschke, R., Close, A., Kachroo, P., (2017) A power-responsibility equilibrium framework for fairness: Understanding consumers' implicit privacy concerns for location-based services. Journal of business research 73: 20 – 29
22. Li, Y., (2012) Theories in online information privacy research: A critical review and an integrated framework. Decision Support Systems 54: 471 – 481
23. Li, H., Luo, X., Zhang, J., (2017) Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors. Information & Management 54: 1012 - 1022
24. Markos, E., Milne, G., Peltier, J., (2017) Information Sensitivity and Willingness to Provide Continua: A Comparative Privacy Study of the United States and Brazil. Journal of public policy & marketing 36: 79
25. Martin, K., Borah, A., Palmatier, R., (2017) Data Privacy: Effects on Customer and Firm Performance. Journal of Marketing 81: 36 – 58
26. Martin, K., Murphy, P., (2017) The role of data privacy in marketing, Journal of the Academy of Marketing Science 45: 135 – 155
27. Mosteller, J., Poddar, A., (2017) To Share and Protect: Using Regulatory Focus Theory to Examine the Privacy Paradox of Consumers' Social Media Engagement and Online Privacy Protection Behaviors. Journal of Interactive Marketing 39: 27 – 38
28. Nam T., "Does ideology matter for surveillance concerns? (2017) Telematics And Informatics 23: 134 - 156
29. Nam T. (2018) Untangling the relationship between surveillance concerns and acceptability. Journal of Information Management 38: 262 - 269
30. Norberg, P., Horne, D., (2007) The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. The Journal of Consumer Affairs 41: 100 – 126
31. Nottingha, Q., Collignon, S., Warkentin, M., Ziegelmayer, J.,(2015) The interpersonal privacy identity

(IPI): development of a privacy as control model. Information Technology and Managementn17: 341 – 360

32. Pagani, M., Malacarne, G., (2017) Experiential Engagement and Active vs. Passive Behavior in Mobile Location-based Social Networks: The Moderating Role of Privacy. Journal of Interactive Marketing 37: 133 – 148
33. Potoglou D. Dunkerley F. Patil S. Robinson N. (2017) (COMPUTERS IN HUMAN BEHAVIOR, 2017) Public preferences for internet surveillance, data retention and privacy enhancing services: Evidence from a pan-European study. Computers In Human Behavior 75: 811 – 825
34. Prince, C., (2018) Do consumers want to control their personal data? Empirical evidence. International Journal of Human-Computer Studies 110: 21 – 32
35. Schuster S. Van Den Berg M. Larrucea X. Slewe T. Ide-Kostic P. (2017) Mass surveillance and technological policy options: Improving security of private communications. Computer Standards & Interfaces 50: 76 - 82
36. Spottswood, E., Hancock, J., (2017) Should I Share That? Prompting Social Norms That Influence Privacy Behaviors on a Social Networking Site. Journal of Computer-Mediated Communication, 22. 55–70
37. Steinfeld, N., (2017) Track me, track me not: Support and consent to state and private sector surveillance. Telematics and Informatics 34: 1663 – 1672
38. Wottrich, V., Van Reijmersdal, E., Smit, E., (2018) The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. Decision Support Systems 106: 44 – 52
39. Wu H. Zhang H. Cui L. Wang X. (2017) A Heuristic Model for Supporting Users' Decision-Making in Privacy Disclosure for Recommendation. Security and Communication Networks: 1 – 13
40. Zhao, L., (2014) Disclosure Intention of Location-Related Information in Location-Based Social Network Services. International Journal of electronic commerce 16: 53 - 59
41. Zlatolas, L., Welzer, T., Hericˇko, M., Hölbl, M., (2015) "Privacy antecedents for SNS self-disclosure: The case of Facebook. Computer in Human Behavior 45: 158 - 167

RINGRAZIAMENTI

Ai miei genitori, che mi hanno permesso di intraprendere questo percorso, standomi vicino ed incoraggiandomi. Ma soprattutto hanno sempre creduto in me, nonostante tutto.

A Nuria, la mia forza e la mia fonte di ispirazione più grande

Ai miei amici, che anche se probabilmente non ne hanno idea, non immaginano nemmeno l'aiuto che mi hanno dato a superare i momenti più duri. Un giorno con voi vale anni di sacrifici.

Ai miei compagni di università, questo percorso non sarebbe stato così bello senza di voi.

All'Università LUISS che mi ha messo a disposizione tutti i mezzi migliori per migliorarmi. Non avrei potuto fare scelta migliore.

Dipartimento di Impresa e Management Cattedra: Analisi del Comportamento d'acquisto

Data Privacy nel Marketing: Un' Analisi Esplorativa

RELATORE

Prof.Ssa Romani Simona

CANDIDATO
Viligiardi Tommaso

MATR
682611

CORRELATORE

PROF. Donato Carmela

ANNO ACCADEMICO 2017 / 2018

INDICE

CAPITOLO 3. LA RICERCA ESPLORATIVA: LA RELAZIONE TRA FATTORI DI COMMUNITY, MOTIVI TECNICI E PREOCCUPAZIONI LEGATE ALLA PRIVACY

INTRODUZIONE

Uno dei temi più caldi nel marketing attuale è quello della self – disclosure dei dati personali. Soprattutto a seguito del recente scandalo che ha coinvolto Facebook ed il suo creatore, mai come oggi il tema in questione è considerato estremamente attuale.
Sempre più individui si dichiarano preoccupati sulla diffusione e soprattutto sugli usi che le aziende fanno dei loro dati, e naturalmente allo stesso tempo i soggetti di business sono sempre più interessanti alla raccolta di questi dati sensibili. I dati sensibili sono quei dati personali che riguardano la sfera più intima dell'individuo e, pertanto, necessitano di una speciale protezione. Nell'era del digitale la tutela della privacy è divenuto uno degli obiettivi più importanti da raggiungere. Riprese in pubblico, fotografie, abbonamenti a riviste, iscrizioni a piattaforme online: tutto viaggia velocemente nella rete, rendendo di dominio pubblico (o quasi) i dati personali. Per porre un argine alla diffusione esagerata delle informazioni, la legge italiana ha previsto che alcune di esse possano essere trattate solamente con il consenso espresso dell'interessato ovvero con l'autorizzazione preventiva del Garante della privacy. Si tratta dei cosiddetti dati sensibili. Questi sono dei particolari dati personali che, per la loro delicatezza, necessitano di una disciplina particolare. Nello specifico con l'espressione "Dati Sensibili", vediamo che questi si inseriscono all'interno dei dati personali, i dati sensibili sono quelli che rivelano l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale. I dati sensibili sono soggetti, per la loro delicatezza, ad un particolare trattamento giuridico.
Come dicevo questi dati vengono bramati sempre di più dalle aziende, in quanto è comunemente riconosciuto che riuscire a raccoglierli in grandi quantità, porta grandi benefici, in quanto permette di ideare e produrre prodotti e servizi fatti su misura per un certo target di consumatori.
Questi benefici non sono solo per le aziende, in quanto ricevendo offerte fatte su misure, anche i consumatori ricevono determinati vantaggi. Proprio per questa ragione, a prescindere dalle preoccupazioni e dai rischi che il rilascio dei dati personali comporta, i consumatori sono spesso portati a passare oltre, decidendo quindi di fornire a terze parti i propri dati.
L'obiettivo di questa ricerca è quindi quelli di indagare a fondo su questo argomento tentando di individuare quali sono quei fattori (Anche detti fattori facilitatori) che spingono gli individui a svelare i propri dati. Questi fattori saranno indagati tramite un enorme lavoro, volto a capire in primis il contesto di riferimento e tutto ciò che gli ruota intorno, per arrivare al risultato finale di riuscire a formulare una domanda di ricerca che poi andremo ad analizzare ed a verificare o smentire, tramite l'analisi dei dati.
Quindi, dopo un primo capitolo che sarà necessario a dare un'infarinatura generale sul tema, in cui verrà principalmente visto il significato che oggi viene attribuito alla privacy, le normative in vigore ed i soggetti che sono interessati ai suoi sviluppi, nel secondo capitolo affronteremo nello specifico i temi che sono stati

maggiormente toccati negli ultimi anni. Saranno qua enunciate le principali teorie economiche, la dicotomia che esiste tra i gli atteggiamenti dichiarati ed i comportamenti effettivamente messi in atto dai consumatori, ed in particolare vedremo l'analisi costi – benefici che spinge gli individui a prendere determinate decisioni. Infine, sempre nel secondo capitolo vedremo quali sono quei fattori attualmente riconosciuti dagli esperti, come importanti per la maggior parte degli individui, per negoziare i propri dati sensibili. In particolare i fattori che vedremo sono: fiducia, personalizzazione e controllo.
Infine nell'ultimo capitolo sarà presentata la nostra ricerca: di questa verranno presentati tutti gli step, partendo da come ci siamo avvicinati a questo tema, gli obiettivi che avevamo, la metodologia utilizzata, che vedremo essere formata da due fasi, la raccolta e la lettura dei dati ed, infine, la stesura dei risultati che abbiamo ottenuto in questo lungo percorso

OBIETTIVI DELLA RICERCA

In questo paragrafo verranno definiti in maniera precisa e puntuale gli obiettivi di questa ricerca di tesi. Vedendo le varie ricerche, l'interesse è ricaduto principalmente sul concetto di self-disclosure, ovvero il fenomeno per cui i consumatori rivelano le proprie informazioni alle aziende o ad altri soggetti interessati. Volendo fare un elaborato incentrato su temi legati al business attuale, ritengo che questo sia uno dei più interessanti da indagare, in quanto sempre più sforzi vengono profusi dalle aziende per migliorare le loro dinamiche in questo contesto. La self - disclosure è il racconto di ciò che prima era sconosciuto, in modo tale da diventare conoscenza condivisa: è il processo per far conoscere se stessi agli altri.
Questa conoscenza condivisa potrebbe esistere tra coppie di persone, all'interno di gruppi o tra un individuo e un'organizzazione. Ha una varietà di scopi, in parte dipende dal contesto in cui avviene la divulgazione. Per esempio, all'interno delle coppie, relazioni particolarmente romantiche, serve ad accrescere la comprensione reciproca e crea fiducia rendendo il divulgatore sempre più vulnerabile (emotivamente o meno) all'altra persona. Poiché la self - disclosure viene spesso ricambiata, spesso serve a rafforzare i legami che legano le persone a relazioni romantiche o basate sull'amicizia
Come già abbiamo visto la self - disclosure tra un individuo e un'organizzazione può servire a scopi di autenticazione, ad esempio per stabilire identità, e consentire a un'organizzazione di riconoscerti in futuro al fine di personalizzare le sue offerte. Le organizzazioni potrebbero anche chiedere informazioni personali per scopi di marketing, ad esempio quando si registra per accedere a un sito Web o per entrare a far parte di una comunità online. Naturalmente, le organizzazioni, sotto forma di ricercatori, potrebbero anche chiedere informazioni personali in nome della ricerca accademica.
Le nuove tecnologie, e in particolare Internet, potrebbero cambiare le richieste alle persone di divulgare informazioni personali, nonché le possibili implicazioni di tale divulgazione. Ad esempio, la divulgazione di informazioni personali a un'altra persona online potrebbe non implicare l'aumento della vulnerabilità che di solito segue la self - disclosure di informazioni personali offline (Ben-Ze'ev, 2003). Le organizzazioni

potrebbero anche richiedere maggiori informazioni nel nome dell'autenticazione (anche se questo non deve sempre essere un'informazione personale).
Inoltre, la nuova tecnologia modifica la portata delle informazioni personali che possono essere divulgate o raccolte. Ad esempio, lo sviluppo di dispositivi ambientali e onnipresenti, come i gli smartphone, rende probabile che le informazioni sulla propria posizione, i movimenti e le interazioni sociali possano essere raccolte in futuro in modi ancora sconosciuti. Il modo in cui negoziare la divulgazione di tali informazioni è un problema critico, altrettanto importante quanto il modo in cui i sistemi sono progettati per ridurre al minimo le violazioni della privacy fornendo al tempo stesso livelli adeguati di funzionalità.
Come abbiamo visto i campi di applicazione della self – disclosure sono molti, ma l'obiettivo di questa ricerca è concentrarsi su temi legati al business.
Andando finalmente nello specifico abbiamo individuato alcune aree in cui poteva essere interessante sviluppare certi ragionamenti, colmando dei gap attualmente presenti nella ricerca accademica.
Vediamo quali sono queste aree. Per prima cosa abbiamo visto che gran parte delle ricerche che affrontavano temi di privacy attuali, si concentravano sui social network, in particolare sui più famosi, come ad esempio Facebook, Twitter ed Instagram.
Abbiamo cercato di diversificare la presente ricerca cambiando lo scenario di riferimento, e proprio per questo abbiamo individuato nelle applicazioni questo ambiente da analizzare.
Il mercato delle App è infatti oggi uno dei mercati maggiormente in crescita, contando nel solo 2017 175 miliardi di applicazioni scaricate di dispositivi mobili, per un valore totale di circa 85 miliardi di dollari. Il mondo delle applicazioni come però sappiamo è un mondo estremamente variegato, e spazia dai giochi, applicazioni sulla finanza, applicazioni sul turismo, eccetera.
Per differenziare ulteriormente questo elaborato, è stato deciso di restringere ulteriormente il campo, tentando di individuare determinate da App, che fossero fortemente collegate ai concetti di privacy e che quindi potessero avere un certo rilievo per la nostra analisi.
Abbiamo individuato queste caratteristiche che stavamo cercando nelle cosiddette Applicazioni di tracking, che come è noto tracciano tramite appositi sistemi la posizione dei propri utenti. Le Applicazioni di tracking che useremo sono quelle legate al mondo del fitness, che sono di grande moda tra gli sportivi.
Queste Applicazioni permettono di programmare i propri allenamenti e di renderli noti anche ad altri utenti (non solo utenti dell'applicazione, infatti possono essere condivisi i propri allenamenti con la relativa posizione anche sui vari social network). Ci siamo quindi incuriositi per capire cosa spingesse gli utenti di queste applicazioni, ad usarle nonostante la quantità di informazioni personali, come appunto la propria posizione tramite la geo-localizzazione, che dovevano divulgare all'applicazione. Le principali applicazioni che abbiamo individuato sono le seguenti: "Strava", "Runtustic", "Runkeeper", "Endomondo", "Sworkit" e "Map My Run".
L'epoca che stiamo vivendo ci insegna che gli utenti online agiscono in un contesto sociale caratterizzato dalla presenza sempre maggiore della tecnologia, modificando le relazioni stesse tra gli stessi individui. È noto ormai anche il fatto che le persone utilizzano sempre più spesso queste nuove tecnologie con il fine di

sentirsi parte di qualcosa, di un gruppo. La condivisione delle informazioni personali rappresenta uno strumento attraverso cui migliorare il proprio io all'interno delle comunità.
La ricerca vediamo che aveva bisogno di essere suddivisa in due fasi, una prima indagine esplorativa in cui indagare sul web i comportamenti degli utenti, alla ricerca di atteggiamenti codificabili, che potessero aiutarci nella nostra ricerca. Una volta conclusa questa fase, si renderà necessario la fase di raccolta e di analisi dei dati.

METODOLOGIA

RICERCA QUALITATIVA

Come abbiamo visto, dato che la nostra ricerca rappresenta in un certo modo una novità, e che quindi non potevamo appoggiarci su variabili, dati o scale già esistenti nel mondo accademico. Per questo si è reso necessario per prima cosa svolgere un'analisi esplorativa (ricerca qualitativa), che ci porterà a defiinire le dimensioni e le modalità su cui baseremo la nostra raccolta dei dati. Un'analisi esplorativa ha l'obiettivo di fornire una migliore comprensione del problema di ricerca, che nel nostro caso è quello di capire le ragioni per cui gli individui sono disposti a negoziare e fornire le proprie informazioni personali a soggetti terzi.
L'analisi esplorativa si rende necessaria quando si hanno basi ridotte dell'argomento da affrontare ed è` impossibile formulare ipotesi senza qualche ricerca esplorativa. In definitiva la ricerca esplorativa deve aiutare nella formulazione di un problema ricercabile e di ipotesi testabili.
Come già spiegato, nel nostro per prima cosa abbiamo fatto uno studio dei principali paper di ricerca accademica per individuare l temi della app di tracking che si lega con quelli di privacy. Una volta individuati questi temi, abbiamo deciso di procedere con un'analisi netnografica del web. La Netnografia è un metodo di ricerca di matrice etnografica che permette di entrare nelle esperienze di consumo autentiche degli utenti online al fine di orientare, potenziare e ottimizzare le strategie di business. L'analisi netnografica si dimostra particolarmente funzionale in ambito social media, ambiente in cui diventa possibile monitorare le conversazioni spontanee espresse online e capitalizzare tutti gli insight emersi dallo studio delle stesse conversazioni. La Netnografia si configura come un metodo di ricerca qualitativa precipuo allo studio della cultura di consumo online sia per finalità sociologiche che di marketing. Con l'avvento del Web 2.0, Internet è divenuto il luogo preferito dai consumatori per scambiarsi informazioni su marchi e prodotti esprimendo valutazioni, critiche, modifiche d'uso, possibili miglioramenti e innovazioni per i brand e per i prodotti. In tale contesto, la metodologia di ricerca netnografica riesce ad imporre tecniche di osservazione dirette e non intrusive delle conversazioni, in generale di tutto il passaparola generato online dall'utenza rispetto ad un argomento specifico, ad un brand o ad un prodotto. Obiettivo principale dell'analisi netnografica è quello di definire contorni netti attorno agli ambienti della rete in cui le web tribe si esprimono, al fine di raccogliere basi di dati e insight qualitativi e oggettivi da tradurre in soluzioni utili a potenziare la propria offerta commerciale, applicabili in asset strategici come: Brand Reputation, Product Innovation, Communication

Design, Customer Satisfaction, Crowdsourcing, Trend Watching, Cool Hunting e Community Building, Location-based Insights e Social Innovation.
Quindi nel nostro studio, abbiamo usato gli strumenti che ci permettono di effettuare questa analisi sul web, in particolare è stato utilizzato "Social Mention" per indagare sui social network, le keywords più frequenti collegate alle app di tracking ed al concetto di privacy.
Sono stati esplorati anche i forum dove gli utenti si scambiavano opinioni circa le applicazioni in questione.
Oltre alle keywords, sempre grazie a "Social Mention" abbiamo indagato i "sentiment", andando quindi a vedere quali erano i feelings degli utenti nei confronti di queste applicazioni.
Una volta completata questa esplorazione sul web, è stato creato un documento di 100 pagine in cui sono stati raccolti i principali commenti, su cui abbiamo costruito la nostra ipotesi di costrutti e le relative sub – scales, che sono elencati con le relative spiegazioni ed esempi di commenti incontrati sul web.

RISULTATI

Andiamo adesso a leggere cosa queste analisi di regressione ci hanno detto. Per prima cosa possiamo senza dubbio vedere che tutte e 3 le analisi che sono state condotte, mostrano un'influenza positiva delle nostre variabili indipendenti sulle variabili dipendenti che abbiamo ipotizzato, e che ricordiamo essere "Passive Partecipation", "Active Partecipation" e "Loyalty e Recommendation". Questo primo, ma importante risultato, sta a significare che le nostre supposizioni erano corrette e che quindi queste variabili sono utili per gli individui nella negoziazione dei loro dati sensibili.
Andando nello specifico di queste analisi, possiamo vedere che le variabili che maggiormente risentono dell'influenza delle nostre variabili indipendenti, sono "Active Partecipation" e "Loyalty e Recommendation". Rispettivamente, le nostre IV spiegano il 63% della varianza della partecipazione attiva degli utenti ed il 56% dei comportamenti di Loyalty e Recommendation.
Molto più debole è invece l'influenza che le IV hanno sulla variabile dipendente "Passive Partecipation": solo il 27% della varianza di questa variabile è attribuibile ai fattori di Community, Technical Motives e Privacy.
Questi risultati sono estremamente importanti per la nostra analisi, in quanto vediamo che la nostra analisi esplorativa, ha portato effettivamente dei risultati empirici, lasciando un segno nella ricerca di questo, che successivamente dovrà essere maggiormente indagata per poter esprimere tutto il suo potenziale.
Principalmente, quello che queste analisi ci dicono, è che molto spesso le variabili "Community Identity", "Affiliation Need" e "Technical Motives", sono utili per un numero significativo di soggetti, per superare le preoccupazioni che questi hanno circa la loro sfera personali e, nello specifico, sui loro dati sensibili.
La condivisione, anche legata a consigli tecnici, potranno quindi essere armi importanti per le imprese che vorranno investire tempo e risorse in questo ambito.
Tra le IV, vediamo che maggior peso lo ricoprono le variabili legate alla community (Community Identity ed Affiliation Need) rispetto ai Technical Motives,; quindi sempre con riferimento al mondo del business,

vediamo che se le aziende riuscissero ad incentivare la formazione di queste community, di cui i consumatori desiderano essere parte, i vantaggi ne deriverebbe non sono da sottovalutare.

DISCUSSIONE DEI RISULTATI E CONCLUSIONI

Arrivati alla fine del nostro percorso di tesi, vediamo quali sono state le evidenze che sono venute fuori dai nostri studi, cercando di capire quali possono essere gli sviluppi futuri che vedranno coinvolti questi flussi di ricerche. Il contributo principale che questo elaborato porta, è senza dubbio l'enorme lavoro che è stato fatto, che come abbiamo visto si divide in due fasi principali: la fase dell'analisi qualitativa e la fase dell'analisi quantitativa. L'analisi qualitativa, o esplorativa che dir si voglia, è stata necessaria in quanto data l'importanza del tema, e la mancanza di solide ricerche alle spalle: questo lavoro ha richiesto un grande ammontare di lavoro di ricerca e selezione dei commenti rilevanti.
Come abbiamo visto invece dal fulcro della nostra ricerca, l'analisi dei dati, i risultati ottenuti sono stati importanti, seppur sarà necessario indagare ancora nel futuro, per arrivare ad una visione completa del fenomeno. La metodologia scientifica applicata per legger i dati che abbiamo raccolto grazie alla nostra survey ci ha permesso di dare un senso ai nostri dubbi ed avere a disposizione dei risultati, che andranno poi implementati nel futuro. Le analisi sul coefficiente di regressione hanno dimostrato l'effetto positivo del bilanciamento dei driver sulle variabili dipendenti relative al comportamento degli utenti.
Questi risultati ci dicono infatti che la negoziazione degli individui tra Privacy Concern e i fattori positivi Technical Motive ed i fattori legati al concetto di Community porta spesso a risultati positivi soprattutto per le variabili dipendenti di Loyalty e Recommendation Intention e Active Partecipation. Possiamo dedurre quindi che i benefits derivanti dalle dimensioni in questione sono importanti per superare le preoccupazioni circa la propria privacy.
In aggiunta i coefficienti di regressione che indagano separatamente i fattori positivi ci hanno dimostrato che le variabili "Affiliation Need" e "Community Identity" sono ritenuti più importanti dei Technical Motives per spiegare il fenomeno indagato.

I driver che abbiamo utilizzato si sono rivelati coerenti per descrivere il comportamento di quegli individui che rilasciano i propri dati personali in fase di acquisto dell'applicazione. Indagando maggiormente sui driver che abbiamo selezionato può portare ai soggetti di business benefici importanti: abbiamo visto che il flusso di ricerche presenti sul tema della self – disclosure è ancora in divenire e probabilmente non ha ancora prodotto il potenziale di quello che per il momento si può solamente intravedere.
Riallacciandoci al tema del paradosso della privacy, le nostre regressioni hanno confermato i nostri sospetti, ovvero che seppur gli individui dichiarano di essere preoccupati per quanto riguarda i propri dati, sono in realtà propensi a negoziare questi stessi dati, in primis con benefici legati all'inclusione che essere parte di una community ti dona, e successivamente anche con le informazioni sulla funzionalità delle applicazioni,

che comunque va inquadrato in un'ottica di community dato che questi scambi hanno luogo all'interno di gruppi, forum o blog.
Il cosiddetto marketing relazionale non è sicuramente una novità, infatti è ormai noto che il beneficio legato alla creazione di una community di brand porta grandi vantaggi ai soggetti di business, basti pensare ai casi Ducati o Disney. Quello che però ancora non si sapeva, e che dovrà essere implementato in futuro con altre ricerche degli esperti, era che il senso di appartenenza ad una comunità potrebbe avere effetti positivi come fattore di negoziazione per il rilascio di dati sensibili, allo stesso pari di altri fattori, come ad esempio la personalizzazione e la fiducia che abbiamo visto nel secondo capitolo.
Sarebbe interessante in futuro sviluppare uno studio approfondito di questo fenomeno, magari collegato con altri studi, che permetta di avere una visione più ampia del tema in questione dando dati empirici da utilizzare per migliorare il business.

BIBLIOGRAFIA

1. Acquisti A. John L. (2013) What Is Privacy Worth?. Journal Of Legal Studies: 34 - 41
2. Acquisti A. John L. Loewenstein G. (2012) The Impact of Relative Standards on the Propensity to Disclose. Journal of Marketing Research 49: 160 - 174
3. Andrade, E., Kaltcheva, V., Weitz, B., (2002) Self-disclosure on the web: The impact of privacy policy, reward, and company reputation. Advances in Consumer Research 29: 350 – 353
4. Barth S., De Jong M. (2017) The privacy paradox - Investigating discrepancies between expressed privacy concerns and actual online behavior - A systematic literature review. Telematics and Informatics 34: 1038 – 1058
5. Benamati, J., Zafer, O., Smith, J., (2017) Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. Journal of information science 43: 583 - 600
6. Blank, G., Lutz C., (2018) Benefits and harms from Internet use: A differentiated analysis of Great Britain. New Media & Society 20: 618 – 640
7. Chen D. Fraiberger S. Moakler R. Provost F. (2017) Enhancing Transparency and Control When Drawing Data-Driven Inferences About Individuals. Big data 5: 56 – 87
8. Christofides, E., Muise A. Desmarais S., (2009) Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes? CYBERPSYCHOLOGY & BEHAVIOR 12: 441 - 445
9. Demmers, J., Van Dolen, M., Weltevreden, J., (2018) Handling Consumer Messages on Social Networking Sites: Customer Service or Privacy Infringement? International Journal of Electronic Commerce 22: 8-35
10. Ginosar A. Ariel Y. (2017) An analytical framework for online privacy research: What is missing? Information & Management 54: 948 – 957
11. Gross, G., Acquisti, A., (2005) Information Revelation and Privacy in Online Social Networks (The Facebook case).Workshop on Privacy in the Electronic Society
12. Grossklads, J., Acquisti, A., (2005) Privacy and Rationality in Individual Decision Making. Security & Privacy: 24 – 30
13. Guragai B. Hunt N. Neri M. Taylor E. (2017) "Accounting Information Systems and Ethics Research: Review, Synthesis, and the Future. Journal Of Information Systems 31: 65 – 81
14. Hallam, C., Zanella, G., (2017) Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. Computer in Human Behavior 68: 217 - 227
15. Hsin-Yi, H., (2016) Examining the beneficial effects of individual's self-disclosure on the social network site. Computer in Human Behavior 57: 122 – 132
16. Jordaan, Y., Van Heerden, G., (2017) Online privacy-related predictors of Facebook usage intensity. Computer in Human Behavior 70: 90 – 96

17. Junglas, I., Johnson N., Spitzmu ̈ller, C., (2008) Personality traits and concern for privacy: an empirical study in the context of location-based services. European Journal of Information Systems 17: 387
18. Kokolakis, S., (2017) Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security 64: 122 – 134
19. Krafft, M., Arden, C., Verhoef, P., (2017) Permission Marketing and Privacy Concerns - Why Do Customers (Not) Grant Permissions? Journal of Interactive Marketing 39: 39 - 54
20. Krishnan M. (2006) The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. MIS Quarterly 30: 13 - 28
21. Krishen, A., Raschke, R., Close, A., Kachroo, P., (2017) A power-responsibility equilibrium framework for fairness: Understanding consumers' implicit privacy concerns for location-based services. Journal of business research 73: 20 – 29
22. Li, Y., (2012) Theories in online information privacy research: A critical review and an integrated framework. Decision Support Systems 54: 471 – 481
23. Li, H., Luo, X., Zhang, J., (2017) Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors. Information & Management 54: 1012 - 1022
24. Markos, E., Milne, G., Peltier, J., (2017) Information Sensitivity and Willingness to Provide Continua: A Comparative Privacy Study of the United States and Brazil. Journal of public policy & marketing 36: 79
25. Martin, K., Borah, A., Palmatier, R., (2017) Data Privacy: Effects on Customer and Firm Performance. Journal of Marketing 81: 36 – 58
26. Martin, K., Murphy, P., (2017) The role of data privacy in marketing, Journal of the Academy of Marketing Science 45: 135 – 155
27. Mosteller, J., Poddar, A., (2017) To Share and Protect: Using Regulatory Focus Theory to Examine the Privacy Paradox of Consumers' Social Media Engagement and Online Privacy Protection Behaviors. Journal of Interactive Marketing 39: 27 – 38
28. Nam T., "Does ideology matter for surveillance concerns? (2017) Telematics And Informatics 23: 134 - 156
29. Nam T. (2018) Untangling the relationship between surveillance concerns and acceptability. Journal of Information Management 38: 262 - 269
30. Norberg, P., Horne, D., (2007) The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. The Journal of Consumer Affairs 41: 100 – 126
31. Nottingha, Q., Collignon, S., Warkentin, M., Ziegelmayer, J.,(2015) The interpersonal privacy identity (IPI): development of a privacy as control model. Information Technology and Managementn17: 341 – 360
32. Pagani, M., Malacarne, G., (2017) Experiential Engagement and Active vs. Passive Behavior in

Mobile Location-based Social Networks: The Moderating Role of Privacy. Journal of Interactive Marketing 37: 133 – 148

33. Potoglou D. Dunkerley F. Patil S. Robinson N. (2017) (COMPUTERS IN HUMAN BEHAVIOR, 2017) Public preferences for internet surveillance, data retention and privacy enhancing services: Evidence from a pan-European study. Computers In Human Behavior 75: 811 – 825
34. Prince, C., (2018) Do consumers want to control their personal data? Empirical evidence. International Journal of Human-Computer Studies 110: 21 – 32
35. Schuster S. Van Den Berg M. Larrucea X. Slewe T. Ide-Kostic P. (2017) Mass surveillance and technological policy options: Improving security of private communications. Computer Standards & Interfaces 50: 76 - 82
36. Spottswood, E., Hancock, J., (2017) Should I Share That? Prompting Social Norms That Influence Privacy Behaviors on a Social Networking Site. Journal of Computer-Mediated Communication, 22. 55–70
37. Steinfeld, N., (2017) Track me, track me not: Support and consent to state and private sector surveillance. Telematics and Informatics 34: 1663 – 1672
38. Wottrich, V., Van Reijmersdal, E., Smit, E., (2018) The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. Decision Support Systems 106: 44 – 52
39. Wu H. Zhang H. Cui L. Wang X. (2017) A Heuristic Model for Supporting Users' Decision-Making in Privacy Disclosure for Recommendation. Security and Communication Networks: 1 – 13
40. Zhao, L., (2014) Disclosure Intention of Location-Related Information in Location-Based Social Network Services. International Journal of electronic commerce 16: 53 - 59
41. Zlatolas, L., Welzer, T., Hericˇko, M., Hölbl, M., (2015) "Privacy antecedents for SNS self-disclosure: The case of Facebook. Computer in Human Behavior 45: 158 - 167