Università
Ca'Foscari
Venezia

Corso di Laurea Magistrale in
Marketing e Comunicazione

Tesi di Laurea

Ca' Foscari
Dorsoduro 3246
30123 Venezia

L'utilizzo di big data online per fini commerciali: gli effetti del datagate Facebook e Cambridge Analytica nel privacy paradox

Relatore
Ch. Prof. Francesco Casarin

Correlatore
Ch. Prof. Fabrizio Panozzo

Laureanda
Miriam Battistella
Matricola 848496

Anno Accademico
2017 / 2018

Indice

Introduzione

Il presente elaborato propone di descrivere le prime reazioni avute dagli iscritti a Facebook dopo il datagate che lo ha coinvolto nel caso Cambridge Analytica, iniziato il 17 marzo 2018, con la pubblicazione sul New York Times e sul The Guardian degli articoli "How Trump Consultants Exploited the Facebook Data of Millions" e "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach", in seguito all'inchiesta di Matthew Rosenberg, Nicholas Confessore, Carole Cadwalladr e Emma Graham-Harrison.

La vicenda suscitato una serie di reazioni altalenanti nel corso dell'anno, che ha portato alla chiusura definitiva di Cambridge Analytica e a una radicale messa in discussione di Facebook. Il social network ha subito in prima battuta un crollo finanziario del titolo in Borsa, che ha coinvolto altre aziende attive nella gestione di piattaforme online. Mark Zuckerberg stesso è stato personalmente chiamato a rispondere davanti al Congresso Statunitense e alle autorità comunitarie, tra cui il Parlamento Europeo. Questo è servito a risolvere parte della crisi finanziaria e reputazionale della piattaforma, insieme a una campagna di sensibilizzazione, promossa da Facebook stessa e alla pubblicazione dei risultati economici positivi registrati dalla holding nel primo trimestre dell'anno. La vicenda non comunque avuto dei risvolti positivi per il social network che a luglio, oltre a esser stato sanzionato dall'autorità britannica per la protezione dei dati personali, ha subito un crollo del numero di iscritti sia in Europa che negli Stati Uniti.

A oggi Facebook è ancora il social network più utilizzato al mondo, tanto da poter contare su oltre due miliardi di iscritti e un tasso di crescita del 15% nel solo 2017 (Global Digital 2018, 2018). Il sito rappresenta un mezzo di comunicazione, d'informazione e intrattenimento, per cui gli utenti sono disposti a fornire i propri dati per poter accedere ai servizi offerti dalla piattaforma. Gli stessi alimentano il modello di business del social, basato sulla vendita delle informazioni condivise alle aziende interessate a svolgere un tipo di comunicazione commerciale mirata,

che permetta loro di raggiungere più efficientemente la propria domanda di mercato. Tale strategia prevede dunque una diffusa condivisione di dati personali, che incide di conseguenza sulla privacy degli utenti stessi. Ciò nonostante il sito continua a registrare ogni anno un aumento degli iscritti, giovando come molti altri software online, di un'economia di rete che gli permette di assumere un valore maggiore in proporzione al numero di utilizzatori della piattaforma.

L'analisi dei dati personali a fini commerciali non rappresenta una violazione per gli utenti delle piattaforme se tale attività avviene con il controllo e l'approvazione dagli stessi. Tuttavia, il caso Facebook e Cambridge Analytica ha dimostrato come anche uno dei maggiori siti di social network possa mettere in pericolo la privacy dei suoi iscritti, i quali potrebbero essere soggetti a una raccolta dati non autorizzata. Lo stesso gestore del sito potrebbe avere delle difficoltà nel controllo dell'utilizzo di dati da parte di terzi. Quanto avvenuto a marzo 2018 ha effettivamente esemplificato tale pericolo, incidendo sulla fiducia riposta dagli utenti nell'intero processo di scambio e trattamento di dati.

Il controllo dei dati online rappresenta un ostacolo anche per le persone che consciamente decidono di esporre in rete delle informazioni personali. L'uso di internet è infatti caratterizzato dal fenomeno del privacy paradox, ovvero da una generale incapacità che hanno gli utenti di gestire l'esposizione delle proprie informazioni online. In questo caso sono determinanti diversi fattori soggettivi, tra cui la presenza di gratificazioni immediate e la necessità di accedere ad alcuni servizi offerti dalla rete, che determinano la svalutazione dei rischi dati dalla condivisione di dati personali in rete.

La seguente ricerca si propone di analizzare le modalità di utilizzo delle informazioni personali in rete, considerando l'identità digitale come uno strumento con cui rappresentare la propria personalità all'interno del contesto sociale di appartenenza. Il datagate Facebook e Cambridge Analytica è stato scelto ai fini di verificare le reazioni degli utenti a un ampio caso di abuso di dati personali in rete, fatto ai danni del social network più diffuso al mondo. Oltre a una prima definizione dei fatti, l'indagine mira a definire gli effetti del datagate sulla fiducia degli iscritti alla piattaforma, sia verso il social network stesso, che più in generale, verso le aziende che svolgono attività di trattamento di dati online. Nell'indagine è

stato considerato anche il fenomeno del privacy paradox, quale fattore incisivo nella gestione dei dati online.

La ricerca è stata svolta in due fasi distinte, basate su una prima analisi della letteratura esistente e una successiva verifica di quanto rilevato. Durante la prima parte della ricerca sono stati definiti e analizzati tre elementi fondamentali relativi alla condivisione e alla gestione dei dati personali nella rete: la gestione dell'identità digitale, le normative a tutela della privacy e il fenomeno del privacy paradox. Successivamente è stato condotto uno studio empirico di tipo quantitativo, volto a verificare quanto individuato nella prima parte della ricerca e analizzare le reazioni degli utenti al caso del datagate Facebook e Cambridge analitica.

L'indagine presente nella seconda parte della ricerca è stata preceduta da una breve descrizione del caso preso in considerazione. I fatti sono stati in parte analizzati secondo l'inchiesta di Matthew Rosenberg, Nicholas Confessore, Carole Cadwalladr e Emma Graham-Harrison svolta tra il 2016 e il 2018 e pubblicata a marzo 2018 sulle testate del New York Times e sul The Guardian, per i quali è emersa l'intera vicenda. Le prime reazioni economiche successive alla vicenda, sono state invece approfondite considerando in particolare quanto pubblicato sul quotidiano economico Il sole 24 ore.

Lo studio empirico svolto nella presente ricerca è stato realizzato mediante una raccolta di dati primari, avvenuta sottoponendo un campione di circa duecento soggetti ad un questionario a risposte chiuse e semichiuse. Gli individui sono stati selezionati da una popolazione di riferimento costituita da studenti iscritti a un corso di laurea triennale o magistrale presso l'università Ca' Foscari, nati tra il 1990 e il 1999 e iscritti a Facebook.

L'analisi delle risposte raccolte nei questionari ha permesso di definire e descrivere parte delle reazioni al datagate Facebook e Cambridge Analytica avute da una certa categoria di utenti iscritti al social. Le informazioni ottenute sono state successivamente confrontate con quanto individuato nella letteratura di riferimento, allo scopo di individuare elementi comuni presenti sia nella prima parte della ricerca che nel caso pratico preso in esame.

In questo modo è stato possibile ipotizzare alcuni percorsi di sviluppo futuro per le aziende che intendono includere delle attività di data retention e data mining online nelle loro strategie di business e in particolare in quelle di marketing. Tali considerazioni sono state tratte in base a quanto emerso dallo studio della letteratura e ai comportamenti individuati nell'analisi dei dati primari.

Lo studio del caso Facebook e Cambridge Analytica e l'analisi dati primari raccolti nel corso della ricerca sono stati realizzati nei primi sei mesi successivi alla pubblicazione delle inchieste del New York Times e del The Guardian. La distribuzione dei questionari inoltre, è avvenuta all'interno di una popolazione composta da soli studenti iscritti a corsi di laurea presso l'Università Ca' Foscari di Venezia. Tali limiti sono stati considerati nella valutazione complessiva della vicenda. Per questa ragione, le conseguenze tratte dallo studio svolto sono definibili nel breve periodo.

Capitolo 1
L'identità digitale nel rapporto cliente - azienda

1.1
Definizione di identità digitale

Il concetto d'identità è definibile come l'insieme di caratteristiche appartenenti all'aspetto fisico, psicologico, sociale e storico di una persona. Il processo di costruzione dell'identità, rappresenta una sequenza di fasi che solitamente avviene all'interno di un contesto sociale pubblico. L'individuo può decidere quali informazioni rendere note sulla propria vita privata, controllando la propria immagine pubblica all'interno dell'ambiente in cui vive. Il processo di identificazione costituisce il riconoscimento della persona da parte di terzi, che ne attribuiscono delle caratteristiche distintive. Nel complesso la fase di riconoscimento è composta da tre elementi fondamentali: coloro tenuti all'identificazione della persona, i tratti fisici e caratteriali considerati nella valutazione e le peculiarità che distinguono l'individuo dagli altri soggetti (Camp, 2004).

A livello istituzionale la questione dell'identificazione è stata risolta con l'utilizzo di documenti ufficiali, nei quali sono riportate alcune informazioni basilari attribuibili a ciascun individuo, che ne permettono un riconoscimento pubblico. Tali atti rappresentano una prova fisica certificata dell'identità della persona, in quanto sono rilasciati a livello istituzionale, previo un complesso sistema di registrazione che ne comporta una validità pluriennale e che li rende di per sé degli strumenti di riconoscimento. Nonostante che nel corso degli ultimi decenni vi sia stata una digitalizzazione della burocrazia, finora i documenti per l'autenticazione delle persone non sono stati interamente sostituiti dai sistemi digitali, grazie alle garanzie che ancora oggi la dimensione fisica permette. Internet ha cambiato il

concetto d'identità e il processo di autenticazione, secondo le intenzioni perseguite dagli utenti online e i sistemi per la raccolta e la gestione delle informazioni personali. La rete consente un riconoscimento parziale della persona, la quale può essere rappresentata solamente attraverso l'insieme di informazioni scambiate a livello digitale, senza un effettivo riscontro fisico (Camp, 2004).

Nel mondo occidentale, gli individui hanno la possibilità di scegliere se navigare in internet anonimamente oppure dichiarando la propria identità. Nel primo caso è stato riscontrato come gli individui siano inclini a cambiare il proprio atteggiamento, tendenzialmente in modo negativo, assumendo dei comportamenti talvolta offensivi (Zhao, Grasmuck, Martin, 2008). Ciò avviene a fronte di una repressione di alcuni caratteri identitari, che solitamente si verifica invece nella realtà, allo scopo di controllare la propria immagine all'interno del contesto sociale di riferimento.

L'uso di internet ha plasmato un nuovo modello comportamentale attribuibile all'utilizzo dei social network. In questo genere di piattaforme infatti, le persone pur agendo in un contesto puramente digitale, devono relazionarsi con il proprio ambiente di riferimento tra cui ad esempio, quello familiare o quello professionale. Dall'analisi di quest'ultimo caso, si è evinto come l'atteggiamento predominante in questo contesto consista in una rappresentazione pubblica del sé ideale, che non sempre rispecchia la realtà. Nei social network infatti gli individui tendono a controllare maggiormente la propria identità, gestendo il proprio grado di visibilità in modo più accurato rispetto a una dimensione fisica, sapendo che quanto pubblicato online avrà un riscontro anche nelle relazioni realmente esistenti. Proprio nella considerazione di quest'ultimo aspetto, è stata riscontrata una tendenza a rendere noti solo le qualità migliori della propria identità, talvolta eccedendo in una rappresentazione ideale della persona, piuttosto che descrivendo quella reale (Zhao, Grasmuck, Martin, 2008).

Online gli utenti possono controllare razionalmente la condivisione d'informazioni personali con terzi, agendo di conseguenza sulla rappresentazione della propria persona. Ciò nonostante, in molti casi l'uso della rete e gestione dei propri dati non viene svolta secondo dei criteri logici, ma piuttosto in modo emotivo, a seconda di esigenze immediate o reazioni spontanee. Gli utenti dunque non sempre riescono

ad avere una piena padronanza dei propri caratteri identitari online, tanto che a oggi esistono degli strumenti digitali in cui è possibile definire in modo completo anche i tratti più latenti degli individui. In particolare, un'analisi delle conversazioni registrate nelle piattaforme di messaggistica diretta, nei motori di ricerca e nei siti di e-commerce ha fatto emergere degli atteggiamenti più istintivi, liberi dalle considerazioni sui giudizi altrui. Lo studio complessivo delle impronte digitali lasciate dagli utenti permette di avere un'immagine complessiva dell'identità della persona, sia per quanto riguarda la sua aspirazione ideale sia per la sua personalità reale (Zhao, Grasmuck, Martin, 2008).

A oggi esiste un notevole interesse nello studio delle attività svolte dagli utenti all'interno della rete, giustificabile dal bisogno di conoscenza della domanda di mercato. Gli stessi gestori dei motori di ricerca e dei social media offrono alle aziende degli strumenti per lo studio delle dinamiche online, al fine di facilitare l'elaborazione di informazioni chiave per la comprensione dei consumatori e dell'ambiente competitivo. Spesso sono le imprese stesse a creare delle pagine web o delle piattaforme di e-commerce da cui trarre dei dati primari, utili alla conoscenza del mercato (Leonardi, Huysman, Steinfield, 2013).

L'analisi della domanda attraverso la rete internet deve rispettare l'individualità degli utenti, considerando il fatto che le informazioni online rappresentano l'insieme degli elementi costituenti l'identità della persona. Le attività di navigazione online devono esser fatte consapevolmente dagli individui, i quali devono essere informati dell'utilizzo che terzi fanno dei loro dati personali, al fine di permettere loro la gestione della propria identità virtuale. La sottrazione impropria di dati, oltre a costituire una violazione delle norme sulla privacy, rappresenta anche un motivo di diffida degli utenti verso le aziende attive nella rete. Per questo motivo, le istituzioni pubbliche mondiali, insieme ai grandi attori privati coinvolti nel settore, stanno cercando di collaborare al fine di definire la materia con più precisione, individuandone i diritti e i principi di navigazione online e punirne eventuali (Li, Luo, Zhang, Xu, 2016).

1.1.1
Privacy online: concetto e principi

La tutela dell'identità ha comportato la concettualizzazione della privacy che negli anni è stata interpretata secondo diverse soluzioni, prendendo in considerazione vari aspetti del rapporto tra sfera individuale e società. Nel 1995 Schement e Curtis descrissero la privacy come un mezzo di tutela contro gli interessi invasivi dello Stato, riprendendo in qualche modo la visione Settecentesca della piccola casetta citata da Lord Chatham nel suo discorso davanti al Parlamento inglese, per la quale le forze militari della Corona non potevano violarne l'intimità. Nel ventesimo secolo, la rivoluzione del digitale fu d'impulso per una rivalutazione del concetto della privacy, avvertita come la tutela delle informazioni appartenenti alla persona. Nel 1967, Alan Westin fu uno dei primi studiosi a concettualizzare il fenomeno dell'information privacy, associandolo alla capacità delle persone e delle organizzazioni pubbliche e private di autodeterminare quali informazioni comunicare nel proprio ambiente di riferimento e secondo quali modalità (Westin, 1967).

Per quanto ancora oggi il concetto della privacy subisca delle interpretazioni diverse a seconda del Paese, della cultura e del tipo di settore in cui viene considerato, la tutela dei dati personali è inseribile all'interno di un sistema di giustizia relativo all'utilizzo delle informazioni altrui. Nel corso degli anni Novanta, il tema stato analizzato anche dal punto di vista etico, con lo scopo di definire i parametri di equità riconducibili all'argomento. Ne è emersa una scala multidimensionale di valutazione della privacy, in cui si sono distinte quattro principali tipologie di abusi, relativi a: la raccolta e l'uso non autorizzato di informazioni, gli errori di gestione e gli accessi non autorizzati effettuati da terzi.

Tale strumento di valutazione, il quale doveva fornire una visione globale dell'utilizzo dei dati, è stato contestualizzato alla dimensione online, considerato l'enorme volume di informazioni raccolte e scambiate all'interno della rete. Nel contesto specifico è stato possibile studiare la percezione di equità nell'utilizzo delle informazioni online sia come metodo di definizione delle norme giuridiche

atte a regolare il settore, che come strumento per la comprensione del rapporto tra piattaforme online e utenti. In quest'ultimo caso in particolare, è stato approfondito il rapporto tra aziende e consumatori finali, per cui il web costituisce uno strumento di comunicazione istantanea tra i diversi attori di mercato, a qualsiasi stadio della filiera operino (Smith, Milberg, Burke, 1996).

L'esistenza di piattaforme online nelle quali svolgere delle attività di raccolta di dati personali rappresenta per le imprese lo strumento per la realizzazione di comportamenti potenzialmente opportunistici mentre per gli utenti costituisce un nuovo elemento di vulnerabilità nel controllo della privacy. Le attività di studio del mercato svolte online formano parte della strategia di marketing digitale aziendale, in cui è fondamentale il rispetto dei bisogni e dei valori degli utenti della rete clienti al fine di migliorare il rapporto commerciale con la domanda ed evitare di mettere a rischio l'intera brand reputation (Malhotra, Kim, Agarwal, 2004).

Nonostante la propensione a condividere delle informazioni personali rappresenti una percezione puramente soggettiva, a oggi sono state stabilite quattro dimensioni su cui si delinea il rispetto e la tutela della privacy online, ovvero: la conoscenza delle modalità di raccolta dei dati, il grado di controllo e consapevolezza garantiti agli utenti e il comportamento atteso dalle parti coinvolte nello scambio (Smith, Milberg, Burke, 1996). Il primo fattore costituisce un punto di partenza dello studio dell'information privacy, dal quale si è dedotto come esista una percezione di equità basata sulla reciprocità dello scambio. Gli individui che navigano in internet sono infatti disposti a scambiare le proprie informazioni personali solo quando possono trarne dei benefici concreti, come ad esempio i servizi offerti dalle piattaforme online o le promozioni commerciali distribuite dalle aziende nei loro siti internet. Un secondo elemento di rispetto dell'information privacy è rappresentato invece dal controllo dato agli utenti sulle proprie informazioni personali, il quale è percepito come il principale strumento di tutela per gli utenti contro possibili comportamenti opportunistici. Tale facoltà è rappresentata dalla possibilità di scegliere se accettare o meno di far sottoporre i propri dati personali a trattamenti di raccolta e analisi previsti dalle piattaforme online. A oggi le imprese possono servirsi di vari strumenti digitali per permettere che questo avvenga in modo agevole e diretto, al fine di garantire ai propri utenti

un senso di protezione che ne incrementi la fiducia nel rapporto complessivo (Cohen, 1987).

La percezione di stabilità, definibile con il controllo delle proprie informazioni, è alimentata dalle note di avviso relative al trattamento dei dati personali che l'azienda comunica ai propri utenti. La consapevolezza degli individui, nonostante non rappresenti una scelta attiva all'interno delle pratiche online, è comunque considerata un elemento garante dell'equità tra le parti, in quanto comporta un atteggiamento di trasparenza e sincerità da parte del detentore delle informazioni.

Infine i principi di correttezza dell'information privacy possono rifarsi alle norme che generalmente riguardano le attese all'interno di un qualsiasi rapporto vincolato da uno scambio reciproco tra le parti. Queste infatti, maturano un'aspettativa di correttezza reciproca che va oltre le norme giuridiche e il raggiungimento degli interessi propri (Smith, Milberg, Burke, 1996).

I principi di tutela delle informazioni personali rappresentano gli stessi concetti di equità e giustizia all'interno del sistema di raccolta e analisi delle informazioni scambiate online, anche nel contesto di un rapporto tra azienda e consumatore finale. Gli utenti della rete si attendono gli stessi comportamenti di rispetto della privacy presenti nelle ricerche di mercato e nelle relazioni tipiche del marketing tradizionale. Per questo motivo saranno disposti a condividere i propri dati solo in un contesto di consapevolezza del trattamento a cui sono sottoposti durante la navigazione online e di reciprocità nello scambio di informazioni fatto durante la ricerca (Malhotra, Kim, Agarwal, 2004).

1.2
La ricerca online a fini commerciali

In passato il marketing trovava nella televisione uno dei principali mezzi di comunicazione del mondo occidentale, per la diffusione e la frequenza con cui era utilizzata. Oggi questa posizione sembra essere occupata da internet. Secondo il Global Digital Report 2018 pubblicato da Hootsuite e We are Social, il 53% della

popolazione mondiale utilizza internet per circa cinque ore al giorno per comunicare, informarsi, intrattenersi e fare acquisti. Le informazioni sui comportamenti di navigazione e sulle abitudini degli utenti sono ricavabili proprio grazie alle tracce che gli stessi utenti lasciano online all'interno dei motori di ricerca, delle piattaforme di e-commerce ma soprattutto all'interno delle piattaforme di social media, come i social network e i blog di discussione. Per questo motivo, nonostante la televisione sia ancora un importante mezzo di comunicazione generalista, le aziende non possono non considerare il web come un nuovo strumento per raggiungere i propri utenti. La rete permette all'offerta di relazionarsi direttamente con la domanda e di studiarne i comportamenti, al fine di ricavare delle informazioni utili alla comprensione del mercato (Kaplan,Haenlein, 2010).

Gli strumenti di comunicazione online come i siti internet e i profili social, consentono di gestire in modo completo i contatti tra aziende e utenti, assumendo il ruolo il ambivalente di divulgazione e di conoscenza dei soggetti coinvolti. A livello esterno, le organizzazioni possono infatti mettersi in contatto con la propria comunità d'interesse, nella prospettiva di instaurare una relazione diretta e una comunicazione immediata e in tempo reale. Tale approccio, basato sulle interazioni multilaterali tra gli utenti e le aziende ha trasformato il marketing tradizionale, il quale invece, come nel caso della televisione, si rivolgeva al grande pubblico sfruttando una comunicazione passiva. Il piano di comunicazione può dunque prevedere l'uso dei social media, non solo come mezzo promozione online dell'azienda o dei suoi prodotti, ma anche come strumento per lo studio delle caratteristiche della domanda. Per quanto la di raccolta e analisi dei dati nella rete costituiscano delle attività di marketing più tecniche e meno evidenti agli utenti della rete, la conoscenza delle preferenze individuali permette la realizzazione di una comunicazione commerciale più personalizzata, capace di interagire in modo mirato con la domanda in base alle esigenze raccolte dagli individui stessi (Leonardi, Huysman, Steinfield, 2013).

Le aziende che intendono rendere più efficiente la loro strategia di comunicazione possono integrare l'uso delle piattaforme online sia per un primo studio dell'ambiente competitivo e della domanda, che per una fase finale di controllo dei

feedback. Online infatti tutte le attività di ricerca, comunicazione e acquisto svolte dagli utenti costituiscono una fonte di informazione codificata e registrabile dai motori di ricerca e dai siti internet. Le data retention e il data mining costituiscono i termini tecnici che definiscono la raccolta e l'elaborazione dei grandi volumi dati presenti online, usati per trarne una conoscenza utile allo studio delle caratteristiche di mercato e in particolare della domanda. Le aziende hanno un forte interesse nell'investire in questo settore dal quale possono analizzare le dinamiche di business, aggiornandosi sulle preferenze e sui trend della domanda. Le informazioni tratte dalla rete permettono alle aziende di pianificare con maggior certezza le attività future, preparandosi ad affrontare i conseguenti effetti delle scelte assunte (Linoff, Berry, 2011).

Le aziende possono svolgere delle attività di data retention servendosi di vari strumenti disponibili in rete, che comprendono sia piattaforme di e-commerce, dove raccogliere gli ordini di vendita, che siti di social media, in cui interagire con clienti e persone interessate al prodotto. A questa categoria appartengono diversi tipi di pagine web, tra cui forum di dibattito, piattaforme di collaborazione, blog e microblog, mondi virtuali e social network, tutti definibili come piattaforme di comunicazione multilaterale in cui è presente una rete di collegamenti digitali, capace di unire i vari nodi di interazione rappresentati dagli individui stessi (Leonardi, Huysman, Steinfield, 2013).

Le aziende che integrano l'uso dei social media all'interno delle proprie strategie di marketing possono migliorare il loro rapporto con i consumatori finali, incrementando la brand loyalty e rendendo più efficienti le attività di customer relationship management. Tuttavia per far si che ciò avvenga, l'uso dei social media deve essere preceduto da una pianificazione strategica nella quale l'azienda definisce gli obiettivi e l'immagine aziendale, rispetto a un determinato ambiente competitivo e a dei segmenti di target a cui rivolgersi. Lo svolgimento della ricerca deve avvenire con una prima fase di pianificazione dei propositi aziendali a cui segue la scelta delle metriche di misura e dei termini di paragone dai impiegare nell'analisi. In questo modo, lo studio dei dati raccolti online permette alle aziende di comprendere le dinamiche di mercato in cui sono inserite e scegliere quali strategie di sviluppo adottare in futuro (Kaplan,Haenlein, 2010)

1.2.1
Lo studio della domanda nei social media

L'utilizzo dei social media ha stravolto il rapporto tra aziende e consumatori, cambiando radicalmente i processi di raccolta e gestione delle informazioni, provenienti dai diversi attori di mercato. La rete ha permesso di sviluppare un dialogo diretto tra consumatori, produttori e distributori rivoluzionando il marketing tradizionale. Con l'utilizzo di internet le aziende hanno acquisito la possibilità di attivare una comunicazione di tipo bilaterale verso i propri utenti, monitorandone le reazioni in modo molto più efficace e veloce rispetto al passato (Coviello, Milley, Marcolin, 2001).

Le innovazioni del mondo del digitale hanno cambiato le tecniche di comunicazione commerciale, partendo dalla trasformazione stessa delle caratteristiche e della gestione delle informazioni. Internet ha accelerato lo scambio di dati, aumentandone i volumi e permettendo la creazione di nuovi sistemi di elaborazione e gestione della conoscenza. Il mercato ha iniziato a considerare le informazioni sotto forma di prodotti, aventi delle caratteristiche simili alle commodities. I dati rappresentano infatti risorsa non scarsa, non differenziabile e continuamente rigenerabile, aventi un valore economico proporzionale al loro utilizzo. Il marketing, inteso come l'insieme di informazioni scambiate tra produttore, distributore e cliente si è così evoluto, insieme al rinnovamento delle comunicazioni all'interno della filiera, sia nelle attività a monte che in quelle a valle. La data retention e il data mining hanno avuto un ruolo strategico nella comunicazione commerciale, offrendo alle aziende più strumenti per lo studio della domanda e rendendo i dati più aggiornati e accessibili rispetto al passato (Glazer, 1991).

Una delle prime fasi per la definizione di una strategia aziendale è lo studio dell'ambiente di business e in particolare la valutazione dell'attrattività di mercato. Quest'ultima comporta l'analisi del ciclo di vita del prodotto e lo studio del tasso di crescita del mercato, da cui è possibile dedurre i trend di business attuali e futuri. Tali conoscenze permettono alle aziende di stabilire come orientarsi nel medio e

nel lungo termine, stabilendo quali mosse adottare attraverso la realizzazione di piani strategici. Tuttavia, la presenza di eventi destabilizzanti e poco prevedibili ostacolano una tale programmazione, riducendo le possibilità di successo attese per il raggiungimento degli obiettivi aziendali (Huber, 1984).

Le informazioni reperibili in rete sono solitamente aggiornate, trasferibili e disponibili a costi minori rispetto al passato. Queste possono essere impiegate nelle attività di marketing al fine di maturare una profonda conoscenza sulle dinamiche attuali e future del proprio settore di riferimento. Tendenzialmente, il grado di affidabilità delle previsioni fatte è proporzionale al numero di informazioni prese in considerazione. Per questo motivo, i grandi volumi di dati presenti in internet, permettono alle aziende di realizzazione migliori strategie di marketing predittivo. Quest'ultimo infatti, comporta un'analisi approfondita delle attività svolte online dai propri consumatori, al fine di dedurne le scelte future e dunque realizzare un'offerta commerciale coerente e personalizzata. Dalle attività di web marketing è inoltre possibile ottenere dei feedback diretti, con cui valutare le reazioni della domanda di mercato, rispetto alle strategie di comunicazione assunte. Infine, dall'analisi dei social media, le aziende possono verificare vari aspetti di mercato tra cui il life time value dei propri clienti, le previsioni di spesa della domanda e l'andamento offerta commerciale dei propri concorrenti (Ståhlberg, Maila, 2013).

Internet ha inoltre permesso alle aziende e in particolare ai produttori, di avere un canale di comunicazione immediata con i consumatori finali. Ciò ha ridotto l'importanza delle figure degli intermediari, rendendo il rapporto tra le parti più diretto rispetto al passato e di conseguenza, aumentando la competitività di mercato. Le aziende infatti, hanno più di opportunità di relazionarsi con i singoli soggetti appartenenti alla domanda di mercato, tanto da riuscire a considerare più facilmente anche i bisogni delle nicchie minori. Ne è scaturito un aumento dell'interesse nella diversificazione dell'offerta commerciale, coerentemente alle varie esigenze della domanda, sminuendo invece il ruolo delle strategie aziendali orientate alla produzione (Glazer, 1991).

In passato i rapporti tra aziende e consumatori finali si basavano su un tipo di comunicazione di tipo passivo, legata a un marketing meno evoluto e più

tradizionale. Oggi invece, attraverso le ICT, le aziende possono servirsi dei social media al fine intraprendere un marketing di tipo relazionale, integrando le informazioni sulla domanda di mercato provenienti dalla rete ai modelli strategici tradizionali, al fine di incrementare le vendite e fidelizzare i propri clienti (Glazer, 1991). La realizzazione di una comunicazione personalizzata rende più efficaci le attività promozionali, aumentando il coinvolgimento tra consumatore e brand. Le aziende che riescono a creare un rapporto diretto con i propri clienti all'interno delle piattaforme di social media, hanno la possibilità di stabilizzarlo in una prospettiva temporale di lungo termine. Ciò è possibile attraverso una costante raccolta di informazioni espresse dagli utenti online, sulle quali pianificare un tipo di strategia di fidelizzazione dei soggetti considerati (Ståhlberg, Maila, 2013).

Le aziende che utilizzano internet per aumentare la propria visibilità e il coinvolgimento i propri clienti, possono intervenire sul valore percepito del brand, facendo in modo che si instauri una sorta di rapporto reciproco tra le parti. I social media possono essere utilizzati dalle aziende come delle piattaforme per lo scambio reciproco di opinioni, in cui il profilo aziendale rappresenta lo strumento per l'interazione con il mercato. In questo caso, gli operatori di marketing devono essere capaci di stabilire un piano di comunicazione social all'interno della propria strategia aziendale, al fine gestire il dibattito, cercando di stimolare il passaparola tra gli utenti e arginando gli interventi negativi. L'azienda deve in ogni caso dimostrare un atteggiamento di ascolto ed empatia verso i bisogni espressi dalla domanda, allo scopo di coinvolgere gli utenti della piattaforma, mantenendo comunque un controllo attivo della brand reputation (Kim, Ko, 2012).

Infine, le piattaforme online sono fondamentali nello studio della domanda di mercato, in quanto forniscono delle metriche di misura oggettive relative al grado d'interesse e fidelizzazione dimostrato dagli utenti verso l'attività di marketing aziendale. I social media permettono infatti di gestire una comunicazione di tipo bilaterale, per cui le attività promozionali svolte online, possono essere seguite e giudicate dagli utenti con commenti e messaggi. L'impresa può dunque ottenere un feedback diretto dalla propria domanda di mercato, con cui valutare in tempo reale le reazioni alle attività di marketing realizzate. Gli indici individuabili in questo contesto, permettono inoltre di comparare i risultati raggiunti dalla propria attività

di comunicazione, con gli obiettivi definiti in fase di pianificazione e con le attività svolte dalla concorrenza. Questo serve all'azienda per avere degli stimoli di autocritica, sui quali intervenire per il miglioramento della comunicazione futura (Kaplan, Haenlein, 2010).

1.2.2
Principali strumenti di data retention

Il processo di studio del mercato da parte delle aziende è nato negli anni cinquanta, grazie ai primi programmi di analisi statistica, creati per organizzare e gestire i primi dati digitali. Una delle prime tecniche sviluppate allora riguarda il processo KDD (knowledge discovery from database), attraverso il quale è possibile estrarre delle informazioni da un database, selezionando, processando e interpretando i dati raccolti, al fine di ottenere una conoscenza da utilizzare per le decisioni di marketing. A seguito di tali studi, sono state sviluppate ulteriori tecniche di data mining basate su metodi statistici esistenti, le quali sono state gradualmente inserite in nuovi software per la raccolta dei dati, utilizzati già allora per la ricerca applicata. Tra gli anni Novanta e Duemila, i software di data mining hanno subito una crescita tale, da diventare una tecnologia indipendente, capace di supportare lo studio dei fenomeni in vari ambiti della scienza applicata e diventare uno degli elementi alla base della business intelligence. I sistemi di raccolta ed elaborazione dei dati online utilizzati dalle imprese come strumento di analisi del mercato, hanno rivoluzionato l'approccio di studio della domanda, migliorando la definizione delle preferenze, delle abitudini e della disponibilità economica di ciascun individuo (Mikut, Reischl, 2011).

A oggi le aziende che intendono svolgere un'analisi di mercato attraverso il data mining, possono iniziare realizzando una prima raccolta di dati primari in internet. Online esistono una serie di strumenti capaci di registrare e salvare le attività di navigazione provenienti dai visitatori delle piattaforme. I mezzi più comuni utilizzati dalle imprese per l'analisi di mercato sono: l'e-mail, le web analytics, i

cookies, i sistemi di RFIDs, l'e-commerce e i social network. Le aziende che decidono di fornire un servizio di newsletter spesso utilizzano dei software appositi con cui ottengono informazioni demografiche sui propri destinatari, arricchite anche dai tassi di apertura e interesse valutati per ogni singolo contatto (Ståhlberg, Maila, 2013).

Le pagine web gestite direttamente dalle imprese, raccolgono invece più informazioni sui comportamenti di navigazione dei visitatori del sito. Dalle web analytics è possibile infatti dedurre una serie di elementi strettamente legati alle attività svolte dagli utenti all'interno del sito internet. Queste infatti, registrano il tempo e le frequenze di visita per ogni pagina appartenente al sito web, facilitando l'individuazione dei contenuti che suscitano un maggiore interesse. L'introduzione di cookies consente inoltre di approfondire la conoscenza dei comportamenti degli utenti, registrando le loro attività di ricerca e navigazione svolte di fuori del sito aziendale. Nei dispositivi mobile invece, la presenza di sistemi di RFID (radio frequency identification) localizza ogni visitatore del sito, individuandone la posizione e gli spostamenti, anche per un lungo periodo di tempo. Quest'ultima tecnologia è risultata particolarmente significativa per le aziende di retail aventi uno store fisico, le quali possono analizzare in modo più dettagliato le dimensioni e le dinamiche del proprio bacino di vendita, per creare dei messaggi promozionali online rivolti ai soli utenti localizzati nelle vicinanze del punto vendita, sviluppando un tipo di comunicazione mirata (Laczniak, Murphy, 2006).

Lo stesso tipo di informazioni si possono ottenere anche attraverso le piattaforme e-commerce, in cui sono registrate le caratteristiche e le attività svolte dai clienti durante il processo di acquisto, permettendo la profilazione completa di ciascuno di loro. Lo studio dei comportamenti d'acquisto può essere fatto anche offline, servendosi di metodi di ricerca tradizionali, che comprendono l'osservazione del cliente all'interno del punto vendita. Tuttavia la rete permette di ottenere più informazioni sulle caratteristiche e sull'atteggiamento della domanda rispetto ai sistemi di analisi classici, grazie alle informazioni che spesso sono richieste agli utenti per il completamento degli acquisti nella piattaforma. Esistono inoltre degli indici specifici con cui valutare l'andamento delle vendite e la navigazione nella

piattaforma, individuando quali preferenze sono presenti nell'offerta aziendale ed eventualmente quali ostacoli impediscono le transazioni (Ståhlberg, Maila, 2013).
Infine, la realizzazione di una comunicazione commerciale svolta attraverso i canali di social media, consente una gestione più ampia degli aspetti di vendita e di studio della domanda. Se negli anni Novanta i siti di social network erano percepiti come dei soli strumenti per favorire la socializzazione tra sconosciuti, oggi le aziende possono utilizzare i profili aziendali al fine interagire con la propria domanda, osservandone il comportamento e raccogliendo le impressioni sui prodotti e sulle campagne promozionali. Le imprese possono così monitorare le proprie attività di marketing online, servendosi di indici specifici per la comprensione delle reazioni delle domanda, considerando conversazioni, condivisioni e apprezzamenti registrati all'interno del proprio profilo e dei post pubblicati da terzi che trattano del brand (Ståhlberg, Maila, 2013).
Oggi le aziende possono raccogliere un volume maggiore di informazioni online, con una varietà di contenuti più ampia rispetto al passato, a costi ridotti e con una maggiore frequenza di aggiornamento. Questo consente di individuare con più precisione i bisogni della domanda, per cui realizzare una certa strategia commerciale, adattando l'offerta alle preferenze espresse dal mercato, con lo scopo di ottenere un maggior vantaggio competitivo (Fan, Bifet, 2013).

1.3
I social network

Internet è composto da una serie di collegamenti digitali, che permettono un ininterrotto flusso di conversazioni, strutturate in modo diverso a seconda delle piattaforme esistenti. I social network consentono agli individui di coltivare la propria rete relazionale online, mediante la rappresentazione della propria identità in profili web, dove pubblicare una una breve descrizione di sé, condividere opinioni, foto e video e interagire con altri utenti appartenenti alle cerchie di interesse, che possono esistere o meno anche nella realtà. Anche le aziende hanno

imparato a instaurare delle relazioni all'interno dei social network, sviluppando un tipo di comunicazione personalizzata, capace di raggiungere stakeholder esistenti e utenti interessati all'offerta commerciale (Smith, Kawasaki, 2014).

Con l'espressione di social network si identifica un servizio digitale online, in cui è possibile costruire un proprio profilo, mediante il quale tracciare la propria rete sociale virtuale. Le funzioni disponibili all'interno delle piattaforme permettono una piena personalizzazione del proprio profilo, da cui gli altri utenti possono riconoscere l'individuo e decidere di formalizzare o meno tale connessione, senza che questa esista effettivamente anche nella vita reale. D'altro canto i profili hanno una visibilità controllata, per cui solitamente ciascuno sceglie a chi riservare l'accesso dei contenuti pubblicati, al fine di mantenere un minimo controllo sulle proprie informazioni personali. I social network basano il loro funzionamento sulla gestione delle singole pagine personali, che sono il punto di riferimento per ciascun iscritto, con cui possono scegliere come rappresentare la propria identità all'interno delle proprie cerchie. I profili inoltre sono il mezzo con cui gli utenti condividono i propri interessi e comunicano con gli altri attraverso dibattiti pubblici o messaggi privati (Papacharissi, 2010).

Il primo sito internet che corrispondente alla definizione di social network è SixDegrees.com. Lanciata nel 1997, la piattaforma permetteva di creare profili privati da cui gestire una propria lista di conoscenze, da cui potevano sorgere delle comunità chiuse. SixDegrees.com univa le funzioni di comunicazione, condivisione e collegamento che in precedenza erano state sviluppate solo separatamente da altri siti internet. Ciascuno poteva presentarsi ad altri utenti, inviare messaggi privati, gestendo la visibilità delle proprie informazioni. La piattaforma fu chiusa nel 2000, per il fatto di esser considerata un'innovazione troppo insolita. A posteriori fu valutata come una piattaforma di gran lunga anticipatrice del corso dei tempi e delle esigenze delle domanda, considerando che allora gran parte degli utenti non trovava utile socializzare online. Tale comportamento si giustificava per il fatto che internet allora non era ancora molto diffuso, per cui non esisteva un'ampia rete di connessioni online, mentre quella esistente era ancora troppo lenta (Boyd, Ellison, 2007).

Tra il 1997 e il 2001 vi fu un'esplosione di social network indirizzati a far incontrare persone appartenenti alle stesse comunità tramite l'utilizzo della rete internet. Alcuni dei più famosi siti aperti in questo momento furono ad esempio AsianAvenue, dedicato alla comunità asiatica residente negli Stati Uniti; Black Planet per quella afroamericana e MiGente per quella ispanica. Più tardi nei primi anni del duemila, aprirono le piattaforme online dedicate invece ad argomenti di interesse comune, come nel caso di Linkedin, Visible Path e Xing, dedicati al mondo del business; Care2 per gli attivisti; Couchsurfing.com per i viaggiatori e MyChurch per i cattolici. Infine tra il 2004 e il 2005, fu inventata l'ultima categoria di social network, specializzati per categorie di contenuti, tra cui YouTube, Flickr e Last.FM nei quali condividere rispettivamente video, foto e musica (Boyd, Ellison, 2007).

La condivisione di interessi comuni permetteva alla persone di avere un motivo specifico di utilizzo delle piattaforme. Il primo obiettivo dei siti finora descritti non era quello di trasferire online le relazioni esistenti nella realtà, ma di aiutare le persone a fare delle nuove conoscenze utilizzando la rete. Questo concetto si ridusse gradualmente con l'introduzione di social network più generalisti come MySpace e Facebook. Il primo nacque nel 2003, come piattaforma di blogging e messaggistica a sostituzione di Friendster, un social network analogo, chiuso in quell'anno per una serie di problemi di funzionamento. MySpace riuscì a ottenere un'ampia diffusione immediata grazie ai gruppi musicali indipendenti di successo iscritti alla piattaforma, che in breve attirarono celebrità più conosciute dal grande pubblico. Il sito ebbe un grande successo tra i giovani, grazie alle diverse web communities che si crearono per discutere su temi di interesse comune e condividere ogni genere di contenuto. Qualche anno più tardi Facebook avrebbe preso il suo posto, approfittando di alcuni timori sorti sul controllo delle interazioni tra adulti e minori. Il social network venne fondato ad Harvard nel 2004 da Mark Zuckerberg, Eduardo Saverin, Andrew McCollum, Dustin Moskovitz e Chris Hughes. Il sito nato come strumento di comunicazione per gli studenti dell'ateneo, divenne nel giro di due anni una delle piattaforme di condivisione più utilizzate al mondo grazie alla possibilità di scelta della lingua, alla vasta offerta di funzioni, alla varietà di contenuti e alla presenza di personaggi famosi e grandi aziende (Boyd, Ellison, 2007). A oggi Facebook Inc. rappresenta la più grande holding di social

networking al mondo, considerando che oltre Facebook, la stessa società controlla anche le piattaforme di direct messaging Messenger e WhatsApp e il social network Instagram, a cui sono iscritti circa un miliardo di utenti.

1.3.1
Distribuzione e trend di mercato

A oggi, Facebook è il social network più popolare al mondo, grazie a oltre due miliardi utenti iscritti in tutto il mondo, su circa tre miliardi di persone registrate ai social network. L'azienda basa il suo modello di business sulla vendita di pubblicità personalizzata, indirizzata agli utenti che d'altro canto, possono così accedere ai servizi di comunicazione e condivisione offerti dalla piattaforma. Entrata in borsa il 12 maggio 2012, in quindici anni di attività è cresciuta a tal punto da raggiungere nel 2017 un fatturato di oltre 40 miliardi di dollari, entro i quali Facebook ha acquisito e sviluppato altre attività, tra cui i visori per la realtà digitale Oculus Rift, le applicazioni di messaggistica Facebook Messenger e WhatsApp, a oggi le più utilizzate al mondo e il social network Instagram (Global Digital, 2018).
Facebook per quanto largamente diffuso, non è presente in tutti i Paesi del mondo e in particolare in Russia e in Cina, dove esistono altre piattaforme di social network e direct messaging online. Il sito di Mark Zuckerberg non è riuscito ad attecchire in questi Paesi, come invece è stato per il resto del mondo, a causa di motivi storico culturali, che hanno così limitato un possibile monopolio di Facebook sul mercato globale. Già nei primi anni di diffusione dei social network infatti, i cittadini russi e cinesi si sono orientati verso la scelta di siti nazionali del tutto analoghi a Facebook, per le funzioni offerte e le modalità d'uso. Gli utenti di questi Paesi hanno infatti ritenuto il social network americano meno affidabile e intuitivo rispetto ad altre piattaforme locali, più familiari e congruenti con la cultura del posto. In Russia ad esempio, i social network più diffusi sono Vkontakte e Odnoklassniki, entrambe gestite dall'azienda di comunicazione e servizi online Mail.ru. Nate nel 2006, i due siti costituiscono a oggi le principali piattaforme di social network della Russia,

grazie a un'offerta di funzioni analoghe a Facebook ma più coerenti con le esigenze e le preferenze del mercato locale (Baran, Wolfgang, 2015).

Il mercato cinese della messaggistica istantanea elettronica è invece occupato dal brand WeChat, a cui attualmente sono iscritti circa 980 milioni di utenti, i quali oltre a usufruire di un servizio di comunicazione diretta, hanno a disposizione un portafoglio elettronico con cui pagare gli acquisti online. La piattaforma fu rilasciata nel 2011 dalla holding pubblica cinese Tencent Holding Limited, tramite il supporto finanziario pubblico che ne promosse la progettazione tecnica e la diffusione commerciale. La stessa società fu a sua volta fondata grazie alla creazione di QQ, una prima piattaforma di messaggistica online, nata nel Paese alla fine degli anni Novanta. Allora il sito rappresentava una risposta concreta alle prime piattaforme di comunicazione online come AIM, ICQ Buddy, Skype e al social network Friendster. La sua diffusione fu tale che in breve divenne parte integrante della cultura cinese, tanto che ancora oggi conta ancora 843 milioni di utilizzatori (Boyd, Ellison, 2007). L'applicazione è ricollegabile anche al social network Qzone, il più popolare nel Paese, in cui è possibile tenere un diario personale dove condividere foto, musica e video (Global Digital 2018, 2018).

Oltre al potere oligopolistico di Facebook e delle holding Mail.ru e Tencent, esistono altre piattaforme di condivisione e comunicazione sia nel mercato occidentale che in quello orientale. Youtube ad esempio, è seconda a Facebook per il numero di iscritti, con un milione e mezzo di utenti attivi. La società fondata nel 2005 come sito di video sharing, venne acquistata da Google l'anno dopo, che la rese parte integrante di Google+. Infine nella lista dei social media più diffusi al mondo compaiono anche alcune piattaforme di microblogging tra cui gli occidentali Tumblr e Twitter, seguite rispettivamente da 568 e 330 milioni di utenti e il sito cinese Sina Weibo a cui sono registrate 376 milioni di persone.

Gli utenti iscritti ai social media nel 2018 sono più di tre miliardi di persone di cui oltre il 90% si collega al proprio profilo tramite l'uso di dispositivo mobile. Le regioni aventi il più alto tasso di diffusione sono il nord America, il nord Europa e l'Asia nord orientale, dove le percentuali di penetrazione sono comprese tra il 65% e il 70% (Global Digital 2018, 2018).

I social network, che a oggi registrano un tasso di crescita mondiale del 10%, rappresentano delle piattaforme per la comunicazione, la condivisione di contenuti, l'intrattenimento e l'e-commerce. I social sono una sorta di Cloud condiviso, al quale ciascun utente ha accesso tramite un profilo proprio e con il quale può interfacciarsi con delle pagine semplici e funzionali. I siti di social network facilitano il fenomeno del crowdsourcing online, definibile come la produzione di conoscenza collettiva condivisa, realizzabile tramite il grande volume di persone coinvolte in un dialogo comune. Ne scaturisce così un effetto rete delle piattaforme social, per cui il valore del servizio offerto dal sito è proporzionale al numero di iscritti, tanto che è l'uso stesso della piattaforma ad attrarre e coinvolgere nuovi utenti (Hanna, Rohm, Crittenden, 2011).

1.3.2
I social network come fonte di conoscenza

La diffusione dei social network ha avuto una crescita esponenziale nel breve periodo, con il conseguente aumento di contenuti pubblicati all'interno delle piattaforme. Le informazioni condivise quotidianamente nei social media rappresentano opinioni, preferenze e gusti di una parte della popolazione. Le aziende sono interessate a estrarre e analizzare tali contenuti per comprendere le preferenze della domanda e avere una panoramica completa e aggiornata dei destinatari dell'offerta commerciale. L'obiettivo delle aziende è infatti quello di riuscire a ottenere più informazioni possibili sulla domanda, allo scopo di realizzare una profilazione e una segmentazione del mercato, rendendo la comunicazione promozionale più efficiente possibile. Per fare questo sono stati creati vari sistemi di ricerca e analisi dei contenuti pubblicati nelle piattaforme di social network, su cui si è sviluppata una sorta di intelligenza artificiale facilmente fruibile dalle imprese incorporano la raccolta e il trattamento di dati personali nelle loro strategie di mercato (Zeng, Chen, Lusch, Li, 2010).

Il web marketing realizzato per mezzo di piattaforme di social networking presume la presenza un social media plan, in cui le aziende possono descrivere gli obiettivi e le strategie di comunicazione che intendono realizzare. La stesura di un piano marketing comporta già dalle prime fasi la scelta delle piattaforme in cui si intende effettuare la propria campagna promozionale e l'analisi dei mittenti a cui è destinato il messaggio. Lo studio delle informazioni scambiate nelle piattaforme social permette di capire le percezioni sull'offerta commerciale e di ottenere un feedback sulle attività di marketing svolte (Hanna, Rohm, Crittenden, 2011).

Le attività di ricerca svolte all'interno dei social media possono essere di vario genere a seconda dello scopo per cui vengono fatte o della tipologia di informazioni considerate. La conoscenza prodotta dall'analisi delle piattaforme supporta le decisioni di marketing in tema di analisi dell'ambiente competitivo, valido per descrivere il posizionamento del brand e migliorare lo studio delle dimensioni e dei bisogni della domanda, fondamentale invece per la segmentazione e la profilazione del target. L'azienda può decidere di realizzare delle ricerche proprie, raccogliendo da sé dei dati primari, aggiornati e coerenti con gli obiettivi di studio stabiliti. Ciò comporta l'attuazione di un processo di data cleaning capace di individuare e correggere eventuali mancanze ed errori, necessari per procedere ad una successiva analisi di quanto raccolto. Le informazioni tratte dallo studio dei dati devono essere comparate con altre fonti e contestualizzate nel tempo e nel luogo di raccolta, allo scopo di trasformarle in una conoscenza utile a supportare le decisioni di marketing (Batrinca,Treleaven, 2014).

La ricerca svolta nei social network può essere di tipo qualitativo o quantitativo a seconda dei dati che si intendono estrarre. Nel primo caso è possibile condurre una ricerca etnografica, per comprendere quali utenti e comunità sono interessate all'azienda, oppure fare delle osservazioni, mediante il campionamento casuale di dialoghi, commenti e opinioni sul brand e i prodotti offerti. Quest'ultima pratica è detta social media listening e permette di registrare il comportamento degli utenti online, individuando riscontri positivi o negativi dell'attività commerciale dell'impresa e di quella della concorrenza. Nonostante esistano degli strumenti in open source che aiutano gli operatori di marketing a ottimizzare l'analisi delle conversazioni (Es. Twitter Search, Social Mention), le ricerche di questo tipo non

possono essere generalizzate all'intera popolazione, ma devono essere inserite in un progetto di ricerca più ampio che comprenda altri metodi di studio (Hanna, Rohm, Crittenden, 2011).

Per quanto riguarda invece la ricerca quantitativa online, gli operatori del marketing devono assicurarsi che questa venga condotta nel modo più affidabile possibile cercando di stilare preventivamente un progetto di ricerca al fine di pianificare gli obiettivi e le fasi di raccolta e analisi delle informazioni. Come avviene generalmente nelle ricerche di mercato, è necessaria una prima fase di raccolta di dati grezzi, detta in questo caso web scraping. Per i social media è possibile servirsi di software specifici capaci di estrarre contenuti e parole chiave utilizzate con più frequenza dagli utenti all'interno di blog personali, forum di discussione e commenti. I dati sono poi salvati in database aziendali e ripuliti da eventuali errori, ripetizioni ed elementi fuorvianti dal tema di studio. Da quì è possibile intraprendere l'analisi del sentiment, intesa come lo studio delle emozioni e degli atteggiamenti dagli utenti oppure un'analisi dei contenuti, per interpretare il significato delle informazioni raccolte. Nel primo caso sono utilizzati dei software per il text mining in cui i contenuti raccolti sono studiati in base a una codificazione e una classificazione delle parole, alla quale segue un'interpretazione complessiva degli indici estratti. Per quanto riguarda l'analisi del contenuto invece, vi è una codificazione dei concetti, fatta allo scopo di classificare e schematizzare i dati raccolti, gestendoli in base al significato dei dialoghi, presenti all'interno di forum e commenti (Kaplan,Haenlein, 2010).

La raccolta dei dati svolta all'interno dei social network consente di raggiungere un ampio numero di persone in tempo reale, servendosi di un tipo di comunicazione meno formale, rispetto alle ricerche tradizionali. Ciò supporta le aziende nello studio di mercato e nella comprensione delle dinamiche della domanda, dando loro nuove opportunità di contatto con i propri stakeholder e con nuovi utenti potenzialmente interessati. Tuttavia onde evitare possibili problemi di copertura e campionamento della popolazione, è fondamentale che questo genere di ricerche siano contestualizzate in riferimento al periodo temporale di analisi, agli strumenti utilizzati, alle piattaforme prese in considerazione, ai soggetti e alle comunità coinvolte nel campionamento (Serrat, 2017).

Capitolo 2
Norme sulla tutela dei dati

2.1
Strumenti di tutela esistenti

"Il più povero degli uomini può, nella sua casetta, lanciare una sfida, opponendosi a tutte le forze della Corona. La casetta può essere fragile, il suo tetto può essere traballante, il vento può soffiare da tutte le parti, la tempesta può entrare e la pioggia può entrare, ma il re d'Inghilterra non può entrare; tutte le sue forze non osano attraversare la soglia di tale casetta in rovina."

(William Pitt, Conte di Chatham, discorso pronunciato alla House of Lords nel marzo 1763)

Le parole di Lord Chatham annunciavano con largo anticipo quello che nei nostri anni sarebbe diventato il problema della tutela della privacy. Nonostante la trascrizione del discorso del politico inglese sia poi diventata uno dei primi documenti a favore della protezione della riservatezza individuale, la vera e propria origine dei diritti privacy è rappresentata dal saggio *"The right to be alone"* di Louis D. Brandeis e Samuel Warren. I due avvocati, originari di Boston, il 15 dicembre 1890 pubblicarono una loro relazione, riguardante l'ipotesi sulla necessità di istituire un diritto di essere lasciati soli a godere della propria vita. Quando Brandeis diventò uno dei giudici membri della corte suprema statunitense, riaffermò lo stesso principio dello jus solitudinis in una dissenting opinion, relativa a un caso di contrabbando di alcolici, in cui erano state effettuate delle intercettazioni telefoniche per oltre cinque mesi. La maggioranza dei giudici considerava del tutto legittima l'attività investigativa dell'FBI, perchè i cavi del telefono non intaccavano il domicilio dell'imputato. Braides invece, convinto che l'evoluzione della fisica e la tecnica avrebbero portato a scovare anche le emozioni

più celate, difese le parti dell'imputato, affermando il dovere della Corte di impedire una possibile invasione dello spazio individuale. (Masera, Scorza, 2016).

Internet appartiene ora a una di quelle innovazioni tecnologiche e fisiche ipotizzate da Braides un secolo prima. Internet venne utilizzato per la prima volta negli anni Sessanta, con la creazione di ARPANET, una rete di computer limitata, sviluppata per scopi militari dal dipartimento della difesa degli Stati Uniti. Dagli anni Settanta in poi venne adottato anche da alcune università americane come mezzo di comunicazione per la creazione di forum di discussione tra studenti e ricercatori. Parallelamente anche in Europa vennero create delle reti online nazionali, come in Francia, Gran Bretagna e Finlandia. Nel 1989 internet venne definitivamente aperto ai civili, attraverso la fine di ARPANET e la nascita del linguaggio HTML (Gubitosa, 2007).

Rispetto all'1% del 1995, oggi il 53% della popolazione mondiale utilizza internet per informarsi, comunicare, acquistare e vendere, tanto da essere considerato un mondo virtuale a dimensione globale (L'e-commerce in Italia, 2017). Ciò nonostante le legislazioni in tutto il mondo non sono riuscite a regolamentare a pieno la rete, faticando nel restare al passo con le innovazioni digitali.

Negli anni Novanta, la maggioranza degli utenti pensava che internet dovesse restare uno strumento neutro e libero, al di fuori delle logiche nazionali e in particolare dai meccanismi legislativi che regolamentano il mondo. Nell'immaginario comune infatti, si diffuse l'idea di una rete anarchica, giustificata dal semplice fatto di essere un mezzo di comunicazione, d'informazione e d'intrattenimento internazionale. Il più celebre rappresentante di questa corrente di pensiero fu l'attivista statunitense John Peter Barlow, che nel 1996 pubblicò la sua Dichiarazione d'indipendenza del Cyberspazio. Il testo che ancora oggi rappresenta una delle tappe fondamentali per l'evoluzione di internet, si basava sulla visione di un mondo digitale governato da un sistema di cyber-libertarismo, capace di superare i sistemi giuridici nazionali contrari e vincolanti al carattere internazionale e libero dei collegamenti online (Murray, 2016). Il web non doveva essere soggetto a una sovranità nazionale o internazionale, considerata da Barlow come un potere esterno e invadente. Ognuno avrebbe potuto godere dello spazio digitale, al fine di poterlo sfruttare al meglio per esaltare la propria

autodeterminazione al di là dei vincoli giuridici imposti da ogni Stato, considerato ormai come un'istituzione antiquata e decadente.

Le ideologie di libertà e autoregolamentazione della rete vennero presto smentite dalla realtà dei fatti, con le diverse violazioni al diritto sulla privacy e alla libertà di espressione. Uno dei casi più importanti fu quello relativo all'arresto del giornalista cinese Shi Tao, che nel 2004 utilizzò Yahoo! Mail per comunicare in anonimato a un sito in lingua cinese, la decisione del partito comunista di boicottare la ricorrenza del massacro di piazza Tienanmen. Sotto le pressioni delle autorità cinesi, Yahoo! comunicò le informazioni tecniche sul mittente del messaggio, rivelando in questo modo l'identità dello scrittore, al quale venne imposto il carcere. Le reazioni internazionali di sdegno da parte delle associazioni di giornalisti e delle istituzioni pubbliche, fecero pressione sul governo cinese, che tuttavia scarcerò il giornalista solo nel 2013. L'operato di Yahoo! venne fortemente criticato, riaccendendo il dibattito sulla necessità di una regolamentazione della rete uniforme a livello internazionale (Ji, 2014).

A oggi Internet, è una tecnologia indispensabile per lo sviluppo economico, sociale e culturale di tutti gli Stati che basano i propri ordinamenti su un sistema democratico. Gli utenti della rete infatti, sono in primo luogo cittadini, a cui ogni ordinamento attribuisce diritti e facoltà, che non possono essere messi a rischio nella dimensione virtuale, vantaggio di agenti economici privati, gestori delle piattaforme online. Questo perché la rete è composta da miliardi di persone che proiettano la propria identità nel mondo digitale, attraverso i dati che loro stessi lasciano ogni giorno online. Le informazioni costituiscono l'identità di ogni essere umano, che in rete rischiano di essere messe alla mercé di tutti. A differenza di quanto avviene nella realtà, in internet gli utenti tendono a sottovalutare il valore dei propri dati personali, focalizzandosi di più sui benefici ottenuti dall'uso della rete. Per questa ragione non sempre chi naviga online riesce a comprendere i rischi che comporta una tale esposizione. Le istituzioni pubbliche hanno dunque il dovere di agire per garantire a tutti coloro che usufruiscono della rete di esser tutelati contro i possibili abusi sui propri dati personali, perpetrati sia da grandi aziende che da singoli individui. (Masera, Scorza, 2016).

2.1.1
Regolamentazione della rete internazionale

Nel corso degli anni Novanta, molte istituzioni internazionali si posero la questione su come affrontare il tema della gestione della rete, nonostante sussistessero ancora forti ripulse sulla necessità di una governance del mondo del web. Uno dei primi documenti a cui è possibile far riferimento è la dichiarazione prodotta da Educause nel 1992, chiamata "Rights and Responsibilities of Electronic Learners". L'atto conteneva una serie di norme relative alla produzione e all'uso delle informazioni online, destinate all'educazione e in particolare agli istituti universitari. Nei primi anni del Duemila, altre associazioni internazionali decisero di seguire le orme di Educause, contribuendo alla formazione di un sistema normativo comune. Tra questi, i progetti più rilevanti furono la realizzazione di una bozza della "Internet Rights Charter" prodotta dall'Association for Progressive Communication e la formazione di una seconda costituzione internazionale del web, promossa dall'associazione "The Web We Want" di Tim Barners-Lee. Ancora oggi il tema della governance della rete è affrontato periodicamente, nel corso di vari summit a carattere internazionale, organizzati dalle organizzazioni di settore tra cui Electronic Frontier Foundation, NETMundial Multistakeholder Statement e Internet Governance Forum (Mensi, Falletta, 2015).

Una delle svolte più rilevanti per la definizione di una normativa internazionale fu l'intervento di Hillary Clinton a supporto di alcune organizzazioni giornalistiche statunitensi, che nel 2005 chiesero all'ONU l'universalizzazione del diritto di Free Speech a fronte dell'arresto del giornalista cinese Shi Tao. Il principio di libertà di parola invocato in quel contesto, rappresenta infatti, uno dei diritti fondamentali riconosciuto non solo nella Costituzione statunitense, ma anche nella Dichiarazione dei diritti umani delle Nazioni Unite. A riguardo, l'ordinamento ONU sui diritti umani è ancora oggi un punto di riferimento per la definizione dei diritti di navigazione online, essendo un sistema legislativo valido in tutto il mondo, che riconosce e fa valere i diritti fondamentali anche nel contesto digitale. La normativa permette di tutelare chiunque navighi nella rete, definendo quali sono le attività

che costituiscono pratiche scorrette, spesso realizzate allo scopo di soddisfare interessi economici opportunistici.

Il web costituisce uno spazio senza confini, che ha dato luogo a violazioni analoghe, al di là delle legislazioni nazionali. I giudici, dovendo affrontare casi simili, posti dalle diverse attività di data retention online, fanno spesso riferimento ai diritti fondamentali riconosciuti a livello internazionale, al fine di tutelare omogeneamente tutti gli utenti. Ciò nonostante le istituzioni nazionali sono comunque chiamate a contribuire al rinnovamento e al rafforzamento delle garanzie costituzionali, intervenendo con una logica bottom-up.

Il dialogo multistakeholder e multilevel finora sviluppato tra istituzioni e grandi players è orientato alla creazione di un Internet Bill of Rights ONU, che possa essere comunemente condiviso in tutte le nazioni un cui è utilizzata la rete, al fine di armonizzare il diritto internazionale, anche per quanto riguarda lo scambio di dati tra utenti e aziende. L'obiettivo comune si basa sulla trasposizione nella sfera digitale di alcune facoltà già esistenti, garantendo che vengano mantenute le condizioni perché la rete continui adessere libera e fruibile (Rodotà, 2010).

L'armonizzazione delle normative sulla privacy e sulla gestione dei dati privati online, iniziò a esser considerata già alla fine degli anni Novanta, con la creazione delle prime norme per lo scambio di dati tra Paesi diversi. Nel 1995 ad esempio, l'Unione europea stabilì delle regole per il trasferimento dei dati personali verso Paesi terzi, inserendo l'argomento all'interno del quarto capo della Direttiva 95/46. Con questo, il Parlamento affidava alla Commissione europea il ruolo di controllore sulle garanzie date dagli altri Paesi in tema di trattamento dati e di verifica del rispetto dei principi definiti dalla stessa direttiva.

Nel 1998, Unione Europea e Stati Uniti stabilirono inoltre un accordo sul libero trasferimento di dati appartenenti a cittadini europei verso aziende statunitensi, che operano secondo un ordinamento diverso da quello europeo. Tale accordo, detto Safe Harbor, stabiliva dunque delle regole comuni, accettate da entrambe le parti, regolando definitivamente le attività di data retention e data mining svolte da oltre quattromila aziende americane in Europa. Il Safe Harbor dava luogo così una regolamentazione omogenea e coesa della rete, definendo così anche i processi di data retention e data mining tra Europa e Stati Uniti. L'accordo riconosceva

l'esistenza di alcuni principi basilari tra cui la consapevolezza dell'utente sulla gestione dei dati personali, la protezione della privacy sulle informazioni trattate e la sicurezza dei dati raccolti (Weiss, Archick, 2016).

Nel 2015, la Corte di Giustizia dell'Unione Europea ha sancito la fine del Safe Harbor, dichiarandolo inadeguato alla protezione e alla tutela dei dati dei propri cittadini e dando nuovamente il dovere di vigilanza e controllo alle autorità nanzionali. In questo senso l'istituzione ha voluto riaffermare la necessità del rispetto dello stesso livello di protezione garantito dalle direttive precedenti e dai diritti fondamentali riconosciuti dall'Unione. Nell'immediato c'è stata una inevitabile lacuna normativa sul trattamento dei dati appartenenti a cittadini europei, svolto al di fuori dei territori di competenza delle istituzioni europee e in particolare negli Stati Uniti, in cui sono presenti i maggiori players di settore. Per evitare ulteriori vuoti normativi, l'Unione ha conferito alle autorità nazionali garanti della privacy il ruolo di controllare l'operato delle società statunitensi, rafforzando il potere esecutivo che già in precedenza avevano. Per ristabilire gli equilibri e rafforzare gli standard di sicurezza precedenti è stato definito nel 2016 il "EU-US Privacy Shield" che attualmente si presenta come un accordo normativo internazionale ancora in fase di progettazione (Loidean, 2016).

Il quadro normativo internazionale per la tutela dei dati personali non è stato dunque ancora definito del tutto. Ogni Paese ha realizzato una propria regolamentazione della rete internet e di gestione dei dati online. Allo stesso tempo, sono pochi gli accordi che ufficialmente stabiliscono le modalità di raccolta, trasferimento e trattamento dei dati in modo condiviso tra Paesi diversi. Tali fragilità rappresentano un ostacolo sia nel settore privato che in quello pubblico, a fronte della necessità di gestire grandi quantitativi di informazioni all'interno di un network mondiale. Ciò nonostante si è sviluppata una forte consapevolezza rispetto al nesso che lega la protezione dei dati personali con lo sviluppo dell'economia digitale. La definizione delle corrette modalità di trattamento dei dati nella rete internazionale spetta finora spetta alle Corti o alle Autorità di Garanzia nazionali, che spesso sono chiamate a rispondere di casi specifici, non direttamente trattate dalla legge. Tuttavia ci si attende una futura svolta nella politica internazionale per l'organizzazione di piani di internazionali

regolamentazione della sicurezza online e della gestione del trattamento dei dati (Soro, 2016).

2.1.2
Ordinamento europeo antecedente maggio 2018

Il 25 maggio 2018 è entrato in vigore il nuovo Regolamento n. 2016/679 relativo alla protezione delle persone fisiche, con riguardo al trattamento e alla libera circolazione di tali personali che ha abrogato la direttiva 95/46/CE. Tale intervento normativo è stato realizzato dal Parlamento Europeo e dal Consiglio con l'obiettivo di stabilire definitivamente una regolamentazione omogenea, valida a definire in tutti i Paesi membri dell'Unione le corrette modalità di gestione delle attività di raccolta e trattamento dei dati (De Stefani, 2018).

Il nuovo regolamento rappresenta una complessa revisione degli interventi fatti dall'Unione Europea negli ultimi vent'anni in materia di trattamento dei dati personali e privacy. Il tema della gestione delle informazioni è frutto di una lunga formulazione giuridica, precedente alla diffusione della rete internet e basata sui principi fondatori dell'Unione stessa. Uno dei primi riferimenti per la tutela della privacy è costituito infatti l'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU), firmata da dodici Stati membri durante i trattati di Roma del 1950. Riprendendo il concetto dello *jus solitudinis*, formulato un secolo prima da Louis D. Brandeis e Samuel Warren, l'articolo tutela il diritto al rispetto della vita privata e familiare, concedendo delle deroghe solo in casi eccezionali previsti all'interno di un sistema democratico, volti a garantire la sicurezza e l'ordine pubblico (Rodotà, 2010).

Sempre in ambito del Consiglio d'Europa e della Convenzione europea per la salvaguardia dei diritti dell'uomo (CEDU), esiste una una Corte dei diritti dell'uomo con sede a Strasburgo, la quale agisce per assicurare la tutela di diritti fondamentali riconosciuti dall'Unione Europea. Tra questi è riconosciuto anche il diritto alla tutela dei dati personali, sui quali è intervenuta previo ricorsi

giurisdizionali nazionali ordinari mossi dagli Stati membri o da singoli individui. A essa è integrata l'attività della Corte di giustizia dell'Unione Europea, con sede a Strasburgo, la cui opera al fine di applicare il diritto dell'Unione in modo eguale in tutti i Paesi membri. Il suo intervento ha avuto particolare importanza nella regolamentazione della data retention e in particolare nella definizione del diritto all'oblio e nella stipulazione del Safe Harbour (Pizzetti, 2016).

Più tardi nel 1981, il Comitato dei ministri del Consiglio d'Europa approvò a Strasburgo una serie di raccomandazioni sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, entrati in vigore in Italia nel 1989 come "Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale". La Convenzione 108/1981 rappresenta un punto di riferimento importante nell'ordinamento europeo, in quanto contiene una serie di concetti e principi che furono ripresi anche negli interventi successivi. La normativa fu scritta ispirandosi ai principi fondamentali dell'Unione Europea, relativi al rispetto della vita privata e della libera circolazione dell'informazione tra i popoli. La regolamentazione fu fatta con l'obiettivo di proteggere le informazioni appartenenti a una persona fisica identificata o identificabile, che potesse essere oggetto di qualsiasi tipo elaborazione automatizzata. Con essa, venne istituito il diritto a un trattamento lecito e corretto dei dati personali, per cui il responsabile del casellario automatizzato sarebbe dovuto intervenire nel caso di richieste da parte dell'interessato, relative alla modifica o alla cancellazione delle informazioni possedute. La norma stabiliva inoltre che dati sensibili indicanti l'origine razziale, le opinioni politiche, le convinzioni religiose, lo stato di salute, la vita sessuale e le condanne penali non potevano essere elaborati automaticamente, salvo garanzie specifiche adatte al contesto. Ogni responsabile del casellario automatizzato doveva in ogni caso garantire la sicurezza delle informazioni conservate ed elaborate, evitando che queste potessero essere distrutte, perse o rese accessibili a terzi non autorizzati. Il testo prevedeva delle eccezioni nel caso di interessi di ricerca scientifica o statistica, sicurezza pubblica, interessi monetari dello Stato e per necessità di repressione di reati o protezione della libertà altrui. Infine, la Convenzione adottava a pieno una visione europea dell'ordinamento, ribadendo un'applicazione

della normativa oltre le frontiere nazionali e introducendo la presenza di un comitato consultivo a supporto dell'applicazione e del miglioramento della convenzione.

L'ordinamento europeo in tema di data retention, ha subito una continua evoluzione negli ultimi vent'anni, che è ancora oggi non si è del tutto stabilizzata, al fine di adattarsi al processo evolutivo delle tecnologie digitali. Prima di maggio 2018, in cui è entrato in vigore il nuovo Regolamento europeo in materia di protezione dei dati personali (GDPR), le principali fonti dell'ordinamento europeo sulla protezioni dei dati erano costituite da:

- la Direttiva 95/46/CE "relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati", attuata in Italia come legge 31 dicembre 1996, n. 675;
- il Trattato di Lisbona comprensivo della Carta dei diritti dell'Unione, entrato in vigore come Parte I del trattato consolidato il 1° dicembre 2009;
- la Direttiva 2002/58/CE "relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche", attuata in Italia come legge 31 luglio 2002, n. 201;
- la Direttiva 2009/136/CE recante modifica della Direttiva 2002/22/CE "relativa al servizio universale e ai diritti degli utenti in materia di reti e servizi di comunicazione elettronica" e del Regolamento CE n. 2006/2004 sulla "cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori", recepita in Italia come legge del 15 dicembre 2011, n. 217.

Le fonti appena citate, sono state realizzate dai diversi legislatori seguendo sempre i riferimenti presenti nella Carta dei diritti dell'Unione, nella quale sono presenti i principi fondamentali dell'intero sistema normativo europeo (Pizzetti, 2016).

Fino a maggio del 2018, i principali riferimenti giuridici in materia di protezione dei dati personali erano rappresentati essenzialmente dalle direttive 95/46/CE e 2002/58, relative rispettivamente al trattamento dei dati personali e alla loro gestione all'interno del settore delle telecomunicazioni. La direttiva 95/46/CE è stata quella che in generale ha più influito sull'attuale quadro normativo, definendo un primo metodo di approccio alla materia e identificando i ruoli e le

responsabilità di fornitori e gestori di dati. Nel corso di un ventennio, tale direttiva è rimasta alla base del sistema normativo in materia di trattamento dei dati, nonostante sia stata adattata diverse volte dal legislatore europeo, a seconda delle innovazioni tecnologiche introdotte nel settore del digitale.

La direttiva 95/46/CE è stata realizzata allo scopo di definire un sistema giuridico in tema di tutela di dati personali, con l'obiettivo di garantire la protezione della vita privata dei propri cittadini. La normativa è stata fatta per stabilire delle norme comuni a tutti i Paesi membri dell'Unione, evitando che venissero realizzati dei regolamenti nazionali incongrui, intralcianti le aziende attive in tutto il territorio europeo. Nonostante la direttiva 95/46/CE rappresenti una delle prime normative in tema di trattamento di dati nella rete, la norma riprende gran parte dei principi individuati dalla Convenzione 108/81.

Il testo della direttiva fu organizzato in 34 articoli suddivisi in 6 capi, nei quali oltre a definire alcuni concetti del contesto trattato, si regolavano le modalità con cui dovevano svolgersi le attività legate alla raccolta e al trattamento dei dati. Le principali nozioni definite nell'art. 2 della direttiva, erano quelle di: "dato personale", inteso come l'insieme di informazioni relative a una persona fisica identificata o identificabile; "trattamento dei dati personali" relativo all'insieme di operazioni compiute con o senza l'ausilio di processi automatizzati applicati a dati personali come la raccolta, la registrazione, la conservazione, l'elaborazione o modifica dei dati personali e infine "archivio di dati personali", riferito a qualsiasi insieme strutturato di dati accessibili, secondo determinati criteri. Nell'articolo si individuavano inoltre alcuni ruoli chiave del trattamento dati, tra cui quelli del responsabile, dell'incaricato e del destinatario, intesi come i rispettivi gestori delle finalità, dei processi e delle comunicazioni delle elaborazioni.

Nel testo oltre a ribadire il concetto fondamentale di consenso della persona interessata, inteso come qualsiasi manifestazione di volontà libera, specifica e informata, si definivano anche le condizioni di liceità del trattamento. Quest'ultime in particolare stabilivano le modalità di esecuzione del trattamento, il contenuto minimo dell'informativa destinata all'interessato, le differenze tra tipologie dei dati, i sistemi di controllo garantite agli utenti e le deroghe di legge.

La direttiva dettava inoltre, i cannoni di riferimento con cui poteva essere concesso il trasferimento dei dati al di fuori del territorio europeo, affidando alla Commissione il ruolo di controllore degli standard giuridici, presenti nei Paesi al di fuori del territorio comunitario. Infine, la direttiva 95/46 stabiliva la necessaria presenza anche di un'autorità nazionale garante della privacy, la quale avrebbe dovuto fare da supervisore alla corretta applicazione della norma a livello locale. Tale organo è tuttora presente in ogni Stato membro dell'Unione, e opera insieme alla Commissione Europea allo scopo di vigilare sul corretto rispetto delle normative stabilite in materia di trattamento di dati personali (Pizzetti, 2016).

Nel corso di un ventennio l'Unione Europea ha deciso di introdurre nuovi regolamenti per adattare la direttiva 95/46/CE alle innovazioni tecnologiche introdotte nel mercato e per ridurre l'eccessivo carico di responsabilità che la stessa attribuiva agli utenti nella gestione dei loro dati personali, tramite il solo principio consensuale. Durante i primi anni del Duemila, l'aumento esponenziale del traffico di dati dovuto alla diffusione di internet, determinò la realizzazione di una direttiva specifica relativa al trattamento dei dati personali e al rispetto della vita privata all'interno settore delle comunicazioni elettroniche. La direttiva 2002/58 fu realizzata con lo scopo di abrogare una precedente norma fatta cinque anni prima dall'Unione europea, per regolare il settore delle di telecomunicazioni (Direttiva 97/66/CE), adattando i principi stabiliti dalla direttiva 95/46/CE alle tecnologie presenti allora. La legge infatti definiva le modalità con cui poteva essere realizzato un trattamento dei dati, riprendendo i concetti definiti dal quadro normativo sulla privacy e trattando singolarmente l'uso degli strumenti utili per lo svolgimento delle attività di data retention e data mining (Poullet, 2006).

Dopo una prima puntualizzazione di alcuni concetti come quello di utente, comunicazione, consenso e dati relativi al traffico e all'ubicazione, la direttiva 2002/58 metteva in primo piano le norme riguardanti la sicurezza e la riservatezza. Secondo quanto indicato dal testo, i fornitori di servizi di comunicazione elettronica dovevano assicurare delle appropriate misure tecniche e organizzative per salvaguardare la sicurezza dei prodotti offerti al pubblico, adattandole alla tipologia e al grado di rischio esistente. La legge inoltre, obbligava ogni Stato membro alla realizzazione di leggi nazionali atte a garantire la

riservatezza delle comunicazioni effettuate tramite la rete pubblica o servizi di comunicazione elettronica accessibili al pubblico, con relativi dati sul traffico. La direttiva inoltre vietava tutte le forme di intercettazione e sorveglianza come l'ascolto, la captazione e la memorizzazione di comunicazioni e di dati sul traffico, svolte senza il consenso degli utenti interessati. Allo stesso modo vietava l'uso di software spia, web bugs usati per scopi illegittimi e all'oscuro dell'utente, permettendo invece l'impiego di cookies per scopi commerciali. Infine la norma ribadiva il principio consensuale dando la possibilità agli utenti di conoscere e gestire i propri dati personali relativi alle linee chiamate, all'ubicazione e al traffico, trattati e memorizzati dal fornitore della rete pubblica o dal servizio di comunicazione elettronica.

La direttiva 2002/58/CE venne integrata nel 2006 con la direttiva 2006/24/CE relativa alla "conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione", e nel 2009 con la direttiva 2009/136/CE, la quale modificava anche la direttiva 2002/22/CE relativa al "servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica" e il regolamento (CE) n. 2006/2004 sulla "cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori". Infine nel 2014 venne definitivamente dichiarata invalida dalla Corte di giustizia dell'Unione Europea, dopo le richieste di valutazione fatte dalla High Court irlandese e dalla Verfassungsgerichtshof austriaca, alla luce di provvedimenti nazionali riguardanti la conservazione dei dati relativi le comunicazioni elettroniche e dopo i ricorsi fatti dalla Kärtner Landesregierung in materia costituzionale. La Corte nonostante riconoscesse il ruolo fondamentale della legge nella tutela dei dati personali, dichiarò invalida la direttiva individuando una serie di carenze, tra cui: l'assenza di una necessaria differenziazione del trattamento dei dati volto supportare la lotta contro i reati più gravi; l'assenza di un criterio oggettivo che consentisse alle autorità nazionali componenti l'accesso ai dati, utile per la prevenzione, l'accertamento e il perseguimento di reati penali; l'assenza di differenziazioni nella durata di conservazione dei dati e più in generale, una complessiva mancanza di

garanzie, capaci di assicurare una protezione efficace dei dati contro possibili abusi, accessi e usi illeciti (Corte di Giustizia Europea, 2014).
Ciò nonostante dal 2014 al 2018, l'Unione Europea ha continuato a tutelare i dati personali, usati nel corso di trattamenti automatizzati e non, grazie alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale del 1981 e alla direttiva 95/46/CE. Gli stessi principi delle norme finora citate, furono ribaditi anche nel 2009, durante la stipulazione del Trattato di Lisbona comprensivo della Carta dei diritti dell'Unione. In quest'ultimo caso vennero ripresi i principi di tutela e di libera circolazione dei dati, entro i controlli posti dalle autorità comunitarie e nazionali. Infine, a maggio 2018, con l'entrata in vigore del nuovo regolamento n. 2016/679, l'interno quadro normativo europeo in materia di di protezione dei dati ha subito l'ultimo e definitivo cambiamento, realizzato nel rispetto degli stessi principi definiti dalle leggi precedenti.

2.1.3
Regolamento generale sulla protezione dei dati personali: GDPR

Dopo i vari interventi correttivi e integrativi della direttiva 95/46/CE e 2002/58/CE, la Commissione Europea ha deciso di regolare il quadro normativo in materia di tutela dei dati personali, presentando il "Pacchetto europeo protezione dati", costituito dal regolamento 2016/679 e dalla direttiva 2016/680, entrati in vigore a maggio 2018. Il nuovo regolamento europeo sulla protezione dati, definito anche GDPR (General Data Protection Regulation) è stato realizzato con l'obiettivo garantire a tutti i cittadini europei un trattamento uniforme dei dati personali, ponendo fine alle disparità di tutela causate dalle diverse normative nazionali. Per questa ragione il regolamento è entrato in vigore senza che vi fosse alcun atto di recepimento da parte degli Stati membri, mentre sono stati fatti passare due anni dalla data di approvazione a quella di entrata in vigore, al fine di consentire a tutte le organizzazioni interessate l'adeguamento alla normativa.

Il regolamento UE 2016/679 è stato realizzato secondo una diversa impostazione rispetto al precedente ordinamento sulle attività di raccolta e trattamento dati. La norma infatti, pone al centro dell'attenzione il diritto alla tutela dei dati personali, elevandolo a diritto fondamentale, dunque inviolabile, entro il quale devono essere adottate tutte le misure necessarie perché non avvenga alcuna fuga, perdita o uso improprio da parte di terzi. Per far si che ciò avvenisse, il legislatore ha fatto leva sui maggiori principi presenti in materia di privacy, considerando i singoli bisogni delle aziende che svolgono delle attività di data retention e data mining e le evoluzioni future degli strumenti impiegati a questi scopi (De Stefani, 2018).

L'intero regolamento gravita attorno al principio consensuale dell'interessato, al quale si è cercato di garantire anche la massima consapevolezza dei trattamenti a cui è sottoposto, obbligando il titolare alla trasparenza di quanto fatto. Secondo quanto espresso dalla normativa, il principio consensuale può effettivamente tutelare i diritti degli utenti, quando è libero, informato, inequivocabile, specifico, verificabile e revocabile. Per questo motivo, il titolare del trattamento deve fornire una nota informativa rispetto a quanto svolto, allo scopo di rendere trasparente qualsiasi attività di data retention e data mining da lui realizzata. Il codice non specifica in modo dettagliato il contenuto di tale comunicazione, tuttavia ne definisce alcuni elementi minimi tra cui i contatti del titolare, del responsabile, le finalità del trattamento e la forma concisa, trasparente e intelligibile che deve avere (Matarrese, Notarangelo, 2017).

Le caratteristiche del principio consensuale e della nota informativa poste dal legislatore tutelano già di per sè alcuni diritti riconosciuti all'interessato. Il primo citato dal regolamento è costituito dal diritto alla trasparenza, nel quale si garantisce al soggetto le facoltà di conoscere e comprendere le finalità del trattamento, di monitorare i propri dati ed eventualmente di intervenire per poterli modificare. A estensione del concetto di trasparenza, all'interessato sono riconosciuti anche i diritti di informazione in merito alle dinamiche del trattamento, di accesso alle informazioni conservate dal titolare e di rettifica nel caso di dati inesatti o incompleti. Il legislatore ha considerato anche le modalità con cui il soggetto può imporre la fine del trattamento, riconoscendo il diritto alla limitazione o all'opposizione del trattamento; alla portabilità dei dati da un titolare

ad un altro e all'oblio, ossia alla cancellazione di delle informazioni non necessarie o al quale si oppone o revoca il consenso al trattamento. Tali principi sono stati definiti dal regolamento in virtù di consentire all'interessato un pieno controllo sui propri dati personali, realizzando al contempo una protezione integrale del dato personale, al di là della tipologia delle informazioni raccolte e degli strumenti con cui si svolge il trattamento. La definizione dei diritti dell'interessato ha infatti reso flessibile le occasioni di applicabilità della norma, a prescindere dalle condizioni in cui avviene il trattamento dei dati (De Stefani, 2018).

Il regolamento fornisce anche delle direttive chiare e precise sulla data governance dei dati aziendali, intesa come l'insieme delle procedure che mirano ad allineare le operazioni di data management alle strategie aziendali. Alla base di tali regole vige il principio di accountability, ossia il senso di responsabilizzazione che sta alla base dell'intero pacchetto normativo. I soggetti maggiormente coinvolti nelle attività di data management all'interno delle aziende sono il titolare del trattamento, ossia colui che determina finalità e mezzi del trattamento e il responsabile, inteso come l'organismo che esegue la raccolta e l'elaborazione dei dati per conto del titolare. Il titolare non deve solo mettere in atto tutte le misure tecniche e organizzative conformi al regolamento, ma ha anche l'obbligo di dimostrare l'adeguatezza di quanto svolto in base alla natura, al contesto e alle finalità del trattamento. Per far si che l'uso dei dati sia conforme alla legge, il titolare ha l'obbligo di formare il responsabile e i dipendenti nominati da quest'ultimo, autorizzati al trattamento. Entrambi dovranno poi redigere dei registri delle attività, nei quali documentare quanto svolto, dimostrando il loro impegno nel rispettare la direttiva. Il regolamento indica solo il contenuto minimo che il registro del titolare e quello del responsabile devono avere, allo scopo fornire più possibilità di dimostrare quanto svolto, considerando la varietà di trattamenti potenzialmente realizzabili e dunque la soggettività delle misure adottabili (De Stefani, 2018).

Una delle più importanti novità apportate dal regolamento è l'introduzione del Data Protection Officer, ossia una figura professionale operante ai vertici dell'organizzazione come supervisore dell'effettivo rispetto degli standard di legge. Oltre ad avere il compito di garantire la sicurezza informatica aziendale, il DPO è stato creato con lo scopo di essere un punto di riferimento per tutti gli stakeholder

dell'organizzazione. Il titolare o il responsabile dell'azienda infatti, possono interpellarlo per avere delle delucidazioni sulle giuste misure da adottare per la sicurezza dei dati oppure per ottenere una valutazione complessiva su quanto svolto. D'altro canto lo stesso DPO deve poter agire in modo indipendente dall'azienda, allo scopo di essere un mediatore per gli interessati coinvolti nei trattamenti e per il Garante nazionale della privacy, soprattutto nel caso in cui dovessero verificarsi delle problematiche nella gestione delle informazioni. Infine, nonostante il regolamento preveda che sia il titolare del trattamento a tenere un registro delle attività, nella realtà questo compito sarà affidato al DPO, sulla base delle informazioni fornite dagli organi dell'intera azienda. La nomina del DPO spetta al titolare ed è obbligatoria quando il trattamento è svolto da un'autorità pubblica o quando consiste in un monitoraggio regolare e sistematico degli interessati o quando coinvolge categorie particolari di dati. Questo può essere un dipendente oppure un soggetto esterno all'organizzazione, operante tramite un contratto di servizio (Scafati, Perelli, 2016).

Infine il regolamento tratta anche delle modalità di gestione di eventuali casi di data breach che potrebbero verificarsi nel corso del trattamento dei dati. Per data breach s'intende qualsiasi violazione della sicurezza dei dati personali, che comporti l'accidentale o illecita perdita, distruzione, divulgazione o modifica delle informazioni registrate dal titolare. La norma europea obbliga quest'ultimo a fornire un'informativa su quanto accaduto sia all'autorità Garante che agli interessati del trattamento coinvolti nella violazione dei dati personali. Nel testo si sottolinea l'importanza della tempestività e della completezza che deve avere la notifica alle autorità, indicando come termine massimo di comunicazione alle autorità 72 ore, entro le quali il DPO deve fornire una descrizione completa sulla natura, le circostanze e le conseguenze di quanto accaduto. Ulteriori informazioni riguardo gli estremi del titolare e del responsabile devono essere fornite anche agli interessati, soprattutto nel caso in cui la violazione coinvolga dati personali sensibili, per cui sussista un grave rischio per la loro persona fisica. Tale intervento obbliga le organizzazioni a essere trasparenti anche sui malfunzionamenti del trattamento e successivamente le spinge a procedere per la completa risoluzione

del danno e l'adozione di nuove misure volte al controllo e alla riduzione di qualsiasi rischio di data breach (De Stefani, 2018).
Nel complesso il regolamento 2016/679 vuole riaffermare il principio consensuale già considerato dalle direttive europee precedenti, ma a differenza di quest'ultime, considera i limiti conoscitivi e interpretativi dell'utente medio. Per questa ragione l'Unione Europea ha imposto alle organizzazioni attive nel trattamento dati una comunicazione più trasparente verso gli interessati e l'obbligo di adottare dei sistemi di tutela e vigilanza più efficaci. Per questa ragione ha ribadito la necessità di un linguaggio semplice nella nota informativa destinata ai soggetti coinvolti nel trattamento dei dati, allo scopo di consentire loro una gestione consapevole delle informazioni. Allo stesso modo, è intervenuta sulle regole di data governance aziendale al fine di permettere alle organizzazioni la massima libertà di azione, alla quale deve sempre fare capo la dimostrazione del rispetto del regolamento su quanto realizzato (De Stefani, 2018).

2.1.4
Quadro normativo nazionale

Le prime leggi a tutela della privacy online sono entrate in vigore in Italia grazie all'ordinamento giuridico realizzato dall'Unione Europea per la definizione e la protezione dei dati personali. La prima legge nazionale in materia fu infatti la n. 675 del 31 dicembre 1996, la quale venne realizzata con lo scopo di attuare nel territorio nazionale la direttiva comunitaria 95/46/CE. La normativa permise di affermare anche in Italia di alcuni elementi chiave per la regolamentazione del settore, tra cui i ruoli del titolare e del responsabile, l'obbligo di trasparenza e i meccanismi di affermazione del diritto consensuale per l'approvazione di quanto svolto. La legge istituì inoltre il Garante per la protezione dei dati personali che rappresenta ancora a oggi, un'autorità amministrativa indipendente volta a controllare, promuovere e curare l'applicazione delle normative nazionali ed europee in materia di trattamento dei dati personali. Il Garante opera infatti in

modo autonomo, valutando possibili casi di trattamento illecito, rilasciando le autorizzazioni necessarie per il trattamento dei dati e facendo valere i diritti dell'interessato nel caso non vi siano altre autorità giudiziarie competenti (Gorla, Ponti, 2018).

Nel 2003 la legge 675/96 fu abrogata a favore del Decreto legislativo n. 196 del 30 giugno 2003. Il codice in materia di protezione dei dati fu il primo vero intervento giuridico realizzato a livello nazionale in materia di privacy. La legge fu realizzata in forma di testo unico, volto a raccogliere e razionalizzare tutte le norme europee per la tutela dei dati allora in vigore in Italia. In questo modo fu possibile conservare i concetti espressi dall'ordinamento precedente, mantenendo la linea espressa dall'Unione Europea. Nella prima parte del testo ad esempio, furono ripresi alcuni concetti basici tra cui quelli di trattamento, dato personale, dati sensibili, titolare, responsabile, interessato e violazione, già definiti dalla direttiva europea 95/46/CE e ripresi anche nell'attuale regolamento generale sulla protezione dei dati.

La normativa proponeva di tutelare la riservatezza delle informazioni appartenenti all'interessato, riconoscendo il diritto alla protezione dei dati personali come diritto fondamentale. La logica del testo si basava sulla necessità di far conoscere all'interessato quanto svolto dal titolare, il quale era tenuto a rendere accessibili i dati personali coinvolti dal trattamento e semplificare gli eventuali interventi richiesti dal soggetto. Secondo quanto previsto dal testo infatti, l'interessato aveva il diritto di conoscere la possibile presenza di dati personali all'interno dei trattamenti svolti dal titolare. In caso di conferma, il titolare doveva comunicare all'interessato le origini dei dati che lo riguardavano, le finalità e la logica del trattamento e gli estremi suoi e del responsabile. L'interessato d'altro canto, doveva avere la possibilità di poter intervenire per aggiornare, modificare, eliminare i dati che lo riguardavano. Il trattamento dei dati era consentito solo previo consenso del soggetto, allo scopo di permettere a ogni individuo di poter decidere liberamente sull'esposizione delle proprie informazioni personali. Il principio consensuale permetteva inoltre di far consentire all'intero o a parte del trattamento, tramite una conferma esplicita in forma scritta. Il titolare inoltre, quale responsabile della raccolta dei dati, era tenuto al risarcimento dei danni cagionati nel corso del

trattamento, ai sensi dell'articolo 2050 del codice civile, sulla responsabilità per l'esercizio di attività pericolose.

La legge inoltre stabiliva il dovere del titolare di predisporre di sistemi di tutela adeguati, volti a ridurre i rischi di accesso e uso illegittimo, fuga, perdita o distruzione dei dati raccolti. Per garantire una maggiore efficacia dei principi di protezione, la normativa affermava la necessaria adozione di misure di protezione diverse, adeguate alle varie caratteristiche dei dati raccolti. La legge riconosceva infatti l'esistenza di dati sensibili particolarmente riservati, relativi alle convinzioni religiose, filosofiche, politiche e alle condizioni di salute o di lavoro dell'individuo. In questo caso il decreto legislativo prevedeva oltre al consenso scritto dell'interessato, anche l'ottenimento di un'autorizzazione, rilasciata dal Garante per la realizzazione del trattamento. Riguardo a quest'ultimo aspetto, la legge definiva in modo dettagliato le disposizioni sul trattamento dei dati nei rapporti tra dipendente e datore di lavoro, anche nel caso di rapporti lavorativi potenziali, specificando le modalità di utilizzo delle informazioni durante la fase di raccolta e valutazione dei curricula vitae.

Nel 2010, il governo intervenne sul d. lgs. 196/03 attraverso la legge n. 120 del 29 luglio 2010 relativamente ai contrassegni su veicoli a servizio di persone invalide e con la legge n. 183 del 4 novembre 2010 riguardante le Deleghe al Governo in materia di lavori usuranti, di riorganizzazione di enti, di congedi, aspettative e permessi, di ammortizzatori sociali, di servizi per l'impiego, di incentivi all'occupazione, di apprendistato, di occupazione femminile, nonché alle misure contro il lavoro sommerso e alle disposizioni in tema di lavoro pubblico e di controversie di lavoro.

Oltre al codice in materia di protezione dei dati personali del 2003, in Italia si discusse a lungo sulla necessità di creare una Carta dei diritti internet, volta a regolare il fenomeno della rete nella sua dimensione globale. La prima proposta venne avanzata nel 2005 in occasione dell'approvazione del Codice di Amministrazione digitale (D.Lgs 82/2005) e del summit internazionale ONU di Tunisi, volto allo sviluppo dell'uso delle information and communication technologies. Nel 2006, l'Italia presentò all'Internet Governance Forum di Atene, la

propria proposta per una Costituzione del mondo digitale, con cui ottenne anche un riconoscimento dall'ONU, due anni dopo la sua realizzazione.

Nel 2014 il governo brasiliano di Dilma Rousseff, dopo un lungo dibattito durato cinque anni, approvò la prima Carta costituzionale per la rete internet la rete, detta Marco Civil. Il testo, strutturato in cinque capitoli e trentadue articoli, mirava ad affermare quattro diritti fondamentali, quali la libertà di espressione, la definizione della personalità, la tutela della privacy e la salvaguardia dei dati personali. L'iniziativa del Brasile rappresentò uno stimolo significativo per l'Italia che decise così continuare nella realizzazione del progetto iniziale, seguendo quanto fatto dal governo brasiliano (Mederois, Bygrave, 2015). Nello stesso anno, venne dunque stabilita una Commissione di studio composta da 13 esperti e 10 deputati, con lo scopo di realizzare anche in Italia un codice costituzionale interamente volto a regolare la rete internet, in ogni suo aspetto. A ottobre venne presentata la prima bozza della "Dichiarazione dei diritti in Internet", che fu poi successivamente visionata anche dai ventotto Stati membri dell'Unione Europea, in occasione del semestre di presidenza italiana, nel corso del summit riguardante i diritti fondamentali. Da allora il testo venne messo a disposizione di tutti i cittadini, italiani e comunitari, al fine di essere un possibile spunto per una possibile e futura Costituzione europea dei diritti internet (Mensi, Falletta, 2015).

L'approccio adottato dalla Commissione si basava sul principio di corresponsabilità nel governo della rete, detto anche "Multistakeholder". Per questo motivo l'elaborazione del documento ebbe una consultazione pubblica, durata cinque mesi nella quale si chiese l'intervento attivo della cittadinanza, a favore di nuove proposte. Il testo composto da quattordici articoli riconosceva: il diritto di accesso; il diritto alla conoscenza e all'educazione in rete; la neutralità della rete; la tutela dei dati personali; il diritto all'autodeterminazione informativa; il diritto all'inviolabilità dei sistemi, dei dispositivi e domicili informatici; i trattamenti automatizzati; il diritto all'identità; la protezione dell'anonimato; il diritto all'oblio; i diritti e le garanzie delle persone sulle piattaforme; la sicurezza in rete e il governo della rete. Venne inoltre introdotta la definizione di cittadinanza digitale, quale appartenenza dell'individuo a uno spazio digitale definito e inclusivo, esistente a prescindere dai confini geografici nazionali (Masera, Scorza, 2016).

Ciò nonostante a oggi la "Dichiarazione dei diritti in Internet" non costituisce né una legge né una regolamentazione vincolante. La Commissione parlamentare volle infatti bilanciare la necessità di affermare alcuni diritti fondamentali, con quella di evitare di eccedere in una regolamentazione eccessivamente restrittiva, che rischiasse di limitare l'evoluzione digitale. La "Dichiarazione dei diritti in Internet" costituì comunque un'intervento decisivo per l'affermazione di alcuni concetti espressi anche dalla dichiarazione dei diritti fondamentali dell'ONU e dell'Unione Europea come il diritto a esprimere la propria libertà di opinione, il diritto alla partecipazione e quello dell'associazione. In questo modo si cercò di riaffermare alcuni dei principi base del diritto anche nel mondo digitale, allo scopo di rendere il web uno spazio aperto a tutti (Masera, Scorza, 2016).
Dal 25 maggio 2018, in Italia come come nel resto degli altri Stati membri dell'Unione Europea, è entrato in vigore il nuovo regolamento per la protezione dei dati personale (GDPR), che non ha del tutto abrogato il precedente Codice della privacy, ma ha comunque apportato delle innovazioni in materia. Il regolamento è entrato a far parte dell'ordinamento italiano senza alcun intervento da parte del governo, in quanto la Commissione europea ha optato per una formula immediata, volta a favorire l'uniformità della tutela (De Stefani, 2018).

2.1.5
Statuti di autoregolamentazione privata

Finora l'ordinamento internazionale per la regolamentazione dei diritti online, è stato costituito principalmente da normative di "soft law", realizzate allo scopo di generare una maggiore consapevolezza sulla dimensione digitale. L'assenza di un'effettiva regolamentazione della rete, condivisa su scala globale, è frutto del fallimento di vari tentativi promossi per stabilire delle norme comuni, tra cui quello di alcuni rappresentati delle Camera statunitense che nel 2013 proposero un "Global Online Freedom Act". Il mondo economico finora ha dimostrato un forte interesse nell'armonizzazione del diritto di uso e gestione dei dati della rete, mosso

soprattutto dalla necessità di stabilire delle linee strategiche globali. Lo stesso Google ha cercato già in passato di promuovere la costituzione di un'istituzione pubblica mondiale a garante della tutela dei diritti online, proponendo un "Global Privacy Counsel" presso l'ONU (Rodotà, 2014).

Benché non esista ancora un sistema legislativo stabile valido a coprire tutte le attività presenti in rete a livello mondiale, gli operatori di settore stanno cercando di rispettare una linea di trasparenza comune, a fronte applicare dei principi di tutela equi verso tutti gli utenti. Google, Facebook, Amazon e altre aziende di settore hanno così sviluppato un proprio codice di condotta, che rappresenta l'assunzione di un impegno verso l'ambiente sociale in cui operano. Tale attività è infatti considerabile come parte della strategia di Corporate Social Responsibility (CSR), in quanto consiste nella promessa di rispetto di una condotta etica, nei confronti degli stakeholder aziendali e di tutti i soggetti potenzialmente coinvolti, che va al di là dei doveri imposti dalla legge (McWilliams, Siegel, 2001).

Secondo gli studi fatti, esistono due motivi per la realizzazione di strategie di Corporate Social Responsibility: un senso del dovere di buona cittadinanza e di correttezza verso l'ambiente esterno (Donaldson, 1982) oppure l'attuazione di attività di marketing strategico, volte a migliorare l'immagine pubblica (Schwepker, Good, 2011). La tutela dei dati online rappresenta il rispetto dell'identità degli utenti che ogni giorno si devono interfacciare con gli strumenti messi a disposizione da aziende come Google, Facebook e Yahoo. Per questa ragione, la realizzazione di un codice etico consente alle aziende di migliorare il proprio profilo reputazionale, in una prospettiva di lungo termine. Costruire una solida immagine nell'ambiente di business permette alle imprese di stabilire delle relazioni di fiducia con i propri stakeholder, anche nel caso di operazioni che coinvolgono capitale di rischio (Bondy, Matten, Moon, 2004).

Nel 2018, il tema delle informazioni scambiate online è stato ripreso più volte dalla cronaca internazionale sia per quanto riguarda la gestione delle fake news che per la protezione dei dati personali. Le elezioni statunitensi e il caso Facebook e Cambridge Analytica sono state le principali cause di questo dibattito, che tuttavia rappresenta l'effetto delle continue innovazioni digitali per l'integrazione del web in tutte le azioni quotidiane. Quello che è emerso nell'ultimo anno, è la continua

necessità che hanno le aziende di dichiarare i loro principi nel trattamento dei dati, dimostrando in primo luogo, di essere trasparenti sui dati raccolti online e usati per fini commerciali. La tutela dei dati personali, riguarda infatti uno dei diritti fondamentali riconosciuto per legge, di cui le anche aziende sono sempre più chiamate a prendere una posizione etica a riguardo. Oltre all'adozione di sofisticate misure di sicurezza come ad esempio il sistema di blockchain, le aziende saranno sempre più chiamate a ribadire quanto svolto, mediamente la pubblicazione di codici etici, l'invio di notifiche per il consenso e la comunicazione di note informative relative al corretto trattamento dei dati (Fjord Trends, 2018).

Il caso di una possibile violazione illecita di dati, contestuale alla presenza di un codice etico interno, rappresenterebbe un comportamento non coerente che rischierebbe di compromettere l'immagine aziendale, svelando le vere intenzioni delle azioni di filantropia strategica. Le azioni di Corporate Social Responsibility devono dunque essere supportate da una comunicazione costante e dinamica che sia coerente con i valori e le attività svolte. Quando ciò non sussiste, l'azienda rischia di compromettere gli obiettivi di vendita futuri, in quanto i consumatori avvertendo la condotta ipocrita dell'impresa, potrebbero decidere di boicottare l'intera offerta aziendale (Shim, Chung, Kim, 2017).

Nei codici di etici dei grandi big del web come Google, Yahoo e Facebook è sempre presente una sezione dedicata alla questione della privacy e della data retention, basata sulla dichiarazione di impegno al rispetto della tutela e della riservatezza dei dati personali appartenenti ai propri utenti, al di là del sistema legislativo a cui sono sottoposti. Ciò nonostante, il recente datagate di Facebook e Cambridge Analytica, ha dimostrato come possano verificarsi delle accidentali o illecite fughe, pubblicazioni, perdite o distruzioni di dati, conservati da grandi aziende attive nella data retention e data mining online. Finora, tali eventi non hanno ancora inciso nella crescita economica di queste piattaforme del web, che hanno continuato a diffondersi e ad esser utilizzate al di là dei rischi presenti nella rete. Ciò nonostante non è detto che un'escalation di data breach possa irrimediabilmente danneggiare l'immagine aziendale di uno o più gestori di questi siti, compromettendone dunque il successo economico e finanziario (Rosen, 2012).

2.2
Autorità competenti in materia di trattamento dei dati

A oggi la regolamentazione dei dati trattati online rappresenta una sfida decisiva, sia per il settore pubblico che per quello privato. I grandi players internazionali, quali Google e Facebook sono costantemente impegnati nel ribadire i loro principi in materia di trattamento dei dati, dando la possibilità ai propri utenti di accedere ai propri dati e talvolta invitandoli anche a verificare quanto registrato all'interno della piattaforma. L'impatto che hanno queste aziende nella rete internet internazionale è infatti particolarmente rilevante, considerando il volume di dati che devono gestire ogni giorno in tutto il mondo. Ciò nonostante, nel corso di un ventennio di sviluppo della rete, sono state sviluppate delle autorità internazionali e nazionali di monitoraggio della rete, volte a garantire l'applicazione degli ordinamenti vigenti e dunque evitare qualsiasi abuso illecito di dati personali.

Una delle prime autorità internazionali a essersi occupata della gestione dei dati personali scambiati online è stata la Internet Telecommunication Union. Nata nel 1947 come agenzia delle Nazioni Unite per la gestione della rete telegrafica, fu incaricata negli anni Novanta della gestione dei primi siti apparsi nella rete online. Nel 1998, l'area dell'agenzia dedicata al monitoraggio della rete venne scorporata con la creazione dell'Internet Corporation for Assigned Names e Numbers, dedicata interamente all'assegnazione degli indirizzi (Internet Protocol) e alla gestione dei domini di primo livello. L'organizzazione venne realizzata sotto forma di ente non profit, volto a salvaguardare la stabilità operativa di internet e promuovere la competizione di mercato, basando il suo operato sul principio di autoregolamentazione della rete. Più tardi anche l'ONU interviene nel monitoraggio dei flussi di informazioni online, organizzando nel 2006 il primo Internet Governance Forum, un convegno multilaterale volto alla creazione di un dibattito internazionale per il corretto sviluppo di internet (Masera, Scorza, 2016).

La creazione di organi pubblici di controllo e diffusione della rete internet ha avuto uno sviluppo parallelo anche in organizzazioni politiche minori, tra cui l'Unione Europea. Nel 1995, il Parlamento europeo e il Consiglio dell'Unione Europea hanno

infatti deciso di regolamentare il flusso dei dati personali online, con la realizzazione della Direttiva 95/46 sulla "tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati". La direttiva, oltre ad stabilire le modalità di trattamento dei dati appartenenti ai cittadini comunitari, prevedeva anche l'istituzione di nuovi enti pubblici, dedicati alla sorveglianza e alla tutela delle informazioni scambiate online. Venne così fondato il Gruppo di lavoro articolo 29, ossia un organismo indipendente a cui furono assegnate le funzioni di vigilanza in merito all'applicazione dell'ordinamento europeo, promozione della tutela dei dati e consulenza alla Commissione e al Parlamento Europeo.

Nel 2018 con l'entrata in vigore del nuovo regolamento generale sulla protezione dei dati, il Gruppo di lavoro articolo 29 è stato sostituito con il Consiglio europeo per la protezione dei dati (EDBP), composto dai rappresentanti delle autorità nazionali per la protezione dei dati e dal Garante europeo della protezione dei dati. A oggi il comitato ha il ruolo di vigilare sull'applicazione della nuova normativa europea per la tutela della privacy, definendo con la pubblicazione di linee guida, le modalità di raccolta, utilizzo, conservazione e trasferimento delle informazioni raccolte. L'ente deve inoltre promuovere la corretta gestione dei dati, attraverso la cooperazione con altri Paesi e lo sviluppo di corsi di formazione inerenti alla materia. La Commissione può inoltre servirsene per chiedere consulenza sulle modalità di applicazione del regolamento e sui criteri di trattamento e trasferimento dei dati.

La direttiva 95/46 permise inoltre la creazione di nuove autorità nazionali in tutto il territorio dell'Unione Europea. Venne così fondato il Garante per la protezione dei dati personali, un'istituzione presente in ogni Stato membro incaricata di sorvegliare sull'applicazione dell'ordinamento vigente, al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche. L'ente oltre a promuovere la creazione di sistemi di sensibilizzazione e di rispetto dell'ordinamento europeo ha il dovere di raccogliere ed esaminare i reclami sui possibili casi di abusi di dati, decidendo di adottare o meno provvedimenti volti a bloccare o vietare tutto o parte dei trattamenti analizzati (Gorla, Ponti, 2018).

Ciò nonostante, la presenza di autorità garanti la tutela dei dati personali non sostituisce il potere legislativo della Commissione Europea e dei governi nazionali in materia di privacy. Per questa ragione non tutti gli Stati hanno deciso di istituire delle autorità simili, ma piuttosto hanno lasciato la regolamentazione della rete al normale corso della giustizia, trattando la protezione dei dati online come il resto delle materie giuridiche. In Cina e negli Stati Uniti ad esempio, le leggi sul trattamento dei dati sono realizzate rispettivamente dall'Assemblea Popolare Nazionale e dal Congresso, mentre la loro applicazione è vigilata in entrambi i casi dalle autorità nazionali per il commercio. Il loro intervento è comunque fondamentale per la regolamentazione delle reti internazionali, tanto che in molti casi, le decisioni sulla regolamentazione dei flussi di dati internazionali sono realizzati, solo dopo un lungo dibattito tra questi stessi enti. Tale fenomeno fu particolarmente evidente nel 2016, quando il progetto normativo cinese sulla cyber security fu tema di dibattito anche con la Camera di Commercio USA locale, che cercò di evidenziare fin da subito i limiti del piano di sviluppo, a favore invece della continua diffusione di piattaforme statunitensi in Oriente (Mozur, 2016).

2.3
Carenze di sistema e prospettive future

Nell'analisi *"How ethical are businessmen?"* condotta da Baumhart nel 1961, cinque degli otto problemi etici riscontrati da un campione di managers intervistati riguardavano la comunicazione commerciale, gli studi di mercato e le fasi di vendita. La questione del comportamento morale delle attività di marketing venne poi ripresa anche in uno studio del 1984 condotto da Hunt, Chonko e Wilcox in cui vennero coinvolti circa duecento operatori di settore, iscritti all'American Marketing Association. Nell'occasione vennero somministrati oltre mille questionari al fine di comprendere quale fosse la questione etica che più metteva in difficoltà gli operatori. Gran parte degli intervistati individuò nell'analisi della domanda e negli studi sui consumatori delle significative attitudini a una condotta

amorale dell'azienda. L'integrità nelle ricerche di mercato costituisce l'insieme di principi, valori etici, doveri deontologici e standard professionali su cui si fonda una condotta responsabile e corretta da parte di chi finanzia, svolge o valuta la ricerca scientifica nonché da parte delle istituzioni che la promuovono e la realizzano. I risultati evidenziarono come uno dei conflitti etici più sentiti dagli operatori fosse il bilanciamento tra gli interessi aziendali e il rispetto della privacy delle persone contattate durante le ricerche di mercato, al di là del fatto che queste fossero state realizzate internamente oppure fossero state commissionate ad agenzie specializzate (Hunt, Chonko, Wilcox, 1984).

Le tecnologie online adottate dalle aziende nella raccolta di dati dagli utenti hanno fortemente rivoluzionato le attività di analisi della domanda, con delle implicazioni anche dal punto di vista etico. L'adozione di cookies, RFIDs, spam e altri software di data mining ha ridotto lo spazio concesso dalle aziende alla privacy dei consumatori. D'altro canto la maggioranza gli utenti della rete non ha provato un senso di privazione dei propri dati, accettando l'attività ricerca a fini commerciali. Molti hanno acconsentito allo scambio di dati personali al fine di ottenere delle gratificazioni immediate come l'utilizzo di nuovi strumenti digitali, un tipo di comunicazione personalizzata, la customizzazione dell'offerta e ulteriori promozioni commerciali (Laczniak, Murphy, 2006).

Con l'avvento delle tecnologie digitali online, il volume di dati raccolti e gestiti dalle imprese è radicalmente incrementato. Gli operatori di mercato possono così velocemente capire i bisogni dei propri interlocutori dando loro il prodotto giusto, al momento giusto e al prezzo preferito. Gli investimenti fatti dalle grandi aziende nel campo della comunicazione online insieme all'applicazione di sistemi produttivi flessibili hanno moltiplicato le occasioni di contatto tra aziende e domanda, dando il via anche a iniziative di co-progettazione dei prodotti e aumentando la soddisfazione dei clienti (Lee, Chang, 2011).

Le imprese online possono migliorare il loro rapporto con i propri clienti attraverso la comunicazione online, incrementando il livello di coinvolgimento della domanda e moltiplicando le vendite attraverso l'e-commerce. Alla base di un rapporto di fiducia tra utenti e aziende è necessario che le stesse offrano preventivamente delle garanzie sul trattamento dei dati personali online, al fine di

evitare possibili abusi o fughe di informazioni sensibili (Higgins, 1997). La presenza di codici di condotta spesso non basta a evitare possibili abusi da parte delle imprese attive nella data retention come da quanto dimostrato da varie denunce lanciate da parte di utenti di Facebook e Google che si sono visti illecitamente sottrarre dei dati personali (Rosen, 2012). Tuttavia l'impegno dimostrato dalle imprese nella tutela del trattamento delle informazioni personali raccolte online è stato ricompensato da un coinvolgimento significativo e da una maggiore brand loyalty della domanda. Non a caso, è stato riscontrato che le piattaforme online in cui è possibile scegliere alcuni termini di privacy ottengono feedback positivi dagli utenti che si sentono più fiduciosi e incentivati a interagire nella comunicazione e nell'acquisto online. Al contrario chi già in passato ha subito personalmente delle violazioni di privacy è meno propenso all'utilizzo del web e alla condivisione di propri dati personali con terzi (Mosteller, Poddar, 2017).

Nonostante la presenza di una moltitudine di autoregolamentazioni private fatte dalle grandi aziende del digital come i codici di condotta Google o Facebook, gli Stati hanno il dovere di essere i primi a garantire il rispetto dei diritti fondamentali online. La carta dei principi dei diritti Facebook per quanto possa ricordare una carta costituzionale scritta da un governo democraticamente eletto, è frutto di un lavoro fatto da uomini di marketing e legali assunti dall'impresa, il cui scopo è assicurare l'ottenimento di utili ai propri soci. Le autorità nazionali hanno l'obbligo di mantenere il loro ruolo per la tutela dei diritti delle persone in quanto cittadini, prima che come consumatori di un servizio digitale (Masera, Scorza, 2016).

Nell'era di internet dovrebbe delinearsi un nuovo quadro costituzionale che consenta un'adeguata regolamentazione della rete. La presenza di questioni come la necessità di rendere neutrale la rete oppure il riconoscimento di alcuni diritti come la libertà di parola, d'informazione e di accesso alla rete, riflettono i limiti dell'autoregolamentazione privata, gravando invece sul significato attribuito ai principi di soft law. La dichiarazione dei diritti fondamentali ONU è uno dei pochi sistemi legislativi accettati e condivisi a livello internazionale, valido anche a tutela dei diritti fondamentali, contestualizzati all'interno delle attività che si svolgono in rete. Tuttavia un crescente attivismo da parte degli operatori economici coinvolti in questo settore e la considerazione del cambiamento socio-economico apportato da

internet sta mobilitando le organizzazioni governative nella definizione di termini di utilizzo e di gestione dei dati online migliori, che possano affermarsi in modo definitivo anche su scala mondiale (Rodotà, 2010).

In questo senso l'Unione Europea sta creando uno dei sistemi modello per la gestione dei dati mondiali, limitando le facoltà delle piattaforme online, responsabilizzando l'utente e individuando le occasioni di intervento delle autorità garanti pubbliche. Il nuovo regolamento europeo sulla protezione dati (GDPR) ha ribadito il principio consensuale con cui ogni utente è chiamato a scegliere le modalità di trattamento dei propri dati personali, ma allo stesso tempo ha introdotto delle norme più severe per chi opera attivamente nella data retention. Nelle piattaforme infatti, devono essere chiarite le modalità e le finalità di raccolta e trattamento dati, attraverso una comunicazione semplificata, che prevede anche l'uso di immagini e video esplicativi. Allo stesso modo devono essere descritti i termini di utilizzo e cancellazione dei dati raccolti nel rispetto del diritto di oblio (Guida all'applicazione del Regolamento Europeo, 2018).

Il diritto sul trattamento dei dati online in Europa soffre del principio di territorialità nel contesto globale in cui sono strutturati i collegamenti della rete. In questo senso gli Stati Uniti ad esempio, sono una delle mete principali delle informazioni raccolte dai cittadini europei, ed elaborate dai Big del digital come Google, Facebook e Amazon. A riguardo, la dichiarazione d'invalidità del Safe Harbor nel 2016, ha lasciato un'importante lacuna normativa a tutela di tale legame, spingendo il governo statunitense e l'Unione Europa a creare un accordo sostitutivo che potesse sostituire il precedente e incrementare le tutele a favore della privacy dei cittadini europei. Tuttavia a due anni dalla fine del Safe Harbor, il nuovo regolamento detto Privacy Shield è ancora in fase di trattativa tra le due istituzioni, a causa del dovere della Commissione europea di assicurare lo stesso livello di protezione dei dati europei nel territorio statunitense. Non è escluso che le trattative per definire l'accordo possano prolungarsi a lungo, tuttavia il Privacy Shield potrebbe esser la base per la creazione di intese simili future anche verso Paesi dell'Oriente, in cui stanno crescendo grandi piattaforme dell'online, diffuse anche in Occidente (Tracol, 2016).

Finora lo scambio internazionale di dati in internet è stato regolamentato dall'Unione Europea mediante la direttiva 95/46/CE, in cui venivano definiti i parametri necessari per il trasferimento all'estero d'informazioni appartenenti a cittadini comunitari. L'articolo 26 dello stesso regolamento permetteva tale operazione previo il giudizio della Commissione sul livello di protezione garantito dalla legislazione presente nel Paese destinatario delle informazioni. Altre eccezioni erano previste invece nel caso di consenso espresso dal singolo utente interessato oppure nel caso di Binding Corporate rules per operazioni svolte all'interno di gruppi societari.

Gli sforzi fatti finora per l'armonizzazione del diritto internet, sono ancora definibili in diversi spazi circoscritti incapaci di coprire la dimensione globale dei collegamenti online. Una tale lacuna normativa rischia di mettere a rischio alcuni diritti fondamentali esercitabili dagli utenti e allo stesso tempo apre a tutte le organizzazioni governative una nuova materia di confronto per lo sviluppo di una normativa comune. In questo senso l'ONU rappresenta l'unica organizzazione che finora potrebbe potenzialmente prendersi carico di tale questione, promuovendo un tipo di collaborazione comune tra enti pubblici e grandi aziende del settore, al fine di definire dei principi condivisi per la navigazione nel web (Soro, 2016).

Capitolo 3
Il privacy paradox

3.1
Definizione di privacy paradox

Il Semantic Web consiste in un'evoluzione del più conosciuto World Wide Web, che permette di classificare e decodificare i dati presenti online, creando quella rete di informazioni più comunemente chiamata "data web". Il suo sviluppo ha reso più fruibile la conoscenza delle informazioni presenti in internet, permettendo una gestione in larghissima scala di dati provenienti da tutto il mondo. Le attività online di milioni di utenti sono diventate così facilmente registrabili e salvabili, incrementando le possibilità di data retention e data mining da parte di grandi organizzazioni come aziende e istituzioni. Il mobile e altre innovazioni tecnologiche hanno poi accelerato tale processo, consentendo una raccolta continua e giornaliera di dati provenienti da ogni smartphone. La raccolta di informazioni personali da parte di terzi ha messo in evidenza la questione della tutela della privacy e dell'importanza al rispetto dell'individualità della sfera personale (Smith, Kollars, 2015).

In meno di vent'anni dall'introduzione di queste tecnologie, si è sviluppato uno dei più grandi business mondiali, basato sulla raccolta e la gestione di dati provenienti dalle attività di navigazione, registrate ogni giorno in internet. A oggi gli effetti del mercato dei dati online sull'economia internazionale è particolarmente rilevante: si stima infatti che solo in Europa nel 2020 il valore del mercato della data retention raggiungerà i 740 miliardi di euro, pari a circa il 4% del suo PIL. La valutazione inoltre, potrebbe essere anche inferiore alla realtà, considerando che a oggi il tasso di crescita del settore è del 15%, mentre non accenna a diminuire il numero di

imprese interessate allo studio di mercato tramite la raccolta e l'analisi dei dati registrati dalla rete (Tremolada, 2017).

La privacy è diventata una delle più grandi questioni del millennio, considerata come uno dei punti cruciali in tema di uso e gestione della rete internet. Diversi Paesi hanno iniziato da anni a realizzare una legislazione volta a garantire il massimo grado di tutela dei dati degli utenti. L'obiettivo di questi Stati è la definizione dei diritti fondamentali riconoscibili ai cittadini che utilizzano la rete, ai quali dev'essere garantita la possibilità di fare delle scelte consapevoli nel corso della gestione dei propri dati personali, anche quando sono sottoposti ad attività di data retention da parte di terzi.

Gran parte degli utenti del web è a conoscenza dei pericoli che corrono affidando le proprie informazioni personali alla rete. Tuttavia fin dai primi anni del Semantic Web è stata riscontrata una sorta d'indifferenza ai rischi dati dalla data retention che nel tempo è stata definita come Privacy paradox (Brown, 2001). Da diversi studi empirici è stato infatti dimostrato come gli individui non siano in grado di tutelare le proprie informazioni personali nella dimensione digitale, a causa di una diffusa incapacità di dare un valore ai dati personali caricati online. La condivisione di dati infatti avviene in modo volontario e gratuito, allo scopo di soddisfare delle esigenze personali (Carrascal, Riederer, Erramilli, Cherubini, De Oliveira 2013).

Il privacy paradox tuttavia, non si spiega con la sola scarsa attenzione che i consumatori hanno verso i propri dati personali, ma riguarda un insieme più ampio di cause, che comprendono fattori psicologici e sociali. Ciò è stato riconosciuto come un vero e proprio comportamento assunto dagli utenti online, che non percepiscono le dimensioni del rischio corso, anche quando la loro sicurezza informatica è evidentemente compromessa (Acquisti, 2004). Gli individui inoltre, non hanno alcun incentivo per cercare degli strumenti con cui assicurare la propria cybersecurity, esponendo così le proprie informazioni personali a un rischio continuo. A oggi nonostante sia stata riscontrata una diffusa volontà di limitare la diffusione dei propri dati personali online, gli utenti della rete non sono ancora in grado di sviluppare dei comportamenti di controllo, capaci di garantire una protezione di quanto effettivamente divulgato (Barth, Jong, 2017). Oltre alla cybersecurity, vi è infatti una distorsione percettiva nell'identificazione dei

destinatari delle comunicazioni online, in quanto la diffusione di dati personali in piattaforme online chiuse, non permette di far intuire quali soggetti avranno effettivamente accesso alle informazioni condivise. Ciò avviene soprattutto nei social network, dove la possibilità di pubblicare dei dati a una cerchia ristretta di utenti, non esclude che altre persone possano venire a conoscenza e utilizzare i contenuti di quanto comunicato (Wilson, Valacich, 2012).

Il privacy paradox è stato riscontrato dopo alcuni studi svolti negli anni duemila, i quali hanno permesso di mettere in discussione l'efficacia del sistema normativo presente allora basato su un presupposto di perfetta razionalità degli individui, intesi come soggetti economici informati sui meccanismi di gestione delle informazioni (Acquisti, 2005). I primi esperimenti fatti negli Stati Uniti in quel periodo, dimostrarono in particolare come gli utenti avessero un atteggiamento sulla loro privacy diverso dal loro comportamento effettivo nel momento della navigazione. È stato infatti riscontrato come in internet vi sia un calo generale del livello di prudenza assunto, a fronte di possibili rischi di abuso o perdita di informazioni personali e sensibili. Diversi studi hanno dimostrato come online, le persone fossero più disposte a barattare le loro informazioni personali per ottenere dei benefit economici. (Acquisti, Grossklags, 2005).

L'argomento è stato analizzato da vari punti di vista, cercando di comprendere sia i fattori psico-sociali coinvolti nelle scelte di utilizzo delle informazioni personali sia le ripercussioni sulla comunicazione tra utenti e aziende. Lo studio del privacy paradox ha reso possibile l'identificazione dei fattori personali determinanti le scelte di condivisione dei dati come le caratteristiche individuali e i limiti logici della persona. Allo stesso tempo è stato possibile definire anche quali elementi ambientali possano determinare il comportamento dell'utente, fra cui il contesto di scelta dell'utente e in particolare il design e il funzionamento del sito. Infine sono state fatte delle valutazioni monetarie sulle scelte di utilizzo della privacy, quantificando con un prezzo il valore delle informazioni attribuito dalle persone a quanto condiviso (Barth, Jong, 2017).

L'accelerazione tecnologica degli ultimi anni ha accresciuto le occasioni in cui è possibile raccogliere dati personali. Il quadro digitale in cui è inserito l'utente medio oggi è talmente complesso da esser stato chiamato "panoptismo elettronico

incontrollato", considerando le azioni di raccolta e gestione dei dati fatto ogni giorno dalle aziende online. Le stesse, insieme alle diverse autorità pubbliche stanno tuttavia cercando di trovare delle soluzioni comuni per gestire in modo equo le informazioni raccolte online dagli utenti, con una visione internazionale di sviluppo comune, che possa tutelare tutti i collegamenti presenti nella rete web (Barth, Jong, 2017).

3.2
Cause del privacy paradox

Il privacy paradox è un fenomeno particolarmente complesso, che ha coinvolto studi di tipo legislativo, economico, sociologico e psicologico. Durante le prime ricerche fatte negli Stati Uniti, gran parte degli utenti coinvolti nei campionamenti riteneva che la tutela della privacy fosse uno degli elementi fondamentali per la navigazione online (Brown, 2001). Nonostante la maggioranza degli individui fosse a conoscenza dei rischi corsi nella condivisione dei propri dati personali online, è stata riscontrata una discrepanza tra le intenzioni degli utenti e le loro decisioni finali al momento della navigazione in rete (Flender, Müller, 2012).
In seguito è stato possibile rilevare come vi fossero delle differenze sostanziali tra le intenzioni di tutela della privacy dichiarate dai partecipanti e il loro comportamento finale. Il fenomeno è stato approfondito cercando di individuare quali fattori influissero sul processo decisionale dell'individuo. Il momento della condivisione dei dati è stato così descritto determinando tre dimensioni fondamentali di scelta: le condizioni personali, l'ambiente circostante e il contesto sociale. I primi a scomporre in questo senso la gestione delle scelte sulla privacy furono Laufer e Wolfe, che già nel 1977 proposero la loro "multidimensional development theory" (MDT) al fine studiare le dinamiche di protezione dei dati personali in una prospettiva futura. La teoria fu poi applicata anche nel caso del privacy paradox al fine di giustificare la reazione dicotomica individuata dagli esperti. Il comportamento degli utenti è il frutto un'analisi immediata di bilancio

tra pro e contro, che ogni individuo compie ogni qual volta si trova nella situazione di decidere se condividere o meno le proprie informazioni personali online. Il calcolo fatto dagli individui può essere infatti rappresentato con una funzione di utilità in cui si sottrae il valore di rischi di condivisione delle informazioni a quello dei benefici percepiti dallo scambio di dati (Li, Luo, Zhang, Xu, 2016).

Il primo fattore considerato nell'analisi di Laufer e Wolfe riguarda la dimensione personale, ovvero il carattere e il comportamento del singolo individuo nell'uso della rete considerato, escludendo possibili condizionamenti esterni. Nella nostra società il concetto di individualità è fortemente attribuito a quello di autonomia personale e alla concezione di dignità umana. Secondo gli autori dello studio, ogni singolo individuo ha una concezione personale della protezione della propria privacy, che va al di là del contesto ambientale e sociale in cui vive. La tutela dei propri dati personali si lega infatti alla concezione di sviluppo personale, in cui si riflette infine il comportamento di condivisione ed espressione. Esistono quindi vari livelli di percezione della privacy, che nel web si manifestano attraverso le strategie soggettive di gestione delle informazioni, sia nel caso di mera navigazione online che nelle occasioni di condivisione di dati propri, presenti all'interno dei social network, oppure all'interno delle piattaforme di e-commerce (Li, Luo, Zhang, Xu, 2016).

Un secondo fattore fondamentale nel processo di scelta è quello ambientale inteso come lo spazio fisico e dimensionale. Nel caso di internet lo spazio è inteso come la pagina web con cui si deve relazionare l'utente. La dimensione ambientale è stata definita da Laufer e Wolfe come l'insieme di elementi che influenzano l'abilità di percepire, gestire e scegliere le opzioni possibili. Il sito internet costituisce tutti questi elementi, in particolare attraverso il design, i contenuti e il funzionamento stesso delle varie sezioni (Li, Luo, Zhang, Xu, 2016). Nell'e-commerce questa dimensione è fondamentale in quanto è stato riscontrato come le prime impressioni di un sito internet siano la parte decisiva per l'acquisto finale dell'utente. Lo stile e il funzionamento di una pagina forniscono gli elementi necessari alla valutazione dell'esperienza di shopping online (Ethier, Hadaya, Talbot, Cadieux, 2004). Secondo la teoria MDT, le situazioni di scelta sulla privacy sono caratterizzate da una mancanza di conoscenza del contesto. Nel caso di siti

web sconosciuti, la persona è costretta a prendere delle decisioni secondo la sua esperienza passata e gli elementi più palesi forniti dalla pagina. Il design è un fattore che può fornire poche direttive in termini di privacy, ma allo stesso tempo è capace di dare delle emozioni all'utente, tra cui un senso di rassicurazione verso il sito. Per questo motivo, l'aspetto e il funzionamento di una piattaforma di e-commerce è fondamentale nella scelta d'acquisto online, a causa del senso di sicurezza trasmesso ai nuovi utenti. L'aspetto emozionale dell'e-commerce influenza l'intera esperienza d'acquisto, tanto che gli individui maturano un proprio giudizio sulla piattaforma di vendita in soli pochi minuti di navigazione. Allo stesso modo, il senso di rassicurazione dato da una pagina web influisce sulla predisposizione nella condivisione di informazioni personali che il singolo è disposto a comunicare online (Éthier, P. Hadaya, J. Talbot, J. Cadieux, 2006). In sintesi, l'aspetto ambientale è costituito da una valutazione olistica del sito, in cui la comprensione cognitiva del suo funzionamento è affiancata all'esperienza emozionale che questo offre, tramite design e contenuti (Li, Luo, Zhang, Xu, 2016).

Il terzo fattore considerato da Laufer e Wolfe riguarda la dimensione interpersonale della scelta. È stato riscontrato infatti, come la questione della privacy cambi notevolmente a seconda del tipo di rapporto che c'è tra il venditore e il compratore. Gli utenti della rete, come gli acquirenti, tendono a perdere il loro senso di controllo delle proprie informazioni quando il loro coinvolgimento emotivo verso la piattaforma online è più forte. Ciò si rifà anche nel caso di shopping online, per cui il livello di protezione della privacy può essere diverso a seconda del caso in cui nel sito sia possibile o meno interagire con il venditore o meno. Analogamente agli acquisti, l'utente è più disponibile a fornire i propri dati personali quando si riduce il livello di incertezza nell'utilizzo del sito internet e quando è possibile stabilire una sorta di rapporto di reciprocità, che rende la pagina web più familiare (Li, Luo, Zhang, Xu, 2016).

La ricerca di Laufer e Wolfe si focalizzava sull'analisi dei fattori determinanti le scelte quotidiane di gestione della privacy, a seconda della disponibilità di condividere le proprie informazioni con terzi. Tali indagini erano orientate alla conoscenza dei comportamenti abituali assunti dai cittadini nella vita reale, senza alcun riferimento specifico alla navigazione online. Tuttavia gli stessi concetti

rilevati dai ricercatori sono poi risultati coerenti con le modalità di gestione delle informazioni nell'utilizzo di internet.

Nel complesso la rete ha facilitato i processi d'interazione tra imprese e consumatori e in particolare gli aspetti di codificazione, raccolta gestione dei dati, consentendo anche un baratto tra informazioni personali e offerte promozionali. Online poi, il rapporto tra aziende e utenti include sia un coinvolgimento razionale, basato su un senso di equità dello scambio tra parti, che una parte emotiva data dalla fiducia posta dall'individuo nella transazione. Il primo aspetto è solitamente costituito dalle informazioni date dagli utenti alle organizzazioni, al fine di ottenere l'accesso a piattaforme gratuite, promozioni o altri servizi offerti online dalle aziende. La parte emotiva invece, coinvolge l'attività stessa di navigazione in rete, da cui l'utente può ricavarne un'esperienza positiva, capace di rafforzare il grado di fidelizzazione verso un brand gestore di una piattaforma o al contrario, una negativa, che invece rischia di compromettere l'intero rapporto con il cliente interessato. Gli atteggiamenti di gestione delle informazioni in rete, rispondono infatti a percezioni superficiali, legate all'aspetto e al funzionamento del sito oppure alla conoscenza diretta o indiretta che ne hanno gli utenti. Gli stessi infatti tendono ad agire sotto l'influsso delle percezioni suscitate dal contesto in cui operano, il quale limitava la loro capacità di valutazione (Mosteller, Poddar, 2017).

3.2.1
Bias cognitivi individuali

Il nuovo regolamento europeo sulla protezione dati (GDPR) obbliga i responsabili incaricati del trattamento a fornire di una nota informativa tutti verso coloro che sono sottoposti alla raccolta di dati personali. La normativa prevede che la descrizione data all'utente sull'uso delle informazioni sia concisa, trasparente, intellegibile e accessibile al fine di permettere la responsabilizzazione degli interessati, chiamati a esprimere il loro consenso nelle modalità e negli scopi di data retention. I fondamenti di liceità previsti da tale direttiva coincidono in linea

di massima con quelli precedentemente in vigore, previsti d.lgs. 196/2003 ovvero previo: consenso, adempimento a obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri e interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati. Ancora una volta quindi, il sistema giuridico basa la liceità del trattamento sul principio consensuale espresso dagli utenti a favore dei titolare responsabili delle piattaforme online. Da questo punto di vista il legislatore presuppone la capacità dell'interessato di comprendere e scegliere le modalità di utilizzo dei propri dati personali, in base alle informazioni espresse nella nota informativa (Guida all'applicazione del Regolamento Europeo, 2018).

In molti casi è stato dimostrato come gli utenti siano consapevoli dell'importanza della gestione dei propri dati personali online. Chi si approccia alla rete intende controllare le proprie informazioni personali, considerando il valore che queste hanno nel mercato dei dati. A riguardo molti utenti infatti, sono disposti a barattare parte della propria privacy per ottenere delle offerte commerciali vantaggiose. Tuttavia in contrasto ad un comportamento apparentemente logico e consapevole, la dimostrazione del privacy paradox pone la questione su quanto sia realmente efficace il principio di consensuale per il trattamento dei dati. Uno dei primi elementi a spiegazione del fenomeno è costituito dal limite analitico con cui gli utenti si approcciano alla navigazione online, nella quale spesso non sono in grado di confrontare oggettivamente il valore delle proprie informazioni contro quello offerto dalle piattaforme (Barth, Jong, 2017).

Già negli anni Ottanta Herbert A. Simon aveva dimostrato le limitazioni della razionalità umana attraverso la "Theory Bounded Rationality", individuando tre distorsioni nelle capacità valutative dell'individuo relativamente alla definizione dell'utilità delle varie opzioni, al calcolo dei costi per la raccolta delle informazioni e alle fasi del processo decisionale. Il processo decisionale costituisce una stima approssimativa delle opzioni presenti e nell'individuazione di quella che più è appagante per il decisore (Simon, 1982).

La descrizione del processo decisionale per la tutela della privacy parte dalle caratteristiche psicologiche dell'utente stesso. Ogni individuo infatti ha una propria concezione di fiducia verso le piattaforme digitali e di condivisione di dati propri.

Ciò significa che l'esperienza è fondamentale nel determinare ogni processo decisionale, a prescindere delle condizioni ambientali. Questa premessa, costituita dal senso di soggettività con cui vengono fatte le scelte sulla privacy, rappresenta uno dei fattori più importanti da considerare nello studio comportamentale della gestione dei dati personali (Barth, Jong, 2017).

Per quanto l'utente valuti i vantaggi e gli svantaggi della condivisione di dati online, il processo decisionale è condizionato da bias cognitivi dettati dalla sfera emozionale. Le principali limitazioni nel ragionamento complessivo riguardano la stima delle opzioni disponibili, l'incapacità di predire con certezza le conseguenze future, il desiderio di ottenere delle gratificazioni immediate e i condizionamenti contestuali relativamente ai motivi di utilizzo della rete, ai tempi disponibili e alle percezioni dell'ambiente provate dall'utente (Novak, Hoffman, 2008).

L'insieme dei bias cognitivi risulta essere determinante nella valutazione dei rischi e dei benefici dati dall'utilizzo della piattaforma. Nella condivisione di dati sensibili online, l'utente espone la propria identità digitale a terzi che potrebbero non rispettare le norme di tutela della privacy previste per legge. Tuttavia in gran parte dei casi la persona è disposta a correre tale rischio allo scopo di accedere agli strumenti offerti dalla rete. I servizi disponibili online indirizzano l'individuo a focalizzarsi prevalentemente sui benefit immediati piuttosto che a riflettere sulle conseguenze di una propria esposizione (Wilson, Valacich, 2012).

Infine, anche l'ambiente esterno condiziona il comportamento di tutela della privacy e in particolare le decisioni finali assunte dall'utente. Il contesto sociale inteso come l'insieme di consuetudini presenti in un certo ambiente di riferimento, costituisce uno dei fattori di scelta sull'utilizzo delle proprie informazioni online (Barth, Jong, 2017). Uno degli esempi più evidenti corrisponde all'utilizzo dei social network, in cui bias cognitivo sulla privacy è accentuato dalle impostazioni di visibilità e di accesso al profilo, che accrescono la percezione di controllo data all'utente sulla gestione dei propri dati. A tal ragione le persone si sentono più coinvolte nell'utilizzo di tali piattaforme, rivelando molte più informazioni di quanto non farebbero in altri siti internet, in particolare quando la navigazione avviene tramite un dispositivo mobile (Pentina, Zhang, Bata, Chen, 2016). Il tipo di device usato dalla persona influisce sul comportamento effettivo nelle modalità di

tutela della propria privacy. Questo in quanto l'utilizzo dei dispositivi mobile è caratterizzato da un ritmo particolarmente accelerato che riduce il grado di concentrazione mantenuto dall'utente anche nel momento in cui deve scegliere la destinazione delle proprie informazioni personali (Barth, Jong, 2017).
Per queste ragioni dunque, non è possibile affermare che nel corso della navigazione in internet, l'utente sia pienamente consapevole e coerente della propria attività di gestione dei dati personali. La scelta infatti oltre a costituire una razionale ma veloce comparazione dei pro e dei contro delle varie opzioni possibili, è composta appunto da una serie di fattori meno logici, costituiti dal contesto in cui opera l'utente, come l'ambiente, gli strumenti che ha disposizione e l'aspetto complessivo del sito. Quest'ultimi fattori inducono a una continua svalutazione dei rischi corsi nell'esposizione di informazioni proprie online, mettendo a rischio l'efficacia del principio consensuale, su cui si basa l'attuale sistema normativo a riguardo (Mosteller, Poddar, 2017).

3.2.2
Costo delle informazioni

Online le aziende possono ottenere delle informazioni sulle preferenze della domanda in tempo reale attraverso la raccolta e l'elaborazione dei dati provenienti delle attività svolte dagli utenti nei motori di ricerca, nei siti internet e nei social network. I gestori delle piattaforme usufruiscono di vari tipi di software di analisi in cui avviene una costante elaborazione del comportamento degli utenti collegati. Le imprese possono scegliere se sviluppare in proprio una raccolta delle informazioni oppure affidarsi ad agenzie esterne, specializzate nella gestione delle pagine online e nel data mining. L'elaborazione e lo scambio dei dati provenienti dalla rete rappresenta un vero e proprio mercato, che solo in Europa nel ha coinvolto oltre duecentocinquantamila aziende e più di sei milioni di lavoratori. I dati caricati online dagli utenti, sono l'oggetto di scambio di questo commercio a cui è possibile attribuire un valore economico. Il valore dei dati raccolti in Europa

nel 2016 è stato quantificato in circa trecento miliardi di euro, al quale è stata fatta un'ulteriore e incoraggiante previsione di crescita per il 2020, quando il mercato raggiungerà la quota di settecentotrenta miliardi (Final results european data market measuring the size and trends of the EU data economy, 2017).

Gli utenti che navigano nelle piattaforme online sono i primi fornitori delle informazioni raccolte ed elaborate dalle agenzie di data mining, che ne forniscono dei report riassuntivi alle aziende interessate a conoscere l'andamento del proprio settore di riferimento. Talvolta sono le imprese stesse a sviluppare dei sistemi propri di registrazione e interpretazione dei dati presenti in internet, all'interno dei propri siti aziendali oppure anche nelle piattaforme di social network. La conoscenza tratta dallo studio di tali informazioni rappresenta un valore economico per l'offerta di mercato di cui però, chi utilizza la rete non ne ottiene un ritorno. Gli utenti consapevoli di questo sistema, sono comunque disposti ad accettare di scambiare le proprie informazioni, allo scopo di ottenere dei servizi che spesso sono offerti gratuitamente (Kokolakis, 2015).

La decisione di condivisione dei dati personali consiste in una comparazione tra il valore dato dagli utenti alle informazioni richieste dalla piattaforma web e la sua stessa utilità. In molti studi è stato riscontrato come in effetti la maggioranza delle persone sottovaluti il prezzo dei propri dati rispetto a quanto effettivamente valutato dalle stesse aziende che li elaborano e li rivendono a terzi. L'incapacità di dare un valore economico alle informazioni personali tra cui anche quelle sensibili, costituisce un punto di debolezza per chi naviga nella rete, dimostrando come vi sia una diffusa sottovalutazione dei rischi provenienti da una tale esposizione (Huberman, Adar, Fine, 2005).

Le prime ricerche per approfondire il gap tra il prezzo di domanda e quello di offerta dei dati personali scambiati online sono risalenti al 2005. In questi casi le ricerche erano focalizzate su un determinato tipo di dato, considerando che gli individui solitamente differenziano la condivisione delle proprie informazioni a seconda della rilevanza sociale che queste possono avere. Un primo esempio infatti fu lo studio di condotto da Huberman, Adar e Fine sulla valutazione economica data dagli utenti ai dati relativi al proprio peso e alla propria età. L'esperimento dimostrò come gli utenti coinvolti tendessero a differenziare il valore delle proprie

informazioni a seconda dell'imbarazzo che queste suscitavano loro. Venne perciò riscontrato come fosse stato attribuito un valore medio di 57,56 $ per il dato sull'età e di 74,06 $ per quello del peso. Sempre nello stesso anno, fu studiata la disponibilità di condividere le informazioni sulla propria posizione geografica, tramite l'uso di nuove tecnologie. In questo caso il valore medio attribuito dal campione ai dati sulla localizzazione fu di 10 £, ma l'elemento più evidente fu la distribuzione ampia dei dati, giustificata dalle condizioni di utilizzo e dalle abitudini di spostamento degli individui coinvolti nel test. Dalla ricerca si evinse una correlazione positiva tra il numero spostamenti fatti fuori città e una certa disponibilità alla condivisione. Fu poi riscontrato come gli studenti fossero meno propensi a personalizzare le proprie condizioni sulla privacy, proposte a tutela delle loro informazioni personali (Danezis, Lewis, Anderson., 2005).

Più recentemente, nel 2013 uno studio brasiliano ha cercato di quantificare il gap economico tra il valore dato dagli utenti alle proprie informazioni online rispetto a quelle offline. Lo studio rivelò come la maggioranza del campione attribuisse un peso nettamente superiore ai dati anagrafici richiesti in ricerche tradizionali rispetto alle informazioni condivise all'interno delle piattaforme online. Le persone coinvolte valutarono infatti un prezzo medio di sette dollari per la condivisione della propria cronologia di ricerca online e venticinque dollari per la dichiarazione dei propri dati anagrafici in un sondaggio fatto senza l'uso di internet. Ciò dimostrò come gli individui fossero significativamente condizionati dal contesto d'uso delle proprie informazioni (Carrascal, Riederer, Erramilli, Cherubini, De Oliveira 2013).

Il fenomeno indicato dalle ricerche descritte rappresenta la dimostrazione di uno dei bias cognitivi individuati da Simon. La minimizzazione del prezzo fatta verso i propri dati personali è frutto di una fiducia di base verso le piattaforme online, arricchita dall'ottimismo nel controllo delle proprie informazioni, che solitamente gli individui tendono a sopravvalutare. In questo caso il privacy paradox consiste perciò nelle aspettative dei singoli verso i siti internet, in cui si sentono parte di una comunità, prima che utilizzatori di un servizio online. Il processo di decisione fa dunque affidamento all'istinto degli individui che tendono a minimizzare la variabile del data retention proveniente da terzi e massimizzare il valore dato dal contatto con gli altri utenti (Acquisti, Grossklags, 2007).

3.2.3
Gratificazioni immediate

Se i bias cognitivi sono alla base del privacy paradox, uno dei principali problemi dei limiti cognitivi nella valutazione della propria privacy è data dalla focalizzazione che l'utente ha verso le gratificazioni immediate che può ottenere dall'uso della rete (Wilson, Valacich, 2012). In molti casi è stato dimostrato come possa esserci un comportamento atipico da parte delle persone che tendono a scegliere una gratificazione immediata, accettando di subire possibili conseguenze negative nel lungo termine. Ciò si concretizza con la decisione di ottenere nell'immediato una risposta o un piccolo beneficio, piuttosto che attendere la soluzione o la condizione migliore (Laibson, 1997). Tale comportamento che condiziona le scelte di acquisto dei consumatori, ha degli effetti anche nel mondo digitale e nella gestione dei propri dati personali. La possibilità di beneficiare di gratificazioni immediate, modifica l'atteggiamento di condivisione assunto dall'utente relativamente alla gestione delle proprie informazioni online. I riconoscimenti offerti dalle piattaforme online sono uno stimolo per gli utenti alla condivisione di informazioni personali, i quali quasi inconsciamente, mettono così in pericolo la loro stessa privacy (Barth, Jong, 2017).

L'utilizzo della rete è dettato da bisogni conoscitivi, economici e sociali, che combinati insieme definiscono dei modelli comportamentali simili. I primi due fattori corrispondono a un uso strumentale della rete, in cui l'utente cerca ottenere un determinato risultato. I bisogni comunicativi e sociali invece, sono ricollegabili alla libertà di espressione della propria identità e al riconoscimento dell'individuo nella comunità (Tufekci, 2008).

Le gratificazioni individuate nello studio della navigazione online riguardano principalmente il soddisfacimento di desideri economici e sociali (Pötzsch, 2008). Nel primo caso, i benefici dati ai consumatori sono il frutto dell'evoluzione comunicativa con cui le aziende hanno cercato di coinvolgere la propria domanda nelle loro attività commerciali. Diverse aziende hanno incrementato il livello di coinvolgimento dei propri clienti, realizzando delle strategie comunicative online

con cui aumentare la quota di mercato e accrescere la brand loyalty del proprio target di riferimento. La comunicazione personalizzata e l'uso sconti commerciali all'interno di campagne pubblicitarie online hanno così consentito alle imprese di ottenere delle informazioni dettagliate su ciascun cliente, migliorando così la conoscenza del mercato in cui operano (Mosteller, Poddar, 2017). Infine anche le piattaforme di e-commerce hanno rivoluzionato l'esperienza di shopping, offrendo ai consumatori un'ulteriore prospettiva di risparmio e un assortimento maggiore rispetto a quello presente nella distribuzione tradizionale (Pötzsch, 2008).

Tuttavia oltre all'esistenza di benefici economici, internet è uno strumento di comunicazione digitale internazionale in cui sono state sviluppate delle piattaforme di socializzazione. Le comunità sviluppate in questo contesto sono cresciute a tal punto da diventare numericamente superiori alle maggiori comunità riconosciute a livello istituzionale: il numero di utenti iscritti a Facebook ad esempio è superiore rispetto al numero di abitanti della Cina, che a oggi rappresenta lo Stato più popoloso del mondo. Le relazioni personali coltivate nel web comprendono una serie di attività tra cui la comunicazione diretta, la condivisione oppure le collaborazioni professionali. Il comportamento tenuto dagli utenti all'interno di queste piattaforme delinea una personalità digitale costituita da un'attività monitorabile in tempo reale e analizzabile da terzi in un contesto di studio generale del mercato (Pötzsch, 2008).

I social network hanno fornito una moltitudine di servizi agli individui, intesi come membri di una comunità, grazie alle funzioni di comunicazione e condivisione che queste piattaforme offrono. A differenza di altri tipi di siti, i social network coinvolgono la sfera emotiva dei loro iscritti, piuttosto che quella razionale. Chi si appresta a utilizzarli dunque, oltre a esser intenzionato a condividere le proprie informazioni online, vuole anche ottenere un riconoscimento della propria identità, interagendo con gli altri membri. Di conseguenza, il grado di coinvolgimento influisce sugli utenti molto di più della percezione dei rischi provenienti da un'esposizione di dati personali.

Tale affermazione fu confermata nel 2005, tramite uno studio che dimostrava come la cura della propria immagine online, intesa come le informazioni personali visibili agli altri utenti nel profilo social, fosse maggiore di quella destinata alla

tutela della privacy, intesa invece come insieme dei sistemi di sicurezza volti a evitare possibili accessi da parte di terzi, non autorizzati dal proprietario delle informazioni caricate in rete. Questo fenomeno costituisce un fattore di rischio particolarmente grave, soprattutto nel caso in cui sono trattati dati sensibili per i quali l'assenza di adeguate misure di tutela, può mettere in pericolo anche l'incolumità stessa del soggetto a cui appartengono (Tufekci, 2008).

Nelle attività di social networking, la valutazione dei rischi data dalla condivisione dei dati viene sospesa dall'utente, che tende ad assumere così un comportamento diverso rispetto al normale utilizzo degli altri siti internet. Il coinvolgimento emotivo si basa inizialmente sulla volontà di provare delle esperienze digitali nuove a cui segue un istinto al relazionarsi con persone conosciute. Gli utenti sono consapevoli dei rischi dati dall'esposizione dei propri dati online, tuttavia accettano tali pericoli, spesso inconsciamente, per poter aver accesso a un'enorme mole di contenuti d'informazione e intrattenimento appartenenti alla comunità della piattaforma (Barth, Jong 2017). La possibilità di interagire con altri utenti utilizzando questi media, rappresenta una delle principali gratificazioni immediate offerte dai social network, in quanto sono uno strumento di costruzione e mantenimento di rapporti umani, nonostante ciò avvenga in una realtà virtuale (Debatin, Lovejoy, Horn, Hughes, 2009).

Infine, il mobile ha aumentato le occasioni di utilizzo dei social media, entrando nelle azioni abituali delle persone e incrementando il grado di coinvolgimento e fiducia verso le piattaforme online. Ciò ha permesso una graduale accettazione delle attività di data retention e data mining effettuate dai titolari dei siti all'interno delle piattaforme (Barth, Jong 2017).

3.2.4
Contesto sociale

L'uso di internet e in particolare quello dei social network, è giustificato dal fatto di dover soddisfare dei bisogni di informazione, intrattenimento e socializzazione. La

rete rappresenta infatti un insieme di collegamenti digitali a cui gli utenti sono disposti a cedere delle informazioni personali anche al solo scopo di potervi accedere. Per questo motivo il comportamento di navigazione online e il privacy paradox sono stati analizzati considerando l'influsso del contesto sociale a cui appartiene l'individuo (Debatin, Lovejoy, Horn, Hughes, 2009).

Una prima teoria sociologica a spiegazione del privacy paradox è rappresentata dal modello della "structional theory", sviluppato allo scopo di comprendere i limiti del libero arbitrio all'interno di una struttura sociale. Secondo quanto teorizzato infatti, non esiste una vera è propria indipendenza tra capacità di decisione individuale e contesto sociale. Esistono invece dei fenomeni unici, percepiti in modo diverso dai membri della stessa struttura sociale. In questo modo le azioni delle persone non sono dettate dal libero arbitrio dei soggetti ma sono vincolate dalla struttura sociale in cui sono inserite. Per quanto riguarda il privacy paradox può perciò essere spiegato come parte di un fenomeno sociale. Nel complesso l'uso della rete e la condivisione di informazioni personali online, rappresentano un processo di strutturazione della società, in cui gli individui sono particolarmente influenzati dal contesto esterno nelle loro decisioni di esposizione dei dati.

Il contesto sociale di appartenenza condiziona le scelte di condivisione dei dati in circostanze diverse, legate all'uso del mobile, alla geolocalizzazione tramite RFID e alla gestione dei propri profili social (Zafeiropoulou, Millard, Webber, O'Hara 2013). In quest'ultimo caso, è stato riscontrato come anche chi è particolarmente attento alla propria privacy online, sia disposto a condividere la stessa quantità di informazioni personali di un utente medio, dimostrando quanto il grado di vulnerabilità degli iscritti sia lo stesso per tutti (Acquisti, Grossklags, 2007).

Dal punto di vista sociologico il fenomeno del privacy paradox è stato giustificato anche dalle teorie relative alle regole sociali che gli individui rispettano all'interno di sistemi predefiniti. Internet comprende sia il concetto di Gesellschaft, intesa come società civile basata sul meccanismo razionale del sistema legislativo, sia il concetto di Gemeinschaft, ovvero di comunità in cui gli individui rispondono a legami affettivi (Tönnies, Loomis 2003).

Gran parte delle aziende attive nel mercato della raccolta e della gestione dei dati segue degli ordinamenti civili, conformi a logiche socio-economiche. Al contrario

gli utenti che si approcciano alla rete e in particolare ai social network, percepiscono tali piattaforme come delle comunità di comunicazione e condivisione. Per questa ragione, il loro comportamento riprende le stesse logiche dei legami affettivi, basandosi su emozioni e reazioni istintive. Lo stesso è utilizzato anche nei meccanismi di gestione dei dati personali, in sostituzione ai criteri razionali con cui dovrebbero verificarsi questi processi. Gli utenti online sono perciò più vulnerabili nel controllo della propria privacy, in quanto nonostante siano consapevoli della data retention, tendono a sminuire il valore delle proprie informazioni, paragonandolo a una conversazione tra membri appartenenti a una comunità (Luz, Strathoff, 2014).

Infine, il comportamento di navigazione online e in particolare quello relativo alla condivisione dei dati personali è stato studiato dal punto di vista della rappresentazione dell'individuo nella società. La privacy infatti coinvolge anche l'immagine che la persona si crea mediante il proprio profilo digitale, comunicando quali sono i suoi valori, le sue idee, le sue relazioni e le attività in cui è coinvolto. All'interno di un processo di riconoscimento sociale, il soggetto riesce a inserirsi in un nuovo contesto grazie a quella che è stata definita la teoria della rappresentazione sociale. In questo caso gli individui comprendono i concetti alla base dei meccanismi di funzionamento della struttura sociale a cui si stanno approcciando, grazie a un processo di oggettificazione e ancoraggio di quanto percepito. Ciò significa che i nuovi fenomeni individuati dalla persona sono interpretati attraverso una oggettificazione concreta degli elementi astratti, seguita dall'organizzazione in schemi concettuali e dall'integrazione con le esperienze passate vissute personalmente.

Online, non esiste ancora un sistema sociale e un modello comportamentale di riferimento, per cui gli utenti tendono ad adottare degli atteggiamenti simili a quelli della loro vita reale. In questo modo, ciascun individuo può continuare a coltivare le proprie relazioni sociali e rappresentare la propria identità coerentemente con l'immagine che ha già maturato di sé nella realtà. Allo stesso tempo agisce nella sfera digitale con più sicurezza, sapendo di applicare dei modelli comportamentali già testati nella realtà (Oetzel, Gonja, 2011).

3.3
Personalization-privacy paradox

Lo sviluppo della comunicazione online ha cambiato radicalmente il rapporto tra consumatori finali e aziende. Nell'e-commerce non esiste alcuna interazione faccia a faccia né tra consumatore e distributore e né tra consumatore e produttore. La completa assenza di rapporti di tipo personale, è stata compensata da notevoli sforzi di marketing, fatti al fine di sostituire una tale mancanza. Gli operatori di mercato hanno infatti cercato di coinvolgere la propria domanda di mercato tramite la personalizzazione dell'offerta commerciale, al fine di adattarsi ai limiti dati dalla dimensione digitale del contatto. Per fare questo, molte aziende si sono servite della rete internet, allo scopo di raccogliere e analizzare i dati provenienti dagli stessi utenti al fine di realizzare delle strategie di comunicazione di tipo mirato (Culnan, Armstrong, 1999).

Lo studio degli interessi appartenenti agli utenti della rete è un elemento cruciale per la definizione delle strategie aziendali, e in particolare di quelle indirizzate alla personalizzazione dell'offerta. Tuttavia le imprese che intendono raccogliere online le informazioni sul proprio mercato d'interesse rischiano di collidere contro gli stessi consumatori, i quali tendono a percepire tali ricerche come delle violazioni ingiustificate alla loro privacy. In internet infatti, l'insieme di dati appartenenti a ciascun individuo costituiscono la sua identità digitale. Ogni singola persona percepisce e tutela in modo diverso tali informazioni a seconda del contesto in cui si trova oppure in base al tipo dato trattato. Per questo motivo un utilizzo non autorizzato di queste informazioni da parte di terzi potrebbe esser percepito come un abuso dell'identità digitale della persona e avere anche delle conseguenze nella vita reale (Klobas, Clyde, 2000).

Il rispetto della privacy rappresenta uno degli aspetti più difficili da gestire per le aziende, in quanto il grado di disponibilità ad esporre informazioni personali a terzi costituisce un particolare stato psicologico che da luogo a scelte soggettive (Westin, 1967). Nonostante la comunicazione online sia diffusamente percepita come parte di una perdita della privacy, è stato infatti riscontrato come esista una

relazione negativa tra il valore dato dagli individui alle proprie informazioni e la loro disponibilità alla condivisione di dati (Petronio, 1991). Quest'ultima inoltre, può variare in base al sito con cui l'utente ha a che fare e in particolare a seconda della brand equity percepita dal soggetto e all'uso delle piattaforme web fatto precedentemente (Tezinde, Smith, Murphy, 2002).

Le ricerche realizzate dalle aziende per comprendere i modelli comportamentali della domanda sono state fatte presupponendo un ragionamento utilitaristico tra rischi e benefici offerti. Nonostante la comunicazione personalizzata rappresenti una di quelle gratificazioni percepite dall'utente, la sua importanza non è tale da sopportare il valore dato ai dati personali richiesti dalle aziende. Per questo motivo non basta la sola personalizzazione dell'offerta a giustificare lo sforzo richiesto agli utenti della rete (Awad, Krishnan, 2006).

Per superare le avversioni alla partecipazione alle attività aziendali online, l'offerta deve predisporre dei sistemi di garanzia che rassicurino gli individui sulla gestione delle loro informazioni. Una condivisione consapevole di dati online supportata dalla possibilità di controllare la destinazione e i tempi d'uso delle informazioni, permette di rassicurare gli utenti sottoposti a data retention, riducendo il loro grado di avversione verso le attività di marketing online proposte dalle aziende. Al contrario, non avviene lo stesso nel caso di codici aziendali a dimostrazione di politiche a tutela della privacy. Gli utenti infatti, sono molto più coinvolti nel rapporto con le aziende quando queste danno loro la possibilità di decidere sull'uso dei propri dati in modo chiaro e trasparente con delle richieste esplicite di consenso, piuttosto che con la pubblicazione di codici di condotta etici, realizzati dalle imprese a dimostrazione di una politica di rispetto dei dati (Kirsch, 1996).

Gli utenti che si rapportano con le aziende online si attendono un comportamento di trasparenza. Tale concetto è costituito da quattro facoltà richieste dall'utente: accesso alle informazioni personali condivise con terzi, conoscenza dei termini di utilizzo dei dati, spiegazione delle modalità di identificazione della persona e descrizione delle piattaforme con cui l'azienda intende scambiare quanto raccolto online. Una strategia di comunicazione online che rispetta questo genere di bisogni tende a rassicurare gli utenti della rete. In questo modo le imprese possono ridurre

i rischi percepiti durante la navigazione online, garantendo a ogni individuo la piena libertà di scelta di condivisione dei dati (Awad, Krishnan, 2006).
Nella personalizzazione dell'offerta e della comunicazione in internet, gli ostacoli maggiori che le aziende devono affrontare sono la riduzione del grado di rischio percepito dalla domanda e l'elaborazione dei dati raccolti. Superato il primo ostacolo con una politica di trasparenza sul trattamento dei dati, le strategie di offerta possono indirizzarsi verso una politica di comunicazione mirata, previo uno studio dettagliato delle informazioni raccolte. Gli strumenti digitali hanno facilitato le operazioni di gestione ed elaborazione dei dati provenienti dai propri utenti. Più informazioni il venditore riesce ad ottenere dalla navigazione in rete e più materiale ha a disposizione per elaborare le scelte di acquisto future. Online può così predisporre un'offerta che rispecchi gli interessi individuali, ottenendo un feedback positivo dalla comunicazione con i propri clienti, i quali d'altra parte percepiscono un senso di gratificazione dall'atteggiamento di collaborazione e rispetto assunto dall'azienda (Chellappa, Sin, 2005).
La trasparenza dimostrata dalle aziende nelle operazioni di data retention permette di offrire alla domanda un senso di appagamento dall'utilizzo stesso della piattaforma online. Ciò consente all'azienda di instaurare un rapporto duraturo con i propri clienti, dando loro un senso di gratificazione dalle attività di navigazione all'interno del sito e di gestione delle informazioni condivise. La comunicazione personalizzata online permette così di incrementare l'interesse del mercato per i prodotti proposti nella piattaforma, fidelizzando gradualmente chi ne è già coinvolto, nonostante le difficoltà date dalla distanza fisica tra venditore e compratore (Sutanto, Palme, Tan, Phang, 2013).

3.3.1
Effetti della comunicazione personalizzata

Nella comunicazione aziendale la sincerità è fondamentale nell'approccio con gli utenti della rete, in quanto riduce i possibili timori sui rischi dati dall'esposizione

verso terzi, incrementando la fiducia verso il brand. A questo scopo le piattaforme online devono permettere ai consumatori di conoscere le modalità con cui vengono raccolte le informazioni fornite e chiederne il consenso per il loro utilizzo, allo scopo di costruire un rapporto a distanza in cui il mittente si fida del destinatario. Tali concetti sono alla base della creazione di una strategia di data retention stabile dalla quale l'impresa può ottenere dei vantaggi in termini reddituali (Acquisti, Grossklags, 2005). Internet permette alle aziende di controllare in modi diversi le dimensioni e le preferenze della domanda, agendo poi di conseguenza nelle varie fasi del processo di acquisto del consumatore.

Nella fase di pre-acquisto infatti, le aziende possono scegliere di indirizzare le proprie campagne promozionali direttamente verso dei determinati target di mercato, precedentemente individuati attraverso un'analisi delle caratteristiche personali, dei benefici ricercati oppure del comportamento di acquisto. Tale attività deve essere supportata da una raccolta di dati ampia e approfondita che comprende quelli anagrafici e quelli relativi alle abitudini comportamentali della domanda. Internet quindi, facilita questa fase di studio dei consumatori permettendo alle aziende di accedere gratuitamente a ricerche già esistenti e fornendo degli strumenti con cui valutare in tempo reale il comportamento e le preferenze degli utenti (Blattberg, Deighton, 1991).

Attraverso l'uso di piattaforme digitali le aziende possono quantificare le dimensioni della domanda a cui si rivolgono, individuando le preferenze degli utenti, studiandone lo stile di vita e definendo lo spazio territoriale in cui si muovono. Così facendo la comunicazione commerciale viene indirizzata solo a coloro che hanno già dimostrato in passato un minimo interesse verso l'azienda e il suoi prodotti, oppure rientrano nel target dell'offerta. Tale scrematura della domanda di mercato rende le attività di marketing più efficienti. Le imprese che sviluppano un piano di comunicazione mirata, possono inoltre ovviare al problema dell'information overload, che spesso caratterizza la ricerca di informazioni fatta dagli utenti prima dell'acquisto effettivo, per la valutazione delle alternative di prodotto presenti nel mercato (Cheung, Kwok, Law, Tsui, 2003).

Successivamente anche la fase di acquisto potrebbe avvenire online, attraverso una piattaforma di e-commerce. Le vendite in internet facilitano il processo di mass

customization in quanto permettono alle aziende di ricevere gli ordini di acquisto direttamente dai consumatori, offrendo loro un'ampia di gamma di prodotti e talvolta permettendogli di aggiungere ulteriori personalizzazioni. Online le aziende possono registrare tutti i clienti profilando i consumi di ciascuno di essi e individuandone le preferenze. Gli strumenti digitali di raccolta ed elaborazione dei dati aiutano le imprese a personalizzare l'offerta, basandosi sugli acquisti effettuati in passato. Le piattaforme di e-commerce migliorano il rapporto tra consumatori e imprese agendo nella customer journey: chi frequenta il sito è potenzialmente un consumatore, chi effettua un primo acquisto è soggetto a una politica di cross-selling aziendale, mentre serve stabilizzare il rapporto con i clienti già fidelizzati in passato (Schafer, Konstan, Riedl, 2001).

Infine nella fase di post-acquisto le aziende devono cercare di mantenere il proprio rapporto con la domanda fornendo un supporto nell'utilizzo del prodotto e chiedendo ai propri clienti un riscontro sulla loro esperienza di acquisto. Le imprese possono così monitorare il grado di soddisfazione dei clienti valutando le recensioni fatte online e i commenti presenti nei forum di discussione e nei social network. In quest'ultimo caso in particolare, è possibile agire anche cercando di incentivare il word of mouth, pubblicando contenuti di tipo diverso, al fine di ottenere un feedback generico sull'andamento della propria campagna di marketing. Tali attività permettono una partecipazione attiva dei soggetti a cui è indirizzata l'offerta aziendale, mediante la quale aumentare il coinvolgimento della domanda di mercato e individuare le carenze presenti nella propria offerta aziendale, su cui intervenire in futuro (Xia, Bechwati, 2008).

Infine, le aziende che intendono sviluppare un comportamento di trasparenza verso i propri utenti, rassicurandoli sull'uso delle informazioni personali, possono adottare delle tattiche che vanno oltre il semplice rispetto delle leggi sulla privacy. A tale riguardo le piattaforme online deve cercare di instaurare un rapporto diretto con l'utente al fine di supportarlo nelle proprie decisioni. Molte aziende ad esempio richiedono un frequente cambio delle password al fine di incrementare la cybersecurity delle iscrizioni online. Le notifiche per ricordare agli utenti di controllare il proprio grado di esposizione in rete possono essere affiancate a interruzioni delle condivisioni nel caso in cui vengano trattati dei dati sensibili

oppure nel momento in cui vengano rilevati mittenti potenzialmente rischiosi. Infine le piattaforme dovrebbero offrire uno sportello per accogliere e discutere quali possibili modifiche sono adottabili dall'azienda per migliorare la data retention e il data mining. Tali attività permettono all'impresa di aiutare l'individuo a gestire facilmente le proprie informazioni online, dimostrando la volontà di trattare quanto registrato in modo sicuro e corretto, rassicurando così la navigazione online dell'utente (Pötzsch, 2008).

Capitolo 4
Il caso Facebook e Cambridge Analytica

4.1
Definizione del caso

Nato nel 2004 come sito per gli studenti di Harvard, Facebook in poco più di dieci anni è diventato il social network più diffuso al mondo grazie agli oltre due miliardi di utenti registrati. Dopo un primo contributo dell'università, il sito ha iniziato a espandersi a livello globale nel 2006 con un'apertura ad Apple e Microsoft. In breve Facebook è riuscito a differenziarsi nel mercato dei social network, offrendo numerose opzioni di scelta per la condivisione di contenuti multimediali, notizie e informazioni personali, all'interno del proprio profilo (Boyd, Ellison, 2007).
Facebook fu fondato con l'obiettivo di facilitare la comunicazione tra persone, permettendo loro di restare connesse con i propri conoscenti, al fine di rendere il mondo più aperto e collegato. Tale intento, ripreso anche nella mission aziendale, costituisce il primo passo per la realizzazione del business model su cui si fonda la società che gestisce il sito. Il social network infatti, è stato creato sul modello di una piattaforma plurilaterale capace di servire varie categorie di clienti dando loro delle proposte di valore diverse a seconda dei loro interessi..
Facebook rappresenta una risorsa sfruttabile mediante diverse proposte di valore: da una parte gli utenti iscritti ottengono un mezzo di comunicazione ampio e gratuito, mentre dall'altra le aziende possono acquistare i dati rilasciati dagli utenti stessi nel sito, al fine di ottenere delle informazioni sulle tendenze di mercato e realizzare delle campagne pubblicitarie online di tipo mirato. Le aziende che utilizzano la rete per promuovere i propri prodotti, possono così servirsi della piattaforma per realizzare una profilazione dettagliata della domanda, individuando le caratteristiche del loro settore di riferimento e le varie categorie di

target. Dall'analisi di mercato è poi possibile impostare una campagna pubblicitaria mirata, da realizzare all'interno del social network, tramite inserzioni indirizzate esclusivamente ai profili target definiti dall'azienda. In questo modo, Facebook vende un vero e proprio servizio di marketing, volto a ottimizzare gli sforzi fatti nella comunicazione commerciale online.

Una terza proposta di valore realizzata da Facebook costituisce invece nella possibilità data dall'azienda a programmatori esterni, di utilizzare la piattaforma per la creazione di nuove applicazioni. La società ha infatti aperto i propri protocolli di dialogo API (application programming interface) a soggetti esterni, con lo scopo di ottenere un indotto di applicazioni indipendenti, legate al sito dalla condivisione dei dati appartenenti agli utenti. I programmatori che intendono realizzare nuove applicazioni per il web e il mobile, possono così accedere più velocemente a un volume di informazioni maggiore sui propri utenti. Tale pratica permette loro di semplificare la gestione dei dati raccolti e allo stesso tempo personalizzare la propria offerta (Understanding Facebook Business Model, 2012).

Facebook è stato più volte analizzato dal punto di vista psicologico, sociologico ed economico con lo scopo di individuare quali effetti ha portato la diffusione dei social network all'interno della sfera individuale e sociale. Uno dei temi che più di altri è stato studiato dal punto di vista etico e sociale riguarda la privacy degli iscritti al sito. La gestione delle informazioni personali all'interno dei social network rappresenta uno degli elementi più complessi dell'utilizzo degli strumenti digitali, tanto che in molti casi gli individui stessi non hanno la consapevolezza del volume di informazioni lasciate online, per cui ne possono esercitare un controllo parziale. Questo all'interno di una piattaforma come Facebook, in cui è possibile condividere e caricare qualsiasi tipo di contenuto rappresenta un ulteriore elemento di complessità difficilmente controllabile in modo individuale. Ciò nonostante, gli utenti iscritti al sito devono essere consapevoli delle dinamiche di trattamento delle proprie informazioni personali, sia per quanto riguarda il ruolo che queste hanno nella rappresentazione dell'identità dell'individuo rispetto al contesto sociale in cui è inserito, sia per il rischio di possibili violazioni della privacy da parte di terzi non autorizzati (Young, Quan-Haase, 2013).

La questione della tutela della privacy nei social network intesa come la protezione dei dati personali condivisi in Facebook, ha avuto un'ampia risonanza a livello mondiale a marzo del 2018 grazie alle rivelazioni fatte da Christopher Wylie alla giornalista Carole Cadwalladr in un'intervista pubblicata poi nella rivista The Guardian. Il giovane ex dipendente dell'agenzia di consulenza Cambridge Analytica spiegò come la società inglese creata nel 2013 dal miliardario statunitense Robert Mercer, fosse riuscita a raccogliere e analizzare in modo abusivo i dati appartenenti a milioni di utenti iscritti a Facebook per lo più residenti negli Stati Uniti. L'agenzia era in grado di sottrarre tali informazioni sfruttando l'app di intrattenimento "Thisisyourdigitallife" sviluppata inizialmente per fini accademici dal docente di psicologia russo-americano Aleksandr Kogan. Quest'ultimo oltre a esser l'autore dell'applicazione, aveva progettato una sorta di copertura per Facebook, camuffando l'attività di raccolta dati in attività di ricerca universitaria, relativa a studi di psicologia, con lo scopo di venir legalmente accettato dalla piattaforma stessa. Le informazioni registrate venivano raccolte sia dagli utenti che scaricavano l'applicazione che dai profili a loro collegabili, in quanto la registrazione era possibile anche tramite il social login.

Secondo l'ex dipendente di Cambridge Analytica Christopher Wylie, lo scopo dell'agenzia era la profilazione psicologica degli utenti del social network al fine di creare una comunicazione altamente personalizzata, da utilizzare per scopi politici. La società inglese infatti oltre ad esser finanziata da Robert Mercer, riceveva l'appoggio da Steve Bannon, stratega di Donald Trump e Nigel Farage, leader del partito inglese Ukip. L'azione diretta svolta dall'agenzia inglese all'interno di Facebook servì infatti a supportare la campagna elettorale dell'attuale presidente degli USA e a favorire l'esito del referendum sulla Brexit. Sempre in base a quanto affermato da Christopher Wylie, Cambridge Analytica venne consapevolmente fondata da Robert Mercer e Steve Bannon nel Regno Unito, con lo scopo permettere al partito repubblicano di sfuggire alle leggi sulla privacy alle quali è sottoposto il governo statunitense, per le quali non sarebbe stata possibile una tale attività di raccolta e analisi di dati a fini politici (Cadwalladr, 2018).

Già nel 2014 Facebook prese la decisione di limitare lo scambio di dati e applicazioni collegate al social, con lo scopo di prevenire la diffusione di sistemi

abusivi di data retention e controllare l'esposizione delle informazioni appartenenti ai membri della piattaforma. Due anni dopo Facebook decise definitivamente di bloccare la condivisione di dati con "Thisisyourdigitallife" e ne ordinò la cancellazione di quelli raccolti, dopo che la società venne a conoscenza dei reali obiettivi di Cambridge Analytica, tramite un articolo pubblicato nel periodico del The Observer. Già allora l'inchiesta descriveva alcuni aspetti delle attività di Robert Mercer nella questione Brexit e nelle elezioni statunitensi, cercando di definire i ruoli di Steve Bannon, Donald Trump, Nigel Farage e Cambridge Analytica. Nell'articolo si accennava inoltre all'uso politico dei dati raccolti dall'agenzia attraverso Facebook, quale fonte primaria dei dati utilizzati nella profilazione di decine di milioni di utenti (Cadwalladr, 2017).

Tali affermazioni vennero respinte sia da Cambridge Analytica, che da Simon Milner, responsabile della privacy di Facebook per il Regno Unito. Ciò nonostante la vicenda spinse il social network a troncare definitivamente ogni rapporto con l'agenzia e a ordinare l'eliminazione dei dati raccolti. Nonostante la conferma di Cambridge Analytica, le informazioni raccolte non vennero distrutte, d'altro canto Facebook non fece alcuna ulteriore azione per la verifica e il monitoraggio dei dati detenuti dall'agenzia (Cadwalladr, 2018).

4.2
Prime conseguenze delle rivelazioni

L'inchiesta sulle attività di data retention e data mining svolte da Cambridge Analytica venne realizzata dai giornalisti Matthew Rosenberg, Nicholas Confessore, Carole Cadwalladr e Emma Graham-Harrison appartenenti alle testate del New York Times, del The Guardian e del suo periodico The Observer. Le rivelazioni di Christopher Wylie uscirono il 17 marzo 2018 rispettivamente negli articoli "How Trump Consultants Exploited the Facebook Data of Millions" nel New York Times e "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in

major data breach" nel The Guardian (Rosenberg, Confessore, Cadwalladr, 2018) (Cadwalladr, Graham-Harrison, 2018).

Le reazioni del mondo politico ed economico furono immediate a livello globale. Già il giorno seguente il congresso statunitense convocò Mark Zuckerberg a testimoniare sulla vicenda, mentre anche Federal Trade Commission, l'agenzia federale per il commercio, comunicò l'apertura di un'inchiesta sul coinvolgimento di Facebook nella vicenda (Wong, 2018). Lo scandalo ebbe una forte risonanza anche in Europa con l'affermazione del portavoce esecutivo sull'apertura di un'ulteriore inchiesta promossa dalla Commissione Europea per il chiarimento della vicenda. A livello locale, l'autorità britannica per la protezione dei dati (Information Commissioner's Office - ICO) intraprese un'inchiesta relativa ai rapporti tra partiti politici e agenzie per il data mining al fine analizzare le modalità di profilazione dell'elettorato per la promozione di campagne politiche. Anche le autorità italiane per la protezione dei dati personali (Garante Privacy) e per le garanzie nelle comunicazioni (AGCOM) intervennero nella questione facendo delle richieste di chiarimenti a Facebook, per confermare o smentire le ipotesi di utilizzo di dati mosse dalla testata del The Guardian, verificando il coinvolgimento di soggetti politici operanti in Italia (Lo Conte, 2018).

Tale attivismo fu giustificato dalla portata dello scandalo. Infatti, dopo una prima stima di 50 milioni, il numero definitivo di profili spiati fu stabilito a circa 87 milioni, di cui 70 milioni appartenenti a cittadini statunitensi. Tuttavia il caso ebbe una risonanza mondiale coinvolgendo altri Paesi come le Filippine, l'Indonesia e il Regno Unito, che insieme registrarono circa un milione di utenti spiati in ciascuno di essi, mentre in Italia se ne registrarono 214 milia (Simonetta, 2018).

Oltre a quelle politiche, vi furono anche immediate reazioni economiche e finanziarie. Il titolo di Facebook perse in Borsa circa 60 miliardi di dollari nei soli primi due giorni successivi allo scandalo, registrando un calo del 7% già il lunedì successivo alla pubblicazione degli articoli. Sempre in quel giorno, il crollo di Facebook ebbe delle ripercussioni anche sui titoli appartenenti agli altri social network fra cui Snapchat e Twitter che chiuse con un calo superiore al dieci percento (Lo Conte, 2018). In aggiunta al clima d'instabilità finanziaria delle prime settimane, si unirono le espulsioni di Alex Stamos, responsabile della sicurezza

delle informazioni di Facebook e Alexander Nix, CEO di Cambridge Analytica, seguite da una campagna di boicottaggio al social network alla quale aderirono anche Elon Musk, Ceo e fondatore di Tesla e Brian Acton, co-fondatore di WhatsApp e ex dipendente della stessa holding Facebook Inc. (Simonetta, 2018).

Il 21 marzo 2018 Mark Zuckerberg intervenne nella vicenda pubblicando un post nel profilo suo stesso social network. Il fondatore di Facebook chiarì la posizione del social network nel rapporto con Cambridge Analytica e con il ricercatore universitario Aleksandr Kogan. Zuckerberg spiegò come nel 2007 la piattaforma venne integrata con alcune funzioni che permettevano agli utenti di condividere delle informazioni con i propri amici, come la data di compleanno o il luogo di residenza. Tale sistema di gestione dei dati permetteva agli iscritti di Facebook, di poter accedere ad altre piattaforme d'informazione o intrattenimento realizzate da terzi e collegate al social network. Nel 2013 tale meccanismo consentì ad Aleksandr Kogan di accedere ai dati personali di decine di milioni di utenti tramite l'applicazione d'intrattenimento "Thisisyourdigitallife", con cui era possibile effettuare dei test di personalità. Quest'ultima nonostante fosse stata scaricata da sole 300 mila persone, riuscì a raccogliere le informazioni provenienti da milioni di profili, sfruttando i collegamenti di amicizia di coloro che avevano scaricato quel gioco. Nel 2014 il rinnovo della piattaforma di condivisione avrebbe dovuto limitare questo sistema di scambio delle informazioni appartenenti ai membri del social, in modo da prevenire possibili sistemi abusivi di data retention simili a "Thisisyourdigitallife". Infine, nel 2015, le prime inchieste pubblicate sul The Guardian spinsero Facebook a bloccare definitivamente i rapporti con Cambridge Analytica. La società richiese e ottenne anche un certificato in cui l'agenzia dichiarava l'avvenuta eliminazione delle informazioni sottratte.

Dopo questa ricostruzione Mark Zuckerberg ammise le responsabilità della società, affermando la propria determinazione nella realizzazione di maggiori controlli per la tutela della privacy degli iscritti e in particolare per il controllo delle applicazioni collegate al social network. Le scuse sulla vicenda, servirono anche ad affermare i valori di tutela e correttezza applicati dalla società nella gestione dei dati appartenenti agli utenti iscritti al sito, nel rispetto di una politica di trasparenza promossa dal sito.

"Abbiamo la responsabilità di proteggere i tuoi dati, e se non possiamo, non meritiamo di servirti. Ho lavorato per capire esattamente cos'è ' successo e come fare in modo che non succeda di nuovo. La buona notizia è che le azioni più importanti per evitare che ciò accada di nuovo oggi abbiamo già preso anni fa. Ma abbiamo anche commesso degli errori, c'e ' altro da fare, e dobbiamo fare un passo avanti e farlo."

(Mark Zuckerberg, post pubblicato nel profilo Facebook il 3 marzo 2018)

Lo stesso impegno nella tutela della privacy fu ribadito da Zuckerberg il dieci e l'undici aprile 2018 durante la sua testimonianza davanti al congresso statunitense. In questo caso, il CEO di Facebook chiarì la posizione del social relativamente al controllo della distribuzione di dati online, alle autorizzazioni richieste agli utenti e la censura e al marketing politico esercitato nella piattaforma. Lo stesso business model fu preso in causa nel corso del dibattito di Capitol Hill. Tuttavia Zuckerberg, negata l'ipotesi di un possibile intervento a quest'ultimo, affermò il suo impegno al miglioramento della gestione delle applicazioni legate alla piattaforma, al fine di evitare eventuali fughe e abusi di dati personali. Sempre davanti ai rappresentanti del congresso Zuckerberg si scusò con gli iscritti della piattaforma per le mancanze nei controlli a "Thisisyourdigitallife", ribadendo l'atteggiamento opportunistico esercitato da Kogan e da Cambridge Analytica e dichiarando di esserne stato lui stesso vittima (Smith, 2018).

A maggio 2018 Mark Zuckerberg intervenne anche all'Eurocamera per chiarire la posizione del social network sul caso Cambridge Analytica al Parlamento Europeo. Il fondatore di Facebook colse l'occasione per scusarsi su quanto avvenuto, affermando di voler migliorare i processi di gestione dei dati e in particolare il funzionamento degli algoritmi di condivisione delle informazioni. Nel dibattito Zuckerberg cercò di chiarire altri elementi di criticità del sito, relativi alla gestione delle fake news e a una possibile rottura della gestione monopolistica esercitata dalla holding, ipotizzata da diversi parlamentari europei.

Entrambi gli interventi ebbero una doppia funzione: le autorità ottennero una testimonianza chiave per il chiarimento delle responsabilità, mentre Facebook potè difendersi in modo pubblico dalle accuse subite, cercando di salvare la propria brand reputation (Waterson, 2018).

4.2.1 Conseguenze finanziarie e reputazionali

Il datagate di marzo 2018 ha avuto dei risvolti decisivi per Cambridge Analytica, Facebook e altre piattaforme di social network, non direttamente coinvolte nella vicenda. Il primo effetto risolutivo della vicenda fu la chiusura di Cambridge Analytica a maggio 2018. L'agenzia dichiarò bancarotta, ricevendo l'ordine di restituire qualunque tecnologia detenuta, tra cui anche i computer dei dipendenti, da parte del commissario per le informazioni del Regno Unito .

Diversi furono invece gli effetti sul social network, che cercò di superare la crisi finanziaria e reputazionale intervenendo sia sul fronte istituzionale che su quello promozionale. Dopo i primi chiarimenti fatti davanti al Congresso statunitense e al Parlamento Europeo, Facebook intervenne in modo proattivo per ridurre gli effetti delle rivelazioni sull'azienda. Considerando il successo finanziario dell'azienda è proporzionale al numero di iscritti, la società decise di intervenire in modo tempestivo sul rapporto con i propri utenti e in particolare, con quelli interessati delle attività di data retention fatte da Cambridge Analytica. Facebook decise dunque di inviare una notifica di avviso ai profili coinvolti nel datagate, al fine di renderli coscienti della loro posizione. Nel contempo l'azienda promosse una campagna pubblicitaria di sensibilizzazione sull'uso responsabile dei dati personali online e sulla questione delle fake news. Il progetto fu realizzato mediante la pubblicazione di post all'interno del sito stesso e l'impiego di mezzi di comunicazione più tradizionali, come inserzioni nei quotidiani e cartellonistica per esterni (Valsania, 2018).

Il titolo di Facebook Inc. ebbe un andamento altalenante per tutta l'estate del 2018, registrando una prima ripresa a maggio e un successivo crollo a luglio. Dopo lo scandalo infatti, la società riacquisì un valore di mercato precedente alla crisi, arrivando a raggiungere i 530 miliardi di dollari rispetto ai 440 miliardi a cui era precipitata il mese precedente. I nuovi aggiornamenti introdotti nella piattaforma per incrementare la sicurezza delle informazioni personali e l'adeguamento alle nuove normative europee sul trattamento della privacy online sostennero la ripresa del titolo in Borsa. Analogamente anche la pubblicazione dei risultati finanziari del primo trimestre convinsero i mercati, considerato il valore maggiore

degli utili realizzati dall'azienda, rispetto alle stime degli fatte in precedenza dagli analisti. Facebook acquisì inoltre circa 70 milioni di nuovi utenti, che le permisero di raggiungere un giro d'affari di 12 miliardi di dollari, rispetto agli 11,41 miliardi previsti e rendendo un profitto di 1,63 dollari per azione (Simonetta, 2018).

A luglio avvenne un secondo crollo finanziario. A metà del mese l'autorità britannica per la privacy e la protezione dei dati personali (Information Commissioner's Office, Ico) sanzionò Facebook per non aver vigilato abbastanza sulle attività di Cambridge Analytica, sancendo una pena pecuniaria di oltre 565 mila euro. L'ammenda imposta al social network rappresentava il massimo valore previsto dalla vecchia normativa, in vigore all'epoca dei fatti.

Alla notizia seguì la pubblicazione dei report sull'andamento economico della holding nella seconda metà dell'anno. I dati tradirono le aspettative degli azionisti, considerando che il numero di iscritti al social network raggiunse i 2,23 miliardi di utenti, rispetto ai 2,25 attesi, perdendo circa un milione di iscritti solo in Europa. Tale notizia fu giustificata dallo stesso Zuckerberg come l'effetto dell'entrata in vigore del nuovo regolamento europeo per la protezione dei dati (GDPR). I dati incisero anche sull'andamento del titolo, provocandone un crollo in Borsa immediato. Le azioni di Facebook Inc. passarono nel giro di una giornata dal valore di 217 dollari a quello di 175 con una diminuzione del 20% circa (Savioli, 2018). Le stesse difficoltà finanziarie e il calo di iscritti di Facebook, vennero riscontrate anche da Twitter. Entrambe le aziende diedero la colpa al nuovo Regolamento europeo per la privacy. Ciò nonostante gli stessi manager ammisero che il periodo di valenza del GDPR rappresentava una piccola parte del trimestre di valutazione (Magnini, 2018).

Un'ulteriore conferma della crisi di Facebook si verificò qualche mese più tardi con la pubblicazione di una ricerca realizzata dal Pew Research Center. L'indagine faceva emergere un calo di fiducia verso la piattaforma anche negli Stati Uniti, tanto che un americano su quattro dichiarava di aver cancellato l'app dal proprio smartphone, mentre il 54% affermava di aver modificato le impostazioni sulla privacy. Quest'ultimo elemento rappresenta un fattore positivo in materia di tutela dati, ipoteticamente imputabile alla stessa campagna di sensibilizzazione promossa da Facebook stessa nel 2018 (Tre, 2018).

A oggi Facebook Inc. rappresenta ancora una delle holding più importanti nel mercato dei social network e della messaggistica diretta, non solo per i brand di Facebook e Messenger, ma anche grazie alle acquisizioni di WhatsApp, Oculus Rift e Instagram. Proprio il successo di queste ultime ha aiutato Facebook a superare le difficoltà finanziarie date dagli scandali delle fake news e dal datagate di Cambridge Analytica, suscitando tuttavia una serie di turbamenti interni. Nel giro di poco più di un anno, tutti i fondatori delle tre società acquisite da Facebook Inc. hanno deciso infatti di abbandonare i loro ruoli all'interno dell'azienda, a causa di attriti avuti con Mark Zuckerberg. Quest'ultimo starebbe infatti svolgendo una sorta di commissariamento verso le aziende acquisite, affidando a uomini di fiducia propri incarichi cruciali per lo sviluppo e la direzione delle singole società.

Il primo ad andarsene fu il fondatore di Oculus Palmer Luckey, a maggio 2017, al quale fecero seguito nel 2018 i fondatori di WhatsApp, Jan Koum e Brian Acton e quelli di Instagram, Kevin Systrom e Mike Krieger. Quest'ultima uscita ha rappresentato segno evidente delle intenzioni di Zuckerberg sulla gestione dei brand della holding, in quanto sarebbe stata causata dallo spostamento del product manager Adam Mosseri da Facebook a Instagram. Nel 2018 il social network di fotografia ha aiutato Facebook Inc. a superare i problemi finanziari dati dagli scandali, rappresentando oltretutto una via di fuga per gli utenti delusi da quanto accaduto. La società oltre a non esser stata coinvolta nel caso Cambridge Analytica, sta avendo un ottimo successo con le nuove generazioni, grazie al formato di condivisione delle immagini e alle "stories", dove gli utenti possono condividere brevi video, similmente a quanto già avveniva con Snapchat (Savioli, 2018).

Dal momento dell'acquisizione a oggi, Instagram ha centuplicato il suo valore economico, passando dai 30 milioni di utenti attivi nel 2012, all'attuale miliardo di iscritti. Per i prossimi cinque anni ci si attende un'ulteriore crescita del social, da cui sono previste anche delle ottime performance in termini di annunci pubblicitari. Per quanto riguarda quest'ultimo aspetto, uno degli obiettivi attuali di Facebook Inc. è la gestione coordinata dei due social. Secondo quanto ipotizzato per il futuro infatti, i dati raccolti su Instagram potrebbero essere impiegati anche per indirizzare gli annunci pubblicitari su Facebook e viceversa, creando un

supporto reciproco utile nei casi difficili, simili a quelli affrontati dal social network di Menlo Park nel 2018 (Simonetta, 2018).

Il trattamento dei dati su Facebook rappresenta dunque ancora una sfida aperta per la piattaforma, considerando le instabilità finanziarie ed economiche del brand, successive alle inchieste pubblicate dal The Guardian e dal New York Times. La vicenda ha messo in evidenza la vulnerabilità della piattaforma, rispetto a possibili cyber-attacchi e ad eventuali fughe di dati, incidendo fortemente nella sua brand reputation. Le richieste di chiarimento da parte delle autorità internazionali hanno permesso a Mark Zuckerberg di definire il ruolo di Facebook nella vicenda e affermare in modo pubblico il modello di business del social network. Le prospettive economiche e finanziarie delle società acquisite da Zuckerberg, quali Oculus, Instagram e WhatsApp hanno supportato l'intera holding nel superamento della crisi finanziaria data dalla vicenda di Cambridge Analytica. Tuttavia il ridimensionamento interno della holding e le promesse di Zuckerberg per la creazione di nuovi sistemi di sicurezza dei dati potrebbero non bastare alle generazioni future come garanzie di tutela sul trattamento delle informazioni condivise (Simonetta, 2018).

Capitolo 5
Percorso di ricerca

5.1
Scenario: presupposti e motivazioni per la ricerca

La questione della privacy è un fattore soggettivo che coinvolge le persone in modo diverso, a seconda del contesto, del loro vissuto e del loro carattere. Nella dimensione online la privacy è determinata dalla propensione degli stessi alla condivisione di informazioni proprie con terzi. I dati personali sono fondamentali nelle comunicazioni digitali in quanto rappresentano l'identità della persona, che nella rete a differenza della realtà, non possono essere riconducibili a un corpo fisico.

La tutela delle informazioni scambiate all'interno delle piattaforme online rappresenta una delle più importanti sfide dei sistemi legislativi internazionali. Nei primi anni Novanta la diffusione di internet fu interpretata da molti come l'inizio di una nuova era, in cui le piattaforme digitali dovevano rappresentare uno strumento libero da qualsiasi ordinamento giuridico nazionale e internazionale. Ciò nonostante, l'uso diffuso del web diede luogo alla necessità di creare un insieme di norme adeguate, capaci di tutelare gli utenti. Nella pratica tale bisogno fu colmato con l'introduzione di nuove leggi, valide a integrare alcuni aspetti del diritto esistente, indirettamente relativi all'uso di internet.

Online, le aziende possono raccogliere e analizzare tutte quelle informazioni rilasciate dagli utenti, riguardanti il loro profilo identitario, il loro stile di vita e il loro abituale comportamento d'acquisto. I dati posseduti possono essere impiegati nelle attività di marketing, per lo studio della domanda di mercato e la profilazione dei singoli individui, allo scopo di rendere più efficiente la comunicazione aziendale e così migliorare il posizionamento. D'altro canto, le attività di raccolta e d'uso di

queste informazioni sono state percepite da molti come una violazione della privacy, fatta a scopi commerciali e dunque ritenute non eticamente corrette. Per questo motivo, nel corso degli ultimi vent'anni molte aziende attive nel settore, si sono mobilitate per chiedere la creazione un ordinamento giuridico internazionale, volto stabilire le corrette modalità di raccolta e gestione dei dati. Nell'attesa che ciò avvenga, molte di queste hanno realizzato dei codici etici per il corretto trattamento delle informazioni raccolte, con la prospettiva d'instaurare con i propri stakeholder dei rapporti stabili, basati sulla fiducia reciproca.

Finora uno degli ordinamenti più evoluti in materia di trattamento dei dati online è dell'Unione Europea, il quale rappresenta un modello d'ispirazione per gli altri stati e per tutti gli operatori di settore. Le normative europee si basano sulla logica del principio consensuale, facendo leva sulla consapevolezza che gli utenti devono avere sulle modalità di raccolta e gestione delle loro informazioni. Tale principio è in parte ostacolato dal fenomeno del privacy paradox, ovvero dalle difficoltà che gli utenti stessi hanno nella gestione dei propri dati online.

Di recente il datagate di Facebook e Cambridge Analytica ha suscitato in tutto il mondo una serie di reazioni di sdegno e sfiducia verso il social network. A livello politico c'è stata una comune richiesta di chiarimenti, mentre a livello finanziario si è verificato il crollo del titolo in Borsa, nel corso delle prime settimane successive alle rivelazioni. L'evento ha aperto un dibattito sul modello di business di Facebook, dimostrando come anche uno dei più popolari social network possa essere vulnerabile a usi impropri e fughe di dati.

Il caso di Facebook potrebbe sensibilizzare gli utenti sulla gestione consapevole delle informazioni online. Il datagate potrebbe avere delle ripercussioni nel lungo termine, sul livello di fiducia che gli utenti hanno verso i social network e verso le aziende che praticano attività di data retention online. Per questo motivo, le aziende devono maturare un atteggiamento responsabilità sui dati raccolti, cercando di individuare quali pratiche sono ritenute corrette dagli utenti. Un'aperta dichiarazione sulle dinamiche di trattamento dei dati, rende le persone consapevoli della propria identità digitale. Ciò permette loro di scegliere consciamente la destinazione dei loro dati, creando inoltre un senso di fiducia nelle aziende che praticano le attività di data retention e data mining online.

5.2
Oggetto di ricerca

La research question della ricerca è la valutazione di quanto gli utenti siano sensibili alla sicurezza dei propri dati online. L'indagine ha lo scopo di analizzare le modalità di gestione delle informazioni personali online, considerando quanto sia importante per gli utenti soddisfare i bisogni di visibilità all'interno della propria rete sociale, piuttosto che tutelare i dati condivisi nel social network.
La ricerca intende inoltre prendere in considerazione lo scandalo Facebook e Cambridge Analytica, analizzando gli effetti che l'evento ha avuto sul senso generale di protezione della privacy online e sul grado di fiducia verso le aziende che svolgono attività di data retention e data mining. Tale osservazione è stata inserita in riferimento al fatto che lo studio è avvenuto entro i tre mesi successivi al dibattito mediatico internazionale, iniziato il 17 marzo 2018, con la pubblicazione sul New York Times e su The Guardian degli articoli "How Trump Consultants Exploited the Facebook Data of Millions" e "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach", in seguito all'inchiesta di Matthew Rosenberg, Nicholas Confessore, Carole Cadwalladr e Emma Graham-Harrison.

5.2.1
Popolazione di riferimento

La popolazione che si è ritenuto opportuno considerare nella ricerca, è costituita da un campione di circa duecento studenti iscritti a un corso di laurea triennale o magistrale presso l'università Ca' Foscari di Venezia, nati tra il 1990 e il 1999 (compresi) e iscritti a Facebook.
La scelta di queste specifiche caratteristiche è stata ritenuta la più appropriata in forza alla necessità di individuare dei soggetti interessati quotidianamente all'uso dei social network, sia per motivi personali che per scopi accademici, considerando

le attività di supporto fornite dalle communities universitarie presenti nella piattaforma. Il campione inoltre, prende in considerazione degli studenti universitari per i quali l'Università Ca' Foscari si dota di strumenti di informazione quali periodici cartacei (es. Il sole 24 ore), newsletter settimanali, spazi per l'organizzazione di dibattiti e associazioni volontarie (es. This Marketers Life) che hanno trattato del caso in esame. Secondo questa prospettiva, si presume perciò che i soggetti coinvolti nell'indagine siano a conoscenza del tema trattato, dunque anche capaci di contestualizzare i termini di riferimento utilizzati nella ricerca.
La fascia di età scelta per la ricerca, comprende una popolazione tra i 19 e 29 anni, la quale risulta essere la più interessata dall'uso di Facebook anche a livello mondiale, registrando un tasso di penetrazione di circa il 15% (Global Digital Report 2018, 2018). Gli utenti campionati potrebbero inoltre essere stati coinvolti nel caso Cambridge Analytica, considerando nel 2014 avevano già superato l'età minima per l'iscrizione al social network, posta dalla piattaforma a tredici anni.
L'indagine ha coinvolto i soli utenti iscritti a Facebook in quanto oltre a essere il social network più diffuso al mondo, è anche l'unico a esser stato direttamente coinvolto nel datagate di marzo 2018.

5.2.2
La domanda di ricerca

Considerata l'importante evoluzione che sta avvenendo nel rapporto tra aziende e consumatori all'interno delle piattaforme online, studio mira ad individuare i principi considerati etici dalla domanda di mercato, relativamente alle attività di data retention e data mining svolte con fini promozionali.
Nello specifico la ricerca riprende alcuni concetti riguardanti il tema della privacy al fine di individuare i fattori determinanti il comportamento degli individui nelle piattaforme online. Le principali nozioni considerate nella descrizione del fenomeno riguardano la determinazione dei fattori che compongono l'identità digitale, la spiegazione delle attività di data retention e data mining all'interno delle

strategie di marketing, l'esposizione delle normative presenti in materia e infine la rappresentazione del privacy paradox e delle sue cause.
Tale contestualizzazione permette così una prima comprensione dal punto di vista legale ed etico del caso Facebook e Cambridge Analytica avvenuta a marzo 2018. L'ampia risonanza avuta dalla notizia ha avuto degli impatti finanziari e politici immediati. Nella ricerca si ipotizza che lo scandalo abbia suscitato delle reazioni anche nei soggetti iscritti alla piattaforma, ma non direttamente coinvolti nell'abuso di dati fatto da Cambridge Analytica. L'evento infatti, ha dimostrato materialmente i pericoli derivanti dalla condivisione di informazioni personali nella rete, giustificando le sensazioni di rischio percepite dagli utenti. Per queste ragioni, la domanda di ricerca si è focalizzata sull'analisi della gestione dei dati in Facebook, al fine di valutare il comportamento assunto dagli utenti iscritti al social network prima e dopo quanto avvenuto.
Il caso trattato rappresenta un argomento di interesse anche per lo studio del marketing, considerando l'importanza che hanno i social network nella comunicazione commerciale online, per la promozione di brand e prodotti e per lo studio della domanda e la profilazione degli utenti. L'ampio uso delle informazioni personali svolto in rete rischia di esser percepito come una continua violazione della privacy, capace di ledere anche la brand reputation di chi lo svolge. Una dimostrazione di rispetto e impegno nella tutela delle informazioni condivise in rete, aiuta le aziende ad acquisire fiducia dalla domanda di mercato e ottenere ulteriori miglioramenti nella loyalty complessiva.

5.3
Risultati ipotizzabili sulla base della letteratura consultata

In base alla letteratura consultata sono state formulate alcune ipotesi riguardanti i risultati che ci si attendeva dall'indagine, prima che questa venisse effettivamente compiuta. Lo studio ha approfondito degli aspetti relativi alle conseguenze del caso Facebook e Cambridge Analytica, che finora non è stato ancora del tutto trattato in

ambito accademico. Ciò nonostante, sono state utilizzate diverse ricerche svolte in passato, relative al comportamento degli utenti nella gestione dei dati personali in rete. Tali studi analogamente a quanto trattato dall'indagine, delineano il punto di vista dei consumatori, individuando il loro grado di consapevolezza in tema di information privacy e tutela delle informazioni personali.

Di seguito, dunque, si riportano le principali ipotesi effettuate.

In primo luogo, rispetto a quanto è stato osservato, nel privacy paradox esiste una discrepanza tra le modalità di controllo della sicurezza dei dati online e quelle di gestione della propria immagine nelle piattaforme di social network (Young, Quan-Haase, 2013). Per questo motivo, nella ricerca si ipotizza che il numero di modifiche fatte dagli utenti relativamente alle impostazioni sulla visibilità del profilo all'interno del social network, siano maggiori di quelle sulla privacy a tutela dei dati condivisi nella piattaforma.

Rimanendo in tema inoltre, è possibile ipotizzare che il comportamento relativo alla protezione dei dati personali sia omogeneo per tutti gli individui campionati, giustificato da una generale indifferenza a riguardo. Al contrario invece, si ipotizza di individuare due modelli di comportamento che caratterizzano le scelte sulla visibilità: un profilo più incline a condividere informazioni personali e dunque meno interessato al controllo dei propri dati online e un secondo modello comportamentale, caratterizzato da un minor orientamento all'esposizione nei social ma più vigile sulla destinazione delle proprie informazioni.

Una terza ipotesi assunta dalla ricerca approfondisce l'assenza di interesse verso il tema della privacy e il controllo della diffusione dei dati online, dopo il datagate Cambridge Analytica e Facebook. In base alla letteratura considerata si suppone infatti che gli iscritti al social network abbiano scelto di continuare a utilizzare la piattaforma come sempre, nonostante avessero dimostrato in passato un certo grado di conoscenza dei termini di privacy presenti nel sito, intervenendo con alcune modifiche entro due anni precedenti al caso. Ciò dimostrerebbe l'assenza di una correlazione tra le cautele assunte dopo lo scandalo di marzo 2018 e un comportamento responsabile nella gestione della sicurezza dei propri dati online.

Una quarta ipotesi di ricerca riguarda invece l'impatto emotivo del datagate Facebook e Cambridge Analytica. Considerate le caratteristiche del campione

selezionato e la letteratura approfondita, ci si attende una diffusa conoscenza del caso preso in considerazione, basata sull'interesse dimostrato dagli iscritti alla piattaforma e su una diffusa consapevolezza dei rischi che la condivisione dei dati comporta. Tuttavia ci si attende un immutato utilizzo del social network, giustificato dalle gratificazioni percepite dagli utenti (Kokolakis, 2015) e sostenuto dal senso di fiducia verso il nuovo regolamento europeo sulla protezione dei dati (GDPR), entrato in vigore a maggio 2018, ovvero durante la raccolta dei dati.

In correlazione a quanto detto ci si attende inoltre che la maggioranza dei soggetti coinvolti nella ricerca, oltre conoscere la notizia del datagate Facebook e Cambridge Analytica, ritenga che quanto avvenuto possa ripetersi in futuro. La consapevolezza che un abuso simile possa accadere nuovamente, non rappresenta tuttavia un motivo sufficiente per aumentare i controlli sull'uso e la condivisione di informazioni all'interno del sito. Per questo motivo ci si attende che la maggioranza degli utenti coinvolti nel campione pensi che una violazione di dati in Facebook analoga a quella rilevata a marzo 2018, possa ripetersi in futuro, ciò nonostante continua a utilizzare la piattaforma come prima.

Una sesta ipotesi riguarda l'utilizzo di Facebook come piattaforma capace di registrare un alto livello di brand loyalty, grazie all'elevata diffusione che il sito ha in tutto il mondo. Considerando il marketing stesso dei siti di social network, è possibile analizzare i fattori di successo del brand, valutando la frequenza e il tempo complessivo passato dagli utilizzatori nella piattaforma. Per questo motivo la ricerca ipotizza di trovare una correlazione tra l'abituale tempo di utilizzo del sito e l'impatto della notizia nella gestione dei dati personali. Si presume infatti che un'alta frequenza e una lunga durata di navigazione nel social network rappresentino un elevato grado di fidelizzazione al brand, dal quale ne scaturisce un senso di fiducia e sicurezza degli iscritti, quali tenderanno a mantenere invariate le impostazioni sulla propria privacy, anche dopo il caso Cambridge Analytica.

Infine, in base ai dati anagrafici raccolti nel corso della ricerca, è possibile individuare le caratteristiche di chi effettivamente ha avuto una reazione negativa dalla vicenda di Cambridge Analytica. Considerando che dalla letteratura si evince la presenza di una correlazione tra il grado di istruzione e quello di controllo della privacy online, si ipotizza dunque di riscontrare un cambiamento dell'uso del social

network, come effetto di quanto avvenuto, da parte di chi attualmente sta frequentando un corso di laurea magistrale. Allo stesso modo si presume una scarsa conoscenza del caso considerato da parte di chi attualmente è iscritto al primo e al secondo anno di un corso di laurea triennale.

5.4
Disegno di ricerca

Tenendo in considerazione gli obiettivi posti dalla research question, la tipologia di informazioni che si intendono ricercare e i limiti pratici posti in essere dallo studio, è stato definito un progetto di ricerca capace di individuare i fattori determinati o meno le ipotesi assunte.
Il disegno di ricerca si basa sulle seguenti modalità di raccolta di dati primari, utili a confrontare la letteratura considerata nella prima parte della ricerca con la realtà attuale, contestualizzata nell'ambiente universitario di Ca' Foscari. L'obiettivo infatti consiste nella definizione delle reazioni suscitate dal caso Facebook e Cambridge Analytica, rispetto ai comportamenti abitualmente assunti dagli studenti nella gestione dei propri dati personali online.

5.4.1
Metodologia: ricerca quantitativa

La research question analizza la domanda dal punto di vista degli utenti della rete, intesi come consumatori di servizi online e nello specifico come utilizzatori di Facebook. A tale proposito, la metodologia di ricerca adatta all'indagine sociale svolta, presuppone l'utilizzo di un metodo qualitativo non standardizzato, che comprenda un approccio di tipo interpretativo della sfera soggettiva individuale.
Tale ipotesi tuttavia, è stata scartata a favore invece di metodologia di ricerca di tipo quantitativo standardizzato, con cui sopperire alla presenza di alcuni ostacoli

nella raccolta e nella gestione dei dati. Il disegno di ricerca è stato impostato seguendo il modello vari studi già in passato realizzati nell'ambito del privacy paradox, per cui l'atteggiamento degli utenti è stato approfondito secondo una scala di valori quantitativi attribuita dagli utenti alla rilevanza dei dati personali e al controllo sulla propria immagine e sulla propria privacy online. Le informazioni individuate nel corso dell'analisi della letteratura di riferimento e del caso preso in considerazione sono state dunque scomposte in tre sub aree semantiche e definite a loro volta in elementi osservabili specifici (Bernardi, 2005).

Partendo dal macro concetto della gestione della privacy in Facebook, sono state individuate tre dimensioni specifiche, semanticamente indipendenti fra loro, relative: ai sistemi di sicurezza a tutela delle informazioni personali nel social network contrapposto al controllo del grado di visibilità del proprio profilo; allo studio delle reazioni al caso Facebook e Cambridge Analytica e alla raccolta di dati anagrafici. La prima area di significato presa in considerazione è stata definita sul modello di ricerche precedentemente svolte in ambito accademico, riguardanti il tema del privacy paradox e in particolare della dicotomia comportamentale, esistente nell'atteggiamento e nella condotta di tutela della propria privacy online. Il resto dello studio invece, è stato impostato in base agli elementi concretamente osservabili, relativi alle reazioni degli utenti al caso considerato e alle loro caratteristiche personali. Tali indicatori sono stati scelti individuando dei fattori concreti relativi alle abitudini d'uso degli iscritti al social network e alle opzioni di privacy e visibilità controllabili dall'utente nella piattaforma.

5.4.2
Metodologia: il questionario online

Seguendo la scelta di una metodologia di ricerca quantitativa, è stato preso in considerazione il questionario come strumento di raccolta di dati primari. Tale scelta è stata giustificata dai fattori determinanti il contesto e le modalità di analisi.

La scelta del questionario distribuito direttamente tramite Facebook ha permesso di svolgere una prima selezione del campione, individuando solo i soggetti che sono iscritti alla piattaforma. Si suppone dunque che gli stessi utilizzino il sito in modo abituale e che conoscano le funzioni offerte e i sistemi di interazione con gli altri membri. Nel social network inoltre, sono presenti delle communities di studenti iscritti all'università Ca' Foscari che sono state utilizzate nel corso della ricerca per contattare i soggetti coinvolti nella somministrazione del questionario. I gruppi universitari presenti in Facebook sono stati selezionati in base alle caratteristiche del campione scelto per l'indagine.

Parte dell'indagine è stata realizzata utilizzando una ricerca precedentemente svolta in ambito accademico, per l'analisi delle caratteristiche di gestione delle informazioni online. La prima dimensione del questionario è stata infatti impostata seguendo l'analisi comportamentale sviluppata da Young e Quan-Haase nel 2013, relativa al controllo della propria immagine all'interno dei social, piuttosto che alle misure adottate per evitare casi di abusi, fughe e perdite di dati privati. La prima parte del questionario riprende gli stessi indicatori del modello di riferimento, anche se sono state fatte delle integrazioni, volte ad aggiornare le opzioni di scelta degli utenti, rispetto all'evoluzione della piattaforma stessa.

Nella seconda parte del questionario, quella relativa all'analisi del datagate, sono stati inseriti dei collegamenti ipertestuali ad articoli di giornale, considerati nella realizzazione dall'indagine. Tale opzione facilita la comprensibilità dell'utente alle domande poste, semplificando il processo di contestualizzazione dell'argomento. L'uso di questi strumenti è stato fatto con l'obiettivo documentare quanto citato nella breve presentazione del caso Facebook e Cambridge Analytica, che introduce le domande sul tema.

Nel complesso, all'interno del questionario sono state inserite delle matrici di valutazione e delle domande chiuse a scelta singola e doppia. In molti casi è stato ritenuto opportuno rendere flessibile tale schema, inserendo delle opzioni di fuga tipo "non lo so" o a scelta libera come "altro". Ciò ha reso il questionario meno rigido e più inclusivo, tanto da permettere la definizione di fattori non direttamente trattati dalle domande, quali ad esempio atteggiamenti ideali e comportamenti contestualizzati a una determinata condizione.

5.4.3
Modalità di raccolta dei dati

Dopo la stesura del questionario all'interno della piattaforma Google Moduli, i dati sono stati raccolti coinvolgendo un campione di studenti nati tra il 1990 e il 1999 (compresi), iscritti a Facebook e frequentanti un corso di laurea triennale o magistrale presso l'Università Ca' Foscari di Venezia.
Il campione ha interessato circa duecento soggetti, i quali hanno permesso di individuare le diverse caratteristiche del fenomeno preso in esame, rispetto a una popolazione di riferimento composta da studenti appartenenti a un unico ateneo. Per questo motivo, è necessario affermare che lo studio effettuato presenta un limite di rappresentabilità. Non è dunque possibile generalizzare i risultati della ricerca affermando che il campione selezionato descrive le caratteristiche comportamentali e attitudinali dell'intera popolazione di studenti universitari.
Il reperimento dei soggetti coinvolti nella ricerca è avvenuto secondo le modalità di seguito riportate.
I dati sono stati raccolti distribuendo il questionario all'interno delle diverse communities universitarie presenti nella piattaforma, riguardanti corsi di laurea realizzati da Ca' Foscari. I gruppi coinvolti sono stati i seguenti:

- Marketing e comunicazione Ca' Foscari 2016/2017 II anno
- Ca' Foscari_ Lingue Civiltà e Scienze del Linguaggio
- Ca' Foscari
- Magistrale Scienze del Linguaggio Ca' Foscari
- LLEAP Ca' Foscari Ve, curriculum iberistica
- Economia e Gestione Delle Aziende 2017/2019 Università Ca' Foscari
- Mediazione linguistica Treviso - Cà Foscari
- Studenti Di Lettere, Università Ca' Foscari Venezia
- Iscritti al corso di Filosofia a Ca' Foscari
- Studenti di conservazione dei beni culturali di Ca' Foscari

La scelta dei gruppi è stata fatta considerando le materie di interesse degli iscritti, per cui si è cercato di coinvolgere studenti appartenenti a diversi ambiti di studio, tra cui economia e management, lingue e culture, arti e discipline umanistiche e conservazione e gestione dei beni culturali. Fra i vari gruppi in cui è stato diffuso il questionario, "Ca' Foscari" è l'unico a non esser riferito ad un unico corso di studio, includendo in modo omogeneo tutti gli studenti iscritti all'ateneo.
Il file del questionario è stato pubblicato con una breve presentazione relativa allo scopo accademico per cui è stata realizzata la ricerca. Tale sistema ha permesso di raggiungere studenti appartenenti a corsi di studio diversi, selezionando in modo mirato solo quelli aventi le caratteristiche definite dal campione di riferimento.
Il periodo di raccolta è avvenuto dal 18 maggio e il 7 giugno 2018. Le risposte sono state accettate fino a esaurimento del numero di individui preposti dal campione, al fine di ottenere un volume di dati sufficiente a rappresentare la popolazione di riferimento e iniziare a svolgere l'interpretazione del fenomeno preso in esame.

5.4.4
Traccia del questionario

Il questionario è di tipo strutturato ed è composto prevalentemente da domande chiuse con una serie di opzioni a risposta singola, multipla o con una griglia di selezione. Questi sistemi di valutazione sono stati applicati in modo alternato, a seconda dell'indicatore considerato dalla domanda.
La traccia del questionario è stata strutturata in tre parti, descrittive delle tre dimensioni considerate dalla ricerca: la visibilità e la protezione dei dati personali, la reazione al caso Facebook e Cambridge Analytica e le caratteristiche anagrafiche. Le prime due parti sono precedute da una breve spiegazione volta a chiarire il tema e i concetti considerati dai quesiti. Nella terza parte sono state inserite delle domande relative alle informazioni anagrafiche, allo scopo di verificare le ipotesi effettuate. Infine nella parte finale del questionario sono state descritte le finalità, e le modalità del trattamento dei dati, in base a quanto previsto dall'ordinamento.

Prima parte

Gestione di dati personali in Facebook

La tutela della privacy è uno dei temi più dibattuti degli ultimi anni a causa delle varie piattaforme online, in cui è possibile registrare, salvare ed elaborare grandi volumi di dati. Gli stessi rappresentano una merce di scambio tra l'utente che usufruisce di un servizio gratuito, e il gestore del sito che ottiene una remunerazione, rivendendo le informazioni raccolte a terzi, solitamente per scopi commerciali (Young, Quan-Haase, 2013).

1. Da quanto tempo utilizzi Facebook?

- *Meno di 5 anni*
- *Dai 5 ai 10 anni*
- *Oltre i 10 anni*

2. Quante volte utilizzi Facebook?

- *Più volte al giorno*
- *Più volte alla settimana*
- *Più volte al mese*

3. Quanto tempo hai passato su Facebook la scorsa settimana?

- *Più di sei ore*
- *Più di tre ore*
- *Qualche minuto*

4. Quanti utenti sono registrati come amici sul tuo profilo Facebook?

5. Quanti di questi consideri davvero come tuoi amici anche nella vita reale?

6. Qual è il grado di visibilità del tuo profilo Facebook?

- *Il profilo è visibile nei motori di ricerca esterni a Facebook*
- *Il profilo è visibile da chiunque sia iscritto a Facebook*
- *Il profilo è visibile solo dagli amici degli amici*
- *Il profilo è visibile solo ai miei amici*
- *Non lo so*
- *Altro*

7. Quali impostazioni della privacy hai modificato negli ultimi due anni?

- *Chi può vedere i tuoi post*
- *Chi può vedere i post in cui sei taggato*
- *Chi può inviarti richieste di amicizia*
- *Chi può vedere la lista dei tuoi amici*
- *Chi può cercarti utilizzando l'indirizzo mail che hai fornito*
- *Chi può cercarti utilizzando il numero di telefono che hai fornito*
- *Nessuna delle precedenti*
- *Altro*

8. Quali limiti hai utilizzato verso altri utenti negli ultimi due anni?

- *Ho limitato la visibilità dei miei post ad alcuni amici*
- *Ho bloccato alcuni utenti*
- *Ho bloccato i messaggi provenienti da alcuni utenti*
- *Ho bloccato gli inviti alle applicazioni provenienti da alcuni utenti*
- *Ho bloccato gli inviti agli eventi provenienti da alcuni utenti*
- *Ho bloccato alcune applicazioni*
- *Ho bloccato delle pagine*
- *Nessuna delle precedenti*
- *Altro*

9. Quali impostazioni dei tag e del diario hai modificato negli ultimi due anni?

- *Chi può scrivere sul mio diario*
- *Chi può vedere cosa pubblicano sul mio diario*
- *Chi può vedere i post in cui sono taggato*
- *Il controllo dei post in cui sono taggato prima che vengano pubblicati nel mio diario*
- *Nessuna delle precedenti*
- *Altro*

10. Come reagisci solitamente alla richiesta di amicizia di uno sconosciuto?

- *Ignoro la richiesta*
- *Nego la richiesta*
- *Accetto la richiesta per avere più informazioni sulla persona*
- *Segnalo l'utente*
- *Blocco l'utente*
- *Altro*

11. Quali impostazioni di sicurezza hai attivato per tutelare il tuo profilo?

- *Modifico spesso le password*
- *Uso le autenticazioni a due fattori (password + codice dal cellulare)*
- *Ricevo avvisi dagli accessi sconosciuti*
- *Ho scelto degli amici da contattare nel caso non riuscissi ad accedere al mio profilo*
- *Nessuna delle precedenti*
- *Altro*

12. Quali altre informazioni sei disposto a condividere in Facebook?

	Solo io	*Visibilità limitata (amici)*	*Visibilità aperta*	*Non lo so*
Foto in cui sei taggato				
Video in cui sei taggato				
Post pubblicati				
Amici				
Interessi				
Informazioni personali				
Dati anagrafici				

13. Quali di queste soluzioni hai adottato per tutelare la tua privacy?

	1 (mai)	*2*	*3*	*4*	*5 (molto spesso)*
Uso i messaggi privati al posto di commenti pubblici					
Ho cambiato le opzioni sulla privacy nel mio profilo					
Limito le informazioni personali condivise					
Limito l'uso dei tag					
Ho eliminato alcuni post					
Ho limitato la visibilità del mio profilo a terzi					
Ho bloccato alcuni utenti					
Uso informazioni false per evitare un'eccessiva esposizione					

14. Ritieni che il nuovo regolamento europeo sulla protezione dei dati (GDPR) possa migliorare il trattamento delle tue informazioni personali online?

- *Credo possa migliorare il trattamento dei dati degli utenti*
- *Credo non apporti alcuna modifica sostanziale a quanto già esistente*
- *Credo rischi di essere un problema nell'uso della rete*
- *Non conosco la norma citata*
- *Non lo so*
- *Altro*

Seconda parte

Datagate Facebook

Lo scorso marzo, Facebook è stata accusata di non aver sorvegliato sull'uso improprio di dati appartenenti a 87 milioni di profili condotto da Cambridge Analytica, agenzia pubblicitaria che ha sostenuto la campagna elettorale di Donald Trump e la Brexit. Nonostante Mark Zuckerberg si sia impegnato davanti al Congresso Statunitense a contrastare possibili eventi simili invocando la necessità di un sistema legislativo più severo, la società è crollata in Borsa, ricevendo il boicottaggio di Elon Musk (fondatore di SpaceX e Tesla), Brian Acton (cofondatore di WhatsApp) e molte altre aziende americane.

(Fonti: Il sole 24 ore - Facebook: i profili ceduti a Cambridge Analytica sono 87 milioni, 214 mila italiani – di Biagio Simonetta 04 aprile 2018 - consultabile al link: http://www.ilsole24ore.com/art/tecnologie/2018-04-04/facebook-profili-ceduti-cambridge-analytica-sono-87-milioni-212600.shtml?uuid=AEC1evSE; Il sole 24 ore - Da Facebook a Google, perché è impossibile boicottare i big del web – di Biagio Simonetta 04 aprile 2018 - consultabile al link: http://www.ilsole24ore.com/art/notizie/2018-04-04/da-facebook-google-perche-e-impossibile-boicottare-big-web-152813.shtml?uuid=AEdN6kSE)

15. Conoscevi la notizia citata?

- *Sì, ho letto qualche articolo*
- *Sì, ne ho sentito parlare*
- *No, per niente*

16. Qual è stata la tua prima reazione alla notizia?

- *Interesse: ho cercato di approfondire la notizia*
- *Stupore: mi ha colpito ma non ho approfondito l'argomento*
- *Indifferenza: non credo che sia un fatto particolarmente importante*
- *Non conoscevo il caso*

17. Dopo quanto avvenuto, è cambiato il tuo modo di usare Facebook?

- *Intendo eliminare il mio account Facebook*
- *Ho fatto delle modifiche alla gestione dei miei dati personali*
- *Uno Facebook come prima*
- *Ho iniziato a usare di più altri social a cui sono iscritto*
- *Altro*

18. A quali altri social network sei iscritto?

- *Youtube*
- *Twitter*
- *Instagram*
- *Google +*
- *LinkedIn*
- *Pinterest*
- *Snapchat*
- *VERO*
- *Nessuno delle precedenti*
- *Altro*

19. Credi una cosa simile possa ripetersi in futuro?

- *Sì*
- *No*
- *Non so*

Terza parte

Dati anagrafici

20. Sei iscritto a…

- *Corso di laurea triennale*
- *Corso di laurea magistrale*

21. Quale anno stai frequentando attualmente?

- *Primo*
- *Secondo*
- *Fuori corso*

22. Sesso

- *Maschio*
- *Femmina*
- *Altro*

23. Anno di nascita

- *1999*
- *1998*
- *1997*
- *1996*
- *1995*
- *1994*
- *1993*
- *1992*
- *1991*
- *1990*

Informativa ai sensi del D.Lgs. 196/2003 – Codice in materia di protezione dei dati personali e del Regolamento Ue 2016/679 - GDPR General Data Protection Regulation

Con riferimento a quanto previsto dall'art. 13 del D. Lgs. n. 196/03 e al Regolamento Europeo 2016/679, recanti disposizioni a tutela della riservatezza nel trattamento dei dati personali, desideriamo fornirLe le seguenti informazioni:

1) Finalità del trattamento: i dati personali sono trattati al fine di provvedere analisi statistiche in ambito accademico.

2) Modalità del trattamento: il trattamento dei dati personali avviene mediante strumenti informatici, con logiche strettamente correlate alle finalità sopra indicate e, comunque, in modo da garantire la sicurezza dei dati stessi. I dati verranno trattati in forma aggregata e pertanto le informazioni raccolte sono totalmente anonime.

3) Conferimento dei dati: per le finalità indicate, il trattamento dei dati non è di natura obbligatoria, pertanto un Suo rifiuto al trattamento dei dati non comporta alcuna conseguenza.

4) Diritti dell'interessato: l'interessato ha il diritto di conoscere quali dati personali siano registrati, la loro origine e le finalità del trattamento; ottenere la cancellazione dei dati trattati in violazione di norme nonché la rettifica o l'integrazione dei dati; opporsi in tutto o in parte a trattamenti illegittimi dei dati; opporsi al trattamento dei dati per fini di informazione commerciale, invio di materiale pubblicitario, vendite dirette, comunicazione commerciale interattiva.

5) Titolare del trattamento: il titolare del trattamento dei dati è Miriam Battistella, 848496@stud.unive.it

5.4.5
Analisi dei dati

Trattandosi di una ricerca di tipo quantitativo, l'analisi dei dati non ha avuto come obiettivo la definizione di nuovi concetti già presenti nelle domande, ma è servita a misurare le alcune variabili e trovare delle relazioni fra queste.
Le informazioni presenti all'interno dei questionari raccolti sono state ordinate in una matrice dati, in cui sono state misurate le frequenze di risposta per ciascuna delle singole domande, al fine di descrivere l'andamento dei fenomeni osservati. La matrice è stata costruita ordinando i questionari in colonne numerate in ordine crescente e le opzioni di risposta in righe, rapprensentanti le variabili di ricerca.
In totale sono stati raccolti 202 questionari, dai quali è stata fatta una prima pulizia dei dati volta a correggere le risposte ritenute non valide per l'interpretazione dei dati. Sono stati eliminati così cinque questionari perfettamente identici e raccolti consecutivamente, ipotizzando che ci potesse esser stato un errore di sistema. Nel corso dell'analisi dei dati sono state fatte altre correzioni, che hanno comportato l'annullamento di alcune risposte e delle riqualificazioni delle opzioni scelta.
Le domande "Conoscevi la notizia citata?" e "Qual è stata la tua prima reazione alla notizia?" hanno raccolto il maggior numero di risposte non valide. In questo caso infatti, la risposta "No, per niente" alla prima domanda, comportava la scelta dell'opzione "Non conoscevo il caso" nella seconda. Le risposte annullate per questa ragione sono state circa una decina in tutto.
Ulteriori considerazioni sono state fatte nelle domande "Come reagisci solitamente alla richiesta di amicizia di uno sconosciuto?" e "Dopo quanto avvenuto, è cambiato il tuo modo di usare Facebook?", in cui è stato rilevato un alto tasso di scelta dell'opzione "altro". Le affermazioni fatte in questo caso sono state raccolte in un foglio a parte, con lo scopo di analizzare separatamente le tutte le valutazioni fatte dai rispondenti e interpretare in modo omogeneo i fenomeni trattati.
Dalla matrice dei dati aggiustati è stato realizzato il conteggio totale delle risposte date per ciascuna opzione, da cui è stato possibile calcolare le percentuali di scelta per ogni domanda, in base al numero di responsi ritenuti validi. Il calcolo delle

frequenze della matrice dei dati aggiustata ha permesso un primo studio della dispersione delle risposte date, con cui sono stati individuati i casi in cui il comportamento medio non è stato determinante nelle considerazioni successive, perchè non generalizzabile al campione considerato.
Dalla prima fase di analisi delle risposte raccolte dai questionari è stato possibile definire cinque categorie di ricerca, corrispondenti a i fenomeni più significativi presi in considerazione dall'indagine, tra cui:

- la visibilità e il controllo delle informazioni condivise su Facebook;
- i sistemi di tutela dei dati caricati nella piattaforma;
- gli effetti del datagate Facebook e Cambridge Analytica;
- la presenza del privacy paradox nei comportamenti rilevati;
- l'esistenza di una brand loyalty a Facebook.

Tali concetti sono stati analizzati partendo dalla mera osservazione dei risultati raccolti dai dati primari, senza alcuna valutazione sulle possibili relazioni tra le variabili presenti. Quest'ultima fase è stata fatta invece in un secondo momento, dedicato alla verifica delle ipotesi assunte in precedenza. Gli stessi concetti considerati per la definizione delle categorie di analisi, sono stati infatti ripresi e valutati in modo più approfondito, con una comparazione diretta di alcune variabili. In questo modo è stato possibile verificare la presenza delle ipotesi formulate prima della realizzazione dell'indagine, in base a quanto dedotto dalla letteratura riguardante la gestione delle informazioni e il privacy paradox.
Nello studio dei primi due concetti sono state prese in considerazione le variabili presenti nel modello di ricerca realizzato dallo studio di Young e Quan-Haase nel 2013. In questa prima dimensione del questionario è stata così verificata l'assenza di una possibile relazione tra le variabili relative alla tutela delle informazioni online e quelle riguardanti la loro esposizione agli altri utenti iscritti al social network. Una seconda analisi è stata fatta per individuare l'esistenza di due modelli comportamentali, relativi a una maggiore o minore propensione alla condivisione di informazioni personali online e al controllo della sicurezza dei dati messi in rete. Infine i risultati delle prime due categorie di ricerca sono stati comparati con quelli

ottenuti dall'indagine del 2013 allo scopo di individuare possibili analogie e differenze con quanto studiato cinque anni prima.

Il terzo concetto preso in considerazione è stato esaminato in base alle domande presenti nella seconda parte del questionario. Questo in quanto la categoria di ricerca relativa al caso Facebook e Cambridge Analytica, è stata trattata solo in quella sezione. Nella verifica delle ultime due nozioni invece, è stata fatta una valutazione più ampia, che ha coinvolto in modo trasversale diverse dimensioni del questionario. Le risposte raccolte sono state dunque analizzate in modo omogeneo, al fine di ottenere un'osservazione complessiva del tema tratto.

Nel complesso l'indagine ha avuto lo scopo di verificare alcuni concetti già trattati dalla letteratura considerata, definendo il comportamento degli iscritti a Facebook dopo il datagate in cui è stato coinvolto e individuando gli elementi critici nel rapporto tra utenti e aziende nelle attività di data retention e data mining. L'analisi delle relazioni presenti tra le diverse variabili del questionario ha permesso di verificare quanto considerato nella letteratura di riferimento. La ricerca costituisce dunque una panoramica completa sulle caratteristiche comportamentali dell'uso dei social media e della condivisione di dati personali in Facebook.

Capitolo 6
Risultati della ricerca empirica

6.1
Le categorie di analisi

Al termine della raccolta dei dati primari, avvenuta con la compilazione di circa duecento questionari, sono state individuate ed eliminate le risposte non valide. Le informazioni raccolte sono state poi ordinate in una matrice dei dati. Successivamente, è stata effettuata un'analisi dei dati composta da due fasi distinte: una prima dedicata al conteggio delle risposte, utile alla definizione dei trend più significativi della ricerca e una seconda fase di comparazione dei risultati ottenuti dalle domande poste nelle tre diverse sezioni presenti nel questionario.
Nella prima fase si è provveduto a fare un primo conteggio del numero di volte in cui sono state scelte le varie opzioni per ogni quesito trattato dal questionario. Le frequenze sono state rese in percentuale, considerando il numero di risposte ritenute valide per ogni domanda. Questo tipo di analisi è stato svolto parallelamente all'interpretazione delle affermazioni rilasciate nelle opzioni "altro", presenti in alcune domande del questionario. Lo studio delle frequenze ha permesso di realizzare l'analisi preliminare di alcuni fenomeni chiave della ricerca. La definizione di tali categorie di studio è stata di fondamentale importanza per una prima descrizione dei comportamenti espressi dal campione, dunque anche per la successiva verifica delle ipotesi poste dalla ricerca.
Il calcolo delle frequenze ha permesso la definizione di cinque concetti di base, ovvero: il grado di visibilità del proprio profilo Facebook, l'interesse per la tutela dei proprio dati personali nel sito, l'impatto del caso Cambridge Analytica, la presenza del privacy paradox e il grado di fidelizzazione al social. Tali astrazioni sono state identificate in base alla domanda di ricerca e alla letteratura trattata.

La definizione delle cinque categorie di ricerca ha permesso di svolgere una prima interpretazione delle risposte del questionario, le quali sono state trattate in cinque gruppi di studio diversi, rappresentanti dei concetti chiave della ricerca. Questa fase è stata realizzata con l'osservazione dei trend comportamentali rilevati dal calcolo percentuale delle frequenze di risposta e dal raggruppamento delle domande aventi una tematica comune. In questo modo sono stati osservati gli elementi più significativi della ricerca, consentendo di descrivere dettagliatamente solo i fenomeni più importanti rilevati dall'indagine.

Nella seconda parte dell'analisi dei dati primari, i concetti delineati dall'osservazione precedente sono stati ripresi e approfonditi, allo scopo di effettuare la verifica delle ipotesi. Analogamente a quanto avvenuto per lo studio delle categorie di analisi, anche in questa fase le risposte raccolte dai questionari sono state esaminate aggregando le domande aventi delle tematiche comuni. Tuttavia, la verifica delle ipotesi non è stata affrontata con la mera osservazione delle frequenze di risposta, ma piuttosto con un confronto diretto, volto a individuare delle possibili relazioni tra variabili. Infine lo studio dei dati primari si è concluso con la puntualizzazione di ulteriori fenomeni emersi dalla ricerca e non direttamente trattati né dalle categorie di analisi, né dalla verifica delle ipotesi.

6.1.1
Visibilità delle informazioni condivise su Facebook

Le prime categorie di analisi considerate sono state la visibilità delle informazioni condivise nel profilo Facebook e le modalità di tutela dei dati caricati nel social network. Tali concetti, presenti nella prima parte del questionario, sono stati ripresi dalla ricerca "Privacy protection strategies on Facebook" svolta nel 2013 da Young e Quan-Haase, relativa allo studio del privacy paradox tra gli iscritti alla piattaforma. Tali categorie sono state posizionate nella prima parte del questionario, allo scopo di introdurre l'argomento della privacy in Facebook, rilevando da subito il comportamento di utilizzo abituale della piattaforma negli

negli ultimi due anni, ed evitando riferimenti al caso Cambridge Analytica. Quest'ultimo invece, è stato analizzato nella seconda parte dell'indagine, con lo scopo di individuare quali conseguenze ha avuto nella normale gestione del profilo.
Il concetto di visibilità dei dati personali condivisi in Facebook consiste nella propensione che hanno gli iscritti al social network, a pubblicare informazioni personali all'interno della proprio profilo. Facebook permette ai propri utenti di scegliere a chi destinare quanto condiviso online, creando diversi livelli di visibilità, selezionabili in base alle proprie comunità d'interesse o nello specifico, permettendo all'utente di includere o escludere dei singoli profili. Generalmente tali impostazioni riguardano sia il profilo complessivo dell'utente, che i singoli contenuti condivisi dalla persona (post, foto, notizie, ecc), dei quali può scegliere se pubblicarli con una visibilità pubblica oppure limitata alla sola cerchia di amici.
Nella prima parte del questionario somministrato al campione, il tema della visibilità delle informazioni personali condivise in Facebook è stato trattato in sei domande, di cui una a risposta singola chiusa, tre a risposta multipla e due con griglie di valutazione. Nel complesso gran parte dei partecipanti coinvolti nella ricerca, ha dimostrato di essere consapevole delle scelte sulla visibilità delle proprie informazioni personali e dei contenuti condivisi nel proprio profilo Facebook. Il principale trend riscontrato in questa parte della ricerca, consiste infatti nella gestione attiva e consapevole delle pubblicazioni effettuate dagli iscritti, che solitamente preferiscono limitare alla sola cerchia di amici la condivisione di informazioni personali. Ciò è stato riscontrato in particolare nelle domande 6, 9 e 12.

6. Qual è il grado di visibilità del tuo profilo Facebook?

● *Il profilo è visibile nei motori di ricerca esterni a Facebook*	*8*	*4%*
● *Il profilo è visibile da chiunque sia iscritto a Facebook*	*28*	*14%*
● *Il profilo è visibile solo dagli amici degli amici*	*31*	*16%*
● ***Il profilo è visibile solo ai miei amici***	***117***	***59%***
● *Non lo so*	*13*	*7%*
● *Altro*	*0*	*0%*

9. Quali impostazioni dei tag e del diario hai modificato negli ultimi due anni?

- *Chi può scrivere sul mio diario* *54* *28%*
- ***Chi può vedere cosa pubblicano sul mio diario*** ***105*** ***54%***
- *Chi può vedere i post in cui sono taggato* *86* *44%*
- ***Il controllo dei post in cui sono taggato prima che vengano pubblicati nel mio diario*** ***101*** ***52%***
- *Nessuna delle precedenti* *42* *21%*
- *Altro* *0* *0%*

12. Quali altre informazioni sei disposto a condividere in Facebook?

	Solo io		***Visibilità limitata (amici)***		*Visibilità aperta*		*Non lo so*	
Foto in cui sei taggato	***5***	***3%***	***171***	***87%***	***20***	***10%***	***1***	***1%***
Video in cui sei taggato	***6***	***3%***	***173***	***88%***	***15***	***8%***	***3***	***2%***
Post pubblicati	*0*	*0%*	***168***	***85%***	*27*	*14%*	*2*	*1%*
Amici	*22*	*11%*	***105***	***53%***	*68*	*35%*	*2*	*1%*
Interessi	*10*	*5%*	***130***	***66%***	*55*	*28%*	*2*	*1%*
Informazioni personali	*22*	*11%*	***124***	***63%***	*48*	*24%*	*3*	*2%*
Dati anagrafici	*43*	*22%*	***119***	***60%***	*33*	*17%*	*2*	*1%*

Lo studio di quest'ultima matrice ha comportato anche la realizzazione di una scala quantitativa, per la quale è stata fatta una gradazione numerica delle opzioni di risposta a disposizione del campione. Nel conteggio si è cercato dunque di assegnare un voto da uno a tre al livello di protezione dichiarato da ogni individuo, per la condivisione di informazioni personali in Facebook.

I dati raccolti sono stati quindi interpretati come:

- Solo io: 3
- Visibilità limitata: 2
- Visibilità aperta: 1
- Non lo so: sono stati esclusi dal conteggio.

	Media	*Deviazione standard*
1. Foto in cui sei taggato	*1,9235*	*0,3497*
2. Video in cui sei taggato	*1,9536*	*0,3266*
3. Post pubblicati	*1,8615*	*0,3463*
4. Amici	***1,7641***	***0,6387***
5. Interessi	***1,7692***	***0,5306***
6. Informazioni personali	*1,8608*	*0,5814*
7. Dati anagrafici	***2,0256***	***0,6212***

Dal confronto dei risultati ottenuti dalle domande 6 e 9 è chiaro come esista un interesse effettivo al controllo delle informazioni condivise nel proprio profilo e in particolare di chi ne può avere accesso. Dai risultati raccolti dalla domanda 6, si evince come più della metà del campione abbia scelto di limitare la visibilità del proprio profilo alla sola cerchia di amici iscritti al social, mentre solo il 7% degli individui non saprebbe definire il livello di esposizione che ha nella piattaforma. Dei risultati simili si erano ottenuti con la stessa domanda posta nel 2013, dalla ricerca "Privacy protection strategies on Facebook", usata come modello per la redazione della prima parte del questionario. Il 71% degli studenti coinvolti nel campione di allora, dichiarava infatti di aver limitato la visibilità del proprio profilo ai soli amici, mentre rispettivamente il 14% e l'8% non aveva fatto alcuna modifica alle impostazioni di default o aveva reso la sua pagina visibili online.

L'importanza della visibilità del profilo Facebook è stata rilevata anche nella domanda successiva, per cui il 21% degli utenti coinvolti nel campione ha dichiarato di non aver apportato alcuna modifica alle impostazioni di tag e di diario presenti nella piattaforma negli ultimi due anni di utilizzo. Dai risultati raccolti in questa domanda, si evince inoltre che per la maggioranza dei soggetti coinvolti nella ricerca, i contenuti postati da altri all'interno del proprio profilo personale costituiscono degli elementi critici nella gestione delle informazioni all'interno della piattaforma. Più della metà degli intervistati infatti, ha dichiarato di aver fatto delle modifiche alle impostazioni sul controllo della visibilità dei contenuti pubblicati da altri utenti nella propria pagina Facebook, impostando un sistema di

approvazione che anticipa la condivisione definitiva. Lo stesso comportamento è stato verificato anche nei risultati della griglia di valutazione della domanda 12. I soggetti coinvolti nella ricerca hanno dimostrato di essere meno propensi a rendere pubblici i contenuti multimediali condivisi da altri sul loro profilo, registrando in "foto in cui sei taggato" e "video in cui sei taggato" rispettivamente l'87% e l'88% di preferenze per l'opzione "visibilità limitata". Ciò dimostra come il principio consensuale, abbia una profonda importanza per la maggioranza degli utenti, anche nel caso in cui i dati siano trattati da individui inclusi nelle proprie cerchie sociali, con funzioni che lo stesso social network permette.

Il trattamento dei dati svolto nella griglia di valutazione della domanda 12 ha permesso di individuare un secondo fattore a cui gli utenti fanno particolarmente attenzione nella gestione della visibilità dei propri dati online. Una delle medie più alte registrate nella fase di valutazione dei risultati è stata infatti quella relativa ai "Dati anagrafici", l'unica ad aver effettivamente raggiunto e superato il valore di 2. Questo dato dimostra come le informazioni di base per l'identificazione della persona siano state ritenute le più riservate dagli intervistati, quindi anche le più meritevoli di tutela, rispetto a un potenziale accesso pubblico, permesso dalla piattaforma. In questo caso tuttavia, è importante considerare anche il valore della deviazione standard, che segnala un'ampia dispersione dei dati raccolti.

Infine, sempre in base al calcolo delle medie effettuato nella griglia di valutazione della domanda 12, è da segnalare come le voci che hanno ottenuto un punteggio minore siano state "Amici" e "Interessi", per cui il campione sembra dimostrare una maggiore propensione a rendere note tali informazioni, anche verso terzi non direttamente coinvolti nelle proprie cerchie sociali.

La gestione dei dati personali condivisi da altri utenti è stata ripresa nelle domande 8, 10 e nella griglia di valutazione della domanda 13.

8. Quali limiti hai utilizzato verso altri utenti negli ultimi due anni?

- *Ho limitato la visibilità dei miei post ad alcuni amici* *78* *40%*
- ***Ho bloccato alcuni utenti*** ***107*** ***54%***
- *Ho bloccato i messaggi provenienti da alcuni utenti* *66* *34%*
- ***Ho bloccato gli inviti alle applicazioni provenienti da alcuni utenti*** ***94*** ***48%***

- *Ho bloccato gli inviti agli eventi provenienti da alcuni utenti* *42* *21%*
- *Ho bloccato alcune applicazioni* *82* *42%*
- *Ho bloccato delle pagine* *45* *23%*
- *Nessuna delle precedenti* *31* *16%*
- *Altro* *0* *0%*

10. Come reagisci solitamente alla richiesta di amicizia di uno sconosciuto?

- ***Ignoro la richiesta*** ***112*** ***57%***
- *Nego la richiesta* *90* *46%*
- *Accetto la richiesta per avere più informazioni sulla persona* *15* *8%*
- *Segnalo l'utente* *2* *1%*
- *Blocco l'utente* *4* *2%*
- ***Altro*** ***18*** ***9%***

13. Quali di queste soluzioni hai adottato per tutelare la tua privacy?

	1 (mai)	*2*	*3*	*4*	*5 (molto spesso)*	*Media*	*Deviazione standard*
1. Uso i messaggi privati al posto di commenti pubblici	*32 16%*	*46 23%*	*52 26%*	*17 9%*	*50 25%*	*3,0355*	*1,4120*
2. Ho cambiato le opzioni sulla privacy nel mio profilo	*20 10%*	*37 19%*	*65 33%*	*34 17%*	*41 21%*	*3,1980*	*1,2521*
3. Limito le informazioni personali condivise	***9 5%***	***21 11%***	***76 39%***	***26 13%***	***65 33%***	***3,5939***	***1,1813***
4. Limito l'uso dei tag	*38 19%*	*44 22%*	*49 25%*	*23 12%*	*43 22%*	*2,9441*	*1,4120*
5. Ho eliminato alcuni post	*45 23%*	*41 21%*	*52 26%*	*22 11%*	*37 19%*	*2,8223*	*1,4011*
6. Ho limitato la visibilità del mio profilo a terzi	***19 10%***	***21 11%***	***74 38%***	***26 13%***	***57 29%***	***3,4111***	***1,2731***
7. Ho bloccato alcuni utenti	*62 31%*	*44 22%*	*52 26%*	*18 9%*	*21 11%*	*2,4518*	*1,3070*
8. Uso informazioni false per evitare un'eccessiva esposizione	***166 84%***	***14 7%***	***11 6%***	***1 1%***	***5 3%***	***1,2994***	***0,8123***

Queste ultime tre domande sono state analizzate insieme, allo scopo di permettere una piena comprensione dell'abituale gestione della visibilità della rete relazionale costruita dagli utenti di Facebook. Le domande 8 e 10 in particolare, sono state direttamente confrontate sulla possibilità di blocco permessa dalla piattaforma, da un profilo verso terzi utenti, a cui si vuol impedire qualsiasi tipo di accesso a informazioni personali. Oltre la metà dei rispondenti, ha infatti dichiarato di aver bloccato altri utenti negli ultimi due anni. Ciò è avvenuto nella maggioranza dei casi, all'interno di cerchie sociali conosciute dall'individuo, in quanto solo il 2% degli individui ha dichiarato di aver reagito a una richiesta di uno sconosciuto bloccandogli il profilo.

Il blocco del profilo e quello degli inviti di partecipazione a nuove applicazioni sono gli strumenti di limitazione più utilizzati dagli intervistati. Solo il 16% ha dichiarato di non aver utilizzato alcuna impostazione di limite verso altri utenti o pagine presenti nel social network nel corso degli ultimi due anni. Tali scelte rappresentano una sorta di correzione e gestione attiva delle modalità con cui terzi possono contattare un profilo oppure avere accesso a informazioni personali. I limiti imposti in modo mirato a singoli profili, servono a definire dettagliatamente le modalità di comunicazione e visibilità che l'individuo vuole avere nella piattaforma, per le quali non bastano le semplici impostazioni di base.

Le risposte alla domanda 10 sono invece una chiara conferma del trend riscontrato nella domanda 6. Circa la metà degli intervistati dichiara infatti di reagire alla richiesta di amicizia di uno sconosciuto ignorandola, oppure negandola. Così facendo, gli individui evitano di condividere informazioni personali con soggetti che non conoscono, limitando la visibilità dei contenuti ai soli amici. Solo 8% ha infatti dichiarato di accettare l'amicizia di uno sconosciuto per avere più informazioni sulla persona, mentre il 9% ha scelto l'opzione "Altro", spiegando di affidarsi ad amici o allo stesso social per avere più informazioni a riguardo.

Infine, dalla griglia di valutazione della domanda 13 si evince come esista una distribuzione bimodale delle frequenze relative alle varie attività di controllo della privacy e della visibilità, a esclusione dell'ultima opzione "Uso informazioni false per evitare un'eccessiva esposizione". La media delle risposte tende dunque ad aggirarsi su di un valore di 3, mentre in ogni sezione esistono solitamente due o più

picchi significativi. Nelle sezioni "uso i messaggi privati al posto di commenti pubblici", "ho cambiato le opzioni sulla privacy nel mio profilo", "limito le informazioni personali condivise" e "ho limitato la visibilità del mio profilo a terzi" prevalgono infatti i voti 3 e 5. In "limito l'uso del tag" e "ho eliminato alcuni post" il trend prevalente è meno evidente, considerando l'ampia distribuzione delle risposte. Infine in "ho bloccato alcuni utenti" e "uso informazioni false per evitare un'eccessiva esposizione" sono le risposte che hanno ottenuto un valore medio più basso. Nell'ultima sezione in particolare, è stata registrata una forte concentrazione sul volto 1, che ha ottenuto l'84% delle risposte.

Nel complesso dalla matrice si evince come la maggioranza degli utenti preferisca agire preventivamente per ridurre la propria esposizione in Facebook, limitando le informazioni condivise nel proprio profilo personale e in quello dei propri amici. I valori maggiori sono stati riscontrati nelle voci "Limito le informazioni personali condivise" e "Limito l'uso dei tag". La stessa matrice sarà ripresa anche per la valutazione della protezione della privacy all'interno del social network.

6.1.2
Protezione della privacy su Facebook

Nella seconda categoria di analisi è stata considerata la protezione della privacy su Facebook, intesa come le tecniche adottate dagli iscritti per evitare possibili accessi non autorizzati nel proprio profilo o l'uso ingiustificato di dati personali svolto da altre società. Il tema già precedentemente annunciato, pone un confronto tra il grado di visibilità che gli utenti vogliono ottenere dal proprio profilo Facebook e il loro interesse a evitare situazioni rischiose per la propria privacy, quali ad esempio furti e usi impropri di dati personali o possibili cyber attacchi.

Le domande relative a questa tematica sono state stilate prendendo il modello elaborato dalla ricerca "Privacy protection strategies on Facebook" svolta nel 2013 da Young e Quan-Haase nel 2013. Il tema è stato trattato insieme alle domande sulla visibilità delle informazioni personali in Facebook, nella prima parte del

questionario, seguendo la logica della categoria analizzata precedentemente. I punti che riprendono l'argomento della privacy sono presenti nelle domande chiuse 7 e 11 e in parte delle griglie di valutazione delle domande 12 e 13.

Partendo dalle valutazioni dei risultati ottenuti delle domande 12 e 13, si evince come il normale comportamento dei soggetti coinvolti nella ricerca, rispecchi le caratteristiche di utilizzo dei social network, descritte dalla letteratura. Gli individui infatti, hanno dichiarato una loro piena volontà di condividere informazioni veritiere sulla loro identità all'interno della piattaforma, sapendo che quanto pubblicato ha un riscontro reale nella propria cerchia sociale. Per questo motivo l'84% del campione ha dichiarato di non aver mai utilizzato delle informazioni false per evitare un'eccessiva esposizione all'interno della piattaforma. Il comportamento tendenzialmente adottato dal campione è piuttosto caratterizzato dall'omissione delle informazioni sensibili nel proprio profilo social, al quale si somma la gestione delle impostazioni sulla privacy.

La stessa griglia di valutazione della domanda 13, ebbe degli esiti del tutto simili nel 2013, nella ricerca "Privacy protection strategies on Facebook", usata come modello di base per il questionario. Anche in quel caso venne dimostrato come la maggioranza degli utenti tendesse a tutelare la propria privacy limitando la condivisione di informazioni nel proprio profilo personale e agendo sulle impostazioni di sicurezza offerte dal sito. Le sezioni "ho bloccato alcuni utenti" e "uso informazioni false per evitare un'eccessiva esposizione" ottennero delle votazioni medie di 2,91 e 1,66, registrando anche in quel caso, dei risultati minori rispetto a quanto registrato nelle altre sezioni.

Per quanto le impostazioni sulla privacy rappresentino uno dei mezzi per il controllo della propria sicurezza online, la gestione di questi strumenti non fornisce delle soluzioni realmente efficaci per la tutela dei dati. Tale affermazione è verificabile secondo quanto rilevato delle domande 7 e 11.

7. Quali impostazioni della privacy hai modificato negli ultimi due anni?

- ***Chi può vedere i tuoi post*** ***151*** ***77%***
- ***Chi può vedere i post in cui sei taggato*** ***114*** ***58%***
- *Chi può inviarti richieste di amicizia* *41* *21%*

- *Chi può vedere la lista dei tuoi amici* *56* *29%*
- *Chi può cercarti utilizzando l'indirizzo mail che hai fornito* *83* *42%*
- *Chi può cercarti utilizzando il numero di telefono che hai fornito* *90* *46%*
- *Nessuna delle precedenti* *26* *13%*
- *Altro* *1* *1%*

11. Quali impostazioni di sicurezza hai attivato per tutelare il tuo profilo?

- *Modifico spesso le password* *28* *14%*
- *Uso le autenticazioni a due fattori (password + codice da mobile)* *28* *14%*
- ***Ricevo avvisi dagli accessi sconosciuti*** ***108*** ***55%***
- *Ho scelto degli amici da contattare nel caso non riuscissi ad accedere al mio profilo* *29* *15%*
- ***Nessuna delle precedenti*** ***68*** ***35%***
- *Altro* *0* *0%*

Uno dei dati più significativi sulla tutela della privacy è rappresentato dalle frequenze calcolate per le risposte della domanda 11. Il 35% degli utenti coinvolti nella ricerca ha infatti dichiarato di non aver inserito alcuna impostazione per la sicurezza del proprio profilo. Gli individui dimostrano invece di aver fiducia nel sistema di gestione delle informazioni del sito, per cui il 55% degli utenti ha dichiarato di far affidamento alla ricezione di avvisi in caso di accessi sconosciuti. Solo il 15% si affida invece ai propri contatti nel caso ci fossero dei problemi di accesso al profilo, mentre il 14% si affida rispettivamente alla modifica delle password e all'autenticazione a due fattori.

Infine anche nella gestione della privacy per l'accesso e la gestione del proprio profilo personale, i contenuti pubblicati all'interno del diario, rappresentano gli elementi più importanti di gestione per gli individui coinvolti nel campione. Il 77% degli utenti ha infatti dichiarato di aver fatto delle modifiche recenti alla sola visibilità dei post condivisi, mentre il 58% si è concentrato sui tag caricati dagli altri nel suo profilo. Oltre il 40% dei rispondenti ha fatto delle modifiche relative all'esposizione di dati personali riguardanti altri mezzi di comunicazione potenzialmente accessibili da terzi, quali il numero di telefono e la mail. Tali strumenti rappresentano infatti dei dati sensibili per gli iscritti al social network,

che legano il profilo Facebook a un sistema identitario digitale più ampio, relativo alle scelte di utilizzo e consumo di servizi digitali della persona (es. operatore telefonico e di posta elettronica).

6.1.3
Impatto del caso Facebook e Cambridge Analytica

In base alla domanda di ricerca posta dall'indagine, nel questionario è stata inserita una sezione interamente dedicata al caso Facebook e Cambridge Analytica con l'obiettivo di analizzare gli effetti che la vicenda ha avuto sull'abituale uso del social. L'argomento è stato introdotto con una breve presentazione dei fatti, da cui sono state sviluppate cinque domande volte a individuare il punto di vista degli iscritti al sito e le loro prime reazioni. Il caso Facebook e Cambridge Analytica è stato considerato particolarmente significativo per lo studio del privacy paradox in quanto consiste nel più importante attacco realizzato finora, contro uno dei social network più diffusi al mondo. L'evento ha infatti palesato i rischi della condivisione di dati sensibili online, diffondendo un senso di incertezza anche verso i siti web. La raccolta dei dati primari è avvenuta tra maggio e giugno del 2018, dunque a solo un paio di mesi dalla diffusione della notizia e nel corso dell'entrata in vigore della nuovo regolamento europeo per la protezione dei dati (GDPR).

15. Conoscevi la notizia citata?

- *Sì, ho letto qualche articolo* — *85* — *47%*
- ***Sì, ne ho sentito parlare*** — ***92*** — ***51%***
- *No, per niente* — *5* — *3%*

16. Qual è stata la tua prima reazione alla notizia?

- *Interesse: ho cercato di approfondire la notizia* — *55* — *30%*
- ***Stupore: mi ha colpito ma non ho approfondito l'argomento*** — ***94*** — ***52%***
- *Indifferenza: non credo che sia un fatto particolarmente importante* — *28* — *15%*
- *Non conoscevo il caso* — *5* — *3%*

17. Dopo quanto avvenuto, è cambiato il tuo modo di usare Facebook?

● *Intendo eliminare il mio account Facebook*	*2*	*1%*
● *Ho fatto delle modifiche alla gestione dei miei dati personali*	*46*	*23%*
● ***Uno Facebook come prima***	***120***	***61%***
● *Ho iniziato a usare di più altri social a cui sono iscritto*	*20*	*10%*
● *Altro*	*9*	*5%*

18. A quali altri social network sei iscritto?

● ***Youtube***	***114***	***58%***
● *Twitter*	*69*	*35%*
● ***Instagram***	***172***	***87%***
● *Google +*	*63*	*32%*
● *LinkedIn*	*67*	*34%*
● *Pinterest*	*68*	*35%*
● *Snapchat*	*44*	*22%*
● *VERO*	*4*	*2%*
● *Nessuno delle precedenti*	*7*	*4%*
● *Altro*	*4*	*2%*

19. Credi una cosa simile possa ripetersi in futuro?

● ***Sì***	***156***	***79%***
● *No*	*4*	*2%*
● *Non so*	*37*	*19%*

Da quanto emerge dai risultati dei questionari, la maggioranza degli individui coinvolti nel campione conosceva la notizia in questione, in parte per passaparola e in parte informandosi presso qualche agenzia di stampa. Il 30% ha dimostrato un profondo interesse per l'argomento, dichiarando di aver approfondito la notizia, mentre, oltre la metà degli individui ne è rimasta semplicemente stupita.

Nonostante l'ampia diffusione della notizia e l'impatto emotivo che ha suscitato, il fatto in questione non ha prodotto un immediato cambiamento nell'abituale utilizzo del social network. Il 61% ha infatti affermato di utilizzare la piattaforma come prima. Solo il 23% del campione considerato, ha deciso di intervenire apportando delle modifiche alle proprie impostazioni sulla privacy. Nelle opzioni

"Altro" della domanda 17, sono state raccolte alcune valutazioni sulla generale percezione che gli utenti hanno verso il social network. Tali affermazioni sono servite a chiarire in modo esaustivo la posizione di molti utenti sul caso analizzato e più in generale sul social network, fornendo una valutazione complessiva sul grado di soddisfazione dei soggetti contattati.

"Ero tutto meno che stupito dalla notizia, avevo già notato in passato alcuni post sponsorizzati che non sarebbero dovuti esser nel mio facebook, per cui avevo già modificato il mio modo di usarlo"
"Mi ero già tolta da Facebook diversi anni fa ma per necessità pratiche ho dovuto iscrivermi nuovamente"
"Tengo in sospeso le nuove richieste sulla privacy che sono emerse dopo questo caso"
"Penso sia ormai un social obsoleto, ricco di pubblicità e poco accattivante, e per questo ne limito l'uso"
"Uso di meno la piattaforma ma ciò non dipende solamente dalla notizia"
"Quando non mi sarà più di utilità per l'università, molto probabilmente eliminerò il profilo"

Dai commenti rilasciati in questa domanda, si evince come molti utenti non siano da tempo soddisfatti del servizio offerto da Facebook, ma che comunque non abbiano ancora deciso di eliminare il proprio profilo, sfruttando la piattaforma per restare in contatto con la propria rete sociale. La vicenda di Cambridge Analytica non risulta essere un motivo di svolta nella gestione dei dati personali online, tuttavia incrementa gli elementi di disagio percepiti dai membri della piattaforma. Ciò potrebbe nel lungo termine, incidere sul numero di iscritti a Facebook e sul grado di fidelizzazione di membri attuali, a favore di altri social network emergenti. Infine è stato riscontrato come il 79% degli individui contattati sia convinto che una fuga di dati simile a quella verificatasi nel caso Facebook e Cambridge Analytica possa avvenire anche in futuro. Il dato può essere interpretato come una piena consapevolezza dei continui rischi che la condivisione di dati online implica. Nel complesso, da quanto è emerso dai risultati della seconda sezione del questionario, la notizia del datagate Cambridge Analytica non ha avuto un impatto

concreto nella gestione delle impostazioni sulla cyber security, ma costituisce comunque un ulteriore elemento negativo del sito, capace di incrementare un senso di sfiducia verso i sistemi di tutela dei dati realizzati da Facebook..

6.1.4
Presenza del privacy paradox

Lo studio delle categorie di analisi è servito per verificare la presenza del privacy paradox nell'uso di Facebook. L'analisi della gestione dei termini di visibilità e di privacy nel social network ha rilevato l'esistenza un effettivo interesse nel controllo delle informazioni personali online e nella valutazione dei rischi dati dalla condivisione delle informazioni. Alcuni dei dati primari considerati nello studio del privacy paradox sono stati ricavati dalla domanda 14, relativa alla conoscenza del nuovo regolamento europeo sulla protezione dei dati e dalle domande presenti nella prima parte del questionario, già precedentemente trattate nelle prime tre categorie di analisi.

14. Ritieni che il nuovo regolamento europeo sulla protezione dei dati (GDPR) possa migliorare il trattamento delle tue informazioni personali online?

- *Credo possa migliorare il trattamento dei dati degli utenti* *38* *19%*
- *Credo non apporti alcuna modifica sostanziale a quanto già esistente* *35* *18%*
- *Credo rischi di essere un problema nell'uso della rete* *5* *3%*
- ***Non conosco la norma citata*** ***93*** ***47%***
- *Non lo so* *26* *13%*
- *Altro* *0* *0%*

In base a quanto esaminato dalle risposte della prima parte del questionario (6.1.1, 6.1.2), gli iscritti a Facebook sono consapevoli di quanto sia importante il controllo delle proprie informazioni online, tuttavia ciò realizzano nella realtà non corrisponde ai loro principi ideali. La maggioranza degli utenti coinvolti nel sondaggio ha dichiarato di non aver fatto alcuna modifica nell'utilizzo del sito

internet dopo il caso Cambridge Analytica, talvolta affermando di aver già fatto in passato delle modifiche ai termini di privacy presenti nel sito (6.1.3). La notizia non ha comunque motivato la maggioranza degli iscritti a revisionare le funzioni di gestione e controllo dei dati personali, presenti nella piattaforma.

Tale inerzia era stata inizialmente giustificata con l'ipotesi di un possibile senso di fiducia, percepito dagli utenti per le garanzie date dall'entrata in vigore del nuovo regolamento europeo sulla protezione dei dati (GDPR). Nel corso della distribuzione dei questionari, avvenuta a maggio 2018, Facebook, Google, Whatsapp e altri siti internet hanno informato i propri utenti sulle nuove norme per il trattamento dei dati online. La notizia dell'entrata in vigore del regolamento è stata ampiamente diffusa tramite notiziari nazionali, comunicazioni di posta elettronica e l'organizzazione di eventi, promossi anche dall'Università Ca' Foscari. Questo tuttavia, non ha impedito che il 47% del campione coinvolto, dichiarasse di non conoscere il nuovo regolamento europeo per la protezione dei dati (GDPR) negando l'ipotesi che l'immediata assenza di reazioni concrete al caso Cambridge Analytica, fosse dovuta a un senso di fiducia verso il nuovo ordinamento.

Infine riprendendo alcune domande presenti nella prima parte del questionario si evince come esista un interesse maggiore al controllo della visibilità delle informazioni caricate nella piattaforma verso gli altri iscritti, piuttosto che alla gestione delle modalità di accesso al profilo stesso e dunque al tema della tutela della privacy. Nella domanda 11 ad esempio, il 35% dei rispondenti ha dichiarato di non aver inserito nessuna delle impostazioni di sicurezza offerte dal sito per tutelare il proprio profilo personale. Al contrario nelle domande 8 e 9 solo il 20% degli utenti ha dichiarato di non aver posto dei limiti verso altri profili o modificato le impostazioni della visibilità dei tag e del diario, negli ultimi due anni.

Tale scarto percentuale, per quanto irrisorio, rappresenterebbe il segno di un maggiore interesse al controllo della propria immagine sociale all'interno del sito, piuttosto che della sicurezza dello stesso, confermando il trend rilevato nella ricerca "Privacy protection strategies on Facebook" di Young e Quan-Haase, usata come modello per la definizione della prima parte del questionario. Nella ricerca di allora, la raccolta di dati primari era stata effettuata sia tramite la somministrazione di questionari, che con la realizzazione di circa una trentina di

interviste. Proprio quest'ultime hanno evidenziato come gli utenti fossero molto più attenti alla dimensione sociale della condivisione, piuttosto che a quella istituzionale, definita dai sistemi sicurezza adottati a tutela delle loro informazioni. Anche in quel caso, gran parte degli intervistati affermò di proteggere la propria privacy, limitando la visibilità del profilo ai soli membri della propria cerchia sociale. La maggioranza degli studenti dichiarò inoltre, di non utilizzare altri altri sistemi di cyber security, volti a migliorare la tutela delle loro informazioni. L'indagine di Young e Quan-Haase rilevò infatti, che la principale preoccupazione dei soggetti coinvolti nel campione era costituita dall'accesso che i genitori potevano avere su foto e post da loro pubblicati. Per questa ragione, una delle strategie più usate dagli intervistati costituiva nell'eliminazione dei contenuti ritenuti meno opportuni per il loro contesto sociale di appartenenza.
Nonostante la raccolta di dati primari effettuata nel corso della ricerca, non abbia compreso la realizzazione di interviste, la questione della privacy è stata trattata con delle domande a risposta chiusa, che hanno determinato risultati analoghi, a conferma di quanto già analizzato dalla letteratura.

6.1.5
Brand loyalty a Facebook

La ricerca si è basata sull'analisi delle caratteristiche comportamentali degli utenti della rete, focalizzandosi in particolare sulla gestione dei propri dati personali all'interno di Facebook. Il social network ha avuto un ruolo fondamentale nella realizzazione e negli esiti complessivi dello studio. Per questa ragione è stato necessario considerare l'esistenza di una possibile brand loyalty degli iscritti alla piattaforma. Tale circostanza, se confermata avrebbe infatti inciso nelle abitudini di utilizzo del sito e nella gestione delle informazioni online. La valutazione del grado di fedeltà degli iscritti alla piattaforma è stata fatta considerando le normali tempistiche di utilizzo del social network, tra cui il tempo trascorso dall'iscrizione al sito, la frequenza di accesso e la durata di permanenza.

1. Da quanto tempo utilizzi Facebook?

- *Meno di 5 anni* *22* *11%*
- ***Dai 5 ai 10 anni*** ***163*** ***83%***
- *Oltre i 10 anni* *12* *6%*

2. Quante volte utilizzi Facebook?

- ***Più volte al giorno*** ***164*** ***83%***
- *Più volte alla settimana* *30* *15%*
- *Più volte al mese* *30* *2%*

3. Quanto tempo hai passato su Facebook la scorsa settimana?

- *Più di sei ore* *57* *29%*
- ***Più di tre ore*** ***94*** ***48%***
- *Qualche minuto* *46* *23%*

Dalle risposte raccolte si evince come l'uso di Facebook consista in un'abitudine comune tra gli intervistati, tanto da renderlo un motivo di accesso a internet. L'83% dei soggetti coinvolti nel campione ha dichiarato di esser registrato al sito da oltre cinque anni, mentre il 6% da anche più di dieci. Il lungo periodo d'iscrizione alla piattaforma da parte dei rispondenti al questionario, consiste nella prova della profonda dimestichezza che questi hanno del suo utilizzo e allo stesso tempo, li coinvolge negli eventi a cui si riferisce il caso di Cambridge Analytica. Per quanto riguarda la frequenza e la durata di navigazione invece, il trend indicato dalle risposte induce a supporre numerosi ma brevi accessi al social network, definendo l'uso di Facebook come un gesto quotidiano e ripetitivo.

Lo studio delle abitudini di utilizzo di Facebook ha infine comportato l'analisi delle reti sociali gestite dagli utenti nella piattaforma, nelle domande 5 e 4.

4. Quanti utenti sono registrati come amici sul tuo profilo Facebook?

Totale: 130998 *Media: 668*

5. Quanti di questi consideri davvero come tuoi amici anche nella vita reale?

Totale: 13766 *Media: 72*

In questo caso è possibile notare come Facebook permetta ai sui membri di gestire il rapporto con un numero di individui maggiore rispetto a quelli che normalmente concorrono nelle loro reali cerchie sociali. Mediamente solo il 9% degli utenti registrati come amici nel profilo personale, sono effettivamente considerati amici anche nella vita reale. Tale fattore consiste un elemento incisivo nell'analisi delle motivazioni d'uso del social network. Gli utenti intervistati infatti, non intendono abbandonare il sito o cambiare le loro abitudini di navigazione per mantenere le relazioni con gli altri iscritti. Tale concetto riprende il modello di sviluppo delle economie di rete a cui fanno riferimento tutti i social network, negando l'ipotesi di una possibile brand loyalty verso la piattaforma. A conferma di quanto esaminato in quest'ultima categoria di analisi, sono state riprese alcune affermazioni rilasciate nell'opzione "Altro" della domanda 17 (dopo quanto accaduto, è cambiato il tuo modo di usare Facebook?), riguardante il caso Cambridge Analytica, tra cui:

"Mi ero già tolta da Facebook diversi anni fa ma per necessità pratiche ho dovuto iscrivermi nuovamente"
"Quando non mi sarà più di utilità per l'università, molto probabilmente eliminerò il profilo"

6.2
Confronto con le ipotesi precedentemente formulate

Nella stesura del percorso di ricerca svolto per l'analisi del fenomeno del privacy paradox e per lo studio del caso Facebook e Cambridge Analytica, sono state fatte sette ipotesi sulle possibili risposte che si sarebbero ottenute dalla somministrazione dei questionari al campione di riferimento. Tali supposizioni sono state fatte in via preventiva allo scopo di verificare la presenza degli stessi comportamenti di utilizzo dei social network, già individuati nella letteratura di riferimento.
La verifica delle ipotesi ha comportato diversi riferimenti alle categorie di analisi delineate precedentemente e un ulteriore confronto tra i risultati ottenuti dalle

domande presenti nelle tre sezioni del questionario. Questo è avvenuto soprattutto nella fase iniziale dello studio delle ipotesi, per cui sono stati ripresi gli stessi temi di visibilità e privacy trattati dalle prime due categorie di analisi.

Dall'esame delle risposte, si assumeva di osservare una certa discrepanza tra i risultati relativi alle domande sulla visibilità dei dati nel social network e quelli riguardanti il tema della privacy. Nella prima ipotesi si affermava che il numero di modifiche fatte dagli utenti relativamente alle impostazioni sulla visibilità del proprio profilo personale, potessero essere maggiori di quelle sulla privacy a tutela dei dati condivisi nella piattaforma. Tale ipotesi è stata confermata con un confronto diretto delle risposte raccolte dalle domande presenti nella prima parte del questionario, e in particolare quelle comprese tra la 6 e la 12 (analizzate nei capitoli 6.1.1 e 6.1.2). Alla domanda 11 "quali impostazioni di sicurezza hai attivato per tutelare il tuo profilo?" il 35% degli individui scelto l'opzione "nessuna delle precedenti", dichiarando così di non aver effettuato alcun intervento a tutela della propria privacy, rispetto alle impostazioni presenti nel sito. Ciò si contrappone ai risultati ottenuti dalla stessa opzione di risposta delle domande sulla visibilità, come ad esempio "quali impostazioni dei tag e del diario hai modificato negli ultimi due anni?" oppure "quali limiti hai usato verso altri utenti negli ultimi due anni", che hanno ottenuto rispettivamente il 21% e il 16%.

Gli utenti coinvolti nell'indagine sono tendenzialmente coscienti del livello di visibilità dei contenuti condivisi, tanto che nella griglia di valutazione della domanda 12, solo 1% o il 2% dichiara di non sapere a chi sono visibili post, foto e video pubblicati nel proprio profilo personale. Tuttavia nella domanda 6, il 7% degli individui dichiara di non conoscere il grado di visibilità che ha l'intero profilo personale all'interno della rete web e della piattaforma. Nel complesso è comunque possibile affermare come l'interesse per la visibilità delle informazioni condivise in Facebook, sia maggiore di quello per la gestione della privacy e della sicurezza dei dati. Tale concetto conferma lo studio fatto nel 2013 da Young e Quan-Haase nella ricerca "Privacy protection strategies on Facebook", usata come modello di riferimento nella prima parte dell'indagine.

Nella seconda ipotesi posta dalla ricerca, il tema della visibilità e della privacy dei dati condivisi in Facebook, è stato trattato dalla domanda 11 e delle griglie di

valutazione delle domande 12 e 13. In questo caso si supponeva la presenza di un unico modello comportamentale per la gestione della sicurezza e due relativi alla visibilità delle informazioni condivise online.

Dai risultati ottenuti dalla domanda 11, è possibile confermare l'esistenza di un trend comportamentale uniforme nella gestione della privacy, basato su un senso di fiducia verso la piattaforma. Dall'analisi delle risposte si evince infatti l'assenza di un particolare interesse nel controllo della sicurezza dei propri dati online. Mediamente gli utenti hanno attivato una sola impostazione di sicurezza a tutela del proprio profilo personale, confermando la prima parte dell'ipotesi formulata.

Per quanto riguarda il controllo della visibilità, il modello comportamentale prevalente consiste nella limitazione della condivisione di informazioni personali alla sola cerchia di amici. Nonostante nella prima parte del questionario prevale l'esistenza di un unico atteggiamento di gestione della visibilità delle informazioni condivise sulla piattaforma, dalla griglia di valutazione della domanda 13 emergono dei tratti comportamentali diversi. Dalla valutazione dei voti assegnati per ogni sezione della tabella, è possibile evincere come non esita un voto prevalente sugli altri, ma piuttosto una distribuzione bimodale delle risposte. Questa tendenza già analizzata nella prima categoria di analisi, confermerebbe dunque parte dell'ipotesi relativa all'esistenza di due modelli comportamentali nella gestione della visibilità delle informazioni condivise in Facebook. Gli stessi modelli comportamentali sulla visibilità, rispecchierebbero inoltre una maggiore o minore attenzione alla tutela della sicurezza dei propri dati. Confrontando i voti della domanda 13 con le risposte registrate alla domanda 11, è possibile notare infatti, come chi ha dato un punteggio maggiore alla tabella ha anche fatto un numero maggiore di modifiche alle impostazioni sulla privacy.

N. modifiche delle impostazioni sulla privacy	*0*	*1*	*2*	*3*	*4*
Valutazioni medie dom. 13 maggiori di 3	*22* *25,9%*	***35*** ***41,2%***	***23*** ***27,1%***	*3,* *3,5%*	*2* *2,4%*
Valutazioni medie dom. 13 minori di 3	***46*** ***41,1%***	***34*** ***39,3%***	*16* *14,3%*	*6* *5,4%*	*0* *0,0%*

Per quanto rappresentino il segno di una lieve differenza comportamentale, i risultati registrati nella griglia di valutazione della domanda 13, non possono essere estesi all'intera valutazione della gestione della visibilità delle informazioni nella piattaforma. La domanda 13 infatti, si focalizza soprattutto sulle sole impostazioni a disposizione dell'utente, per il controllo della pubblicazione di alcuni contenuti specifici, come post, commenti, video e foto. Nelle domande comprese tra la 6 la 12, il tema della visibilità è trattato in modo più omogeneo, con dei riferimenti all'esposizione dell'intero profilo all'interno social network e nella rete. Dai risultati di queste ultime prevale invece un profilo comportamentale più omogeneo, che permette così di negare interamente la seconda ipotesi.

La terza, la quarta e la quinta ipotesi supponevano la presenza di un'ampia conoscenza della fuga di dati avvenuta da Facebook verso Cambridge Analytica, la quale tuttavia non avrebbe comportato un cambiamento nell'attuale uso della piattaforma o delle modifiche nella gestione delle informazioni condivise. Tale comportamento sarebbe stato rilevato sia nei soggetti particolarmente attenti alla tutela della loro privacy, che in quelli convinti di una possibile reiterazione futura dei fatti. Nella formulazione delle ipotesi, si supponeva che tale noncuranza verso la sicurezza dei dati, sarebbe stata giustificata da un senso di fiducia provato dagli utenti verso l'entrata in vigore del nuovo regolamento europeo sulla protezione dei dati (GDPR), avvenuta contemporaneamente alla raccolta dei questionari.

I risultati dei questionari raccolti hanno quasi interamente confermato quanto supposto dalle ipotesi formulate. La notizia era nota al 97% dei soggetti coinvolti nel campione, i quali hanno dichiarato di aver provato stupore e interesse per quanto avvenuto. Il 61% dei soggetti coinvolti nel campione ha affermato di utilizzare Facebook come sempre, mentre solo il 23% ha fatto delle modifiche alle impostazioni per la gestione della privacy nella piattaforma. Confrontando le risposte della domanda 17 con quelle della domanda 11 si evince l'assenza di un impatto immediato nella gestione dei dati online dopo il caso Cambridge Analytica, che ha coinvolto anche gli utenti più attenti alla loro privacy. Su 120 individui che hanno dichiarato di utilizzare Facebook come prima, 71 di questi ha affermato di aver fatto una delle modifiche alle impostazioni sulla privacy nella prima parte del questionario. Allo stesso modo, analizzando le domande 17 e 19 è possibile

evincere che il 78% di chi utilizza Facebook come prima, sia convinto che un evento simile al caso considerato, possa avvenire anche in futuro.

L'unica ipotesi negata rispetto a quanto supposto in precedenza, riguarda la conoscenza e la fiducia degli utenti verso il nuovo regolamento europeo sulla privacy (GDPR). Il 47% degli individui coinvolti nell'indagine non conosce la norma citata, mentre solo il 19% crede che questa possa migliorare la tutela delle informazioni condivise in rete (6.1.4). Tali risultati dimostrano una scarsa conoscenza di alcuni elementi significativi dell'attuale ordinamento in materia di privacy online. Un quinto degli intervistati ha inoltre espresso un parere di sfiducia sul rinnovamento svolto dal nuovo regolamento europeo.

Nella verifica delle ultime due ipotesi si è cercato di individuare le abitudini di utilizzo del social network e le caratteristiche personali dei soggetti campionati, allo scopo di definire il grado brand loyalty a Facebook e identificare una possibile relazione tra l'uso della piattaforma e il livello di formazione accademica. L'83% del campione ha dichiarato di utilizzare Facebook più volte al giorno, da un periodo di tempo compreso tra i cinque ai dieci anni. La normale permanenza nel sito è però di breve durata, considerando che il 48% degli utenti dichiara di aver utilizzato Facebook per circa tre ore nell'ultima settimana. Ciò dimostra come l'utilizzo della piattaforma sia caratterizzato da un uso ripetitivo ma poco significativo nell'arco di una giornata, considerando l'alta frequenza di accesso e la breve permanenza.

Il comportamento di utilizzo di Facebook non rivela tuttavia una particolare brand loyalty verso il social network. Ciò si giustifica, con diversi risultati raccolti dai questionari, tra cui: il 23% di utenti che utilizza Facebook solo qualche minuto alla settimana, il 93% che afferma di essere iscritto ad altri social network, il 10% che li preferisce dopo quanto rivelato dallo scandalo Cambridge Analytica o infine alcune affermazioni di insoddisfazione rilasciate a commento del caso citato. Per quanto riguarda queste ultime in particolare, si evince come anche i membri più delusi da quanto accaduto, non intendano eliminare il proprio profilo Facebook allo scopo di mantenere un minimo rapporto con la propria cerchia virtuale di amici. Ciò dimostra come il modello dell'economia di rete abbia fortemente inciso sul caso specifico e sull'uso complessivo della piattaforma. Tale sistema infatti permette ai

social network di ottenere un'ampia diffusione mondiale, con cui resistere anche a significativi eventi traumatici che potrebbero incidere sulla brand reputation.
Infine, nell'ultima ipotesi si è cercato di valutare quanto il grado d'istruzione abbia inciso sulla conoscenza del caso Cambridge Analytica e sulla reazione a quanto accaduto. Tale verifica ha comportato l'analisi comparata delle domande presenti nella seconda e nella terza parte del questionario e in particolare della numero 20.

20. Sei iscritto a…

● *Corso di laurea triennale primo*	*34*	*17,5%*
● *Corso di laurea triennale secondo*	*38*	*19,6%*
● *Corso di laurea triennale terzo*	*49*	*25,3%*
● *Corso di laurea triennale fuori corso*	*6*	*3,1%*
● *Corso di laurea magistrale primo*	*29*	*14,9%*
● *Corso di laurea magistrale secondo*	*33*	*17,0%*
● *Corso di laurea magistrale fuori corso*	*5*	*2,6%*

Il 65,5% dei soggetti coinvolti nel campione è iscritto a un corso di laurea triennale, mentre il 34,5% a uno magistrale. Considerando che il 97% dei soggetti coinvolti nel campione conosceva il caso preso in esame, non è possibile affermare che esista una relazione tra la conoscenza della notizia e il grado d'istruzione del campione. Allo stesso modo, è stato riscontrato che il 40% di chi ha dichiarato di continuare a usare Facebook come prima, frequenta un corso di laurea magistrale. Tale dato rispecchia il rapporto percentuale definito dalla domanda 20, negando definitivamente l'ultima ipotesi e dimostrando come il grado di istruzione non abbia inciso nelle reazioni avute dalla notizia.

6.3
Ulteriori considerazioni

La raccolta dei dati primari è stata fatta allo scopo di rispondere alla research question posta dall'indagine, relativa alla valutazione degli atteggiamenti di

condivisione e uso delle informazioni personali online. Dall'analisi della letteratura dedicata al fenomeno del privacy paradox, è emerso come la gestione delle informazioni personali all'interno della rete sia solitamente dettata da un comportamento istintivo, di reazione alle caratteristiche del sito internet. Gli utenti della rete tendono ad esser più cauti nella condivisione di dati personali online, solo se in passato sono stati oggetto di attacchi diretti alla loro privacy. La ricerca si è dunque focalizzata sul caso Cambridge Analytica, il quale è stato uno degli esempi più significativi di utilizzo improprio di dati nel 2018. L'indagine ha avuto come scopo principale la valutazione delle reazioni avute dai membri del social network alla notizia, la quale è stata preceduta da una prima analisi comportamentale sulla condivisione di informazioni personali nella piattaforma.

I risultati raccolti hanno dimostrato come non vi sia stato un cambiamento immediato dell'utilizzo di Facebook, dopo quanto accaduto a marzo 2018. Gli stessi hanno manifestato un certo grado di conoscenza e interesse alla notizia, tuttavia non intendono fare delle modifiche al loro abituale utilizzo del social network, nonostante percepiscano il caso come un fatto non isolato e potenzialmente ripetibile. Gli esiti della ricerca svolta, sono stati del tutto simili a quanto analizzato dall'agenzia di stampa Reuters-Ipsos, che tra aprile e maggio 2018, ha raccolto le reazioni di oltre duemila cittadini statunitensi di età compresa tra i 26 e i 30 anni. Anche in questo caso infatti, oltre la metà degli individui coinvolti nel campione ha dichiarato non aver cambiato il proprio modo di utilizzare Facebook, dopo il datagate che lo ha coinvolto insieme a Cambridge Analytica. Solo un quarto ha sostenuto di utilizzare la piattaforma meno di quanto accaduto, mentre il restante ne ha aumentato l'uso (Kahn, Ingram, 2018).

A dispetto di quanto emerso a luglio 2018, sul calo di iscritti registrato dal social network in Europa nel secondo trimestre dell'anno, l'indagine ha dunque rilevato una certa resistenza di Facebook allo scandalo che lo ha coinvolto. Ciò ha evidenziato come anche un palese uso improprio dati condivisi online, non rappresenti uno stimolo sufficiente a sensibilizzare gli utenti sul tema della privacy e di conseguenza, renderli concretamente più attivi nella gestione delle proprie informazioni personali online. Tale valutazione inoltre, può ipoteticamente dirsi indifferente all'ordinamento esistente in materia di data retention, considerando le

analogie dei risultati con i dati raccolti negli Stati Uniti nello stesso periodo. Ciò tuttavia dovrebbe essere confermata da ulteriori indagini condotte in altri Paesi, egualmente coinvolti nello scandalo Cambridge Analytica.

L'analisi dei dati primari ha evidenziato un secondo aspetto significativo nel normale utilizzo di Facebook, già precedentemente osservato da diverse ricerche svolte in ambito accademico. L'indagine ha infatti rivelato, come i membri iscritti al social network siano molto più attenti all'immagine del proprio profilo virtuale, piuttosto che alla sicurezza informatica dello stesso. Tale comportamento sarebbe motivato dal reale riscontro che gli iscritti alla piattaforma dovrebbero giustificare ai membri della propria rete sociale. La ricerca ha evidenziato come Facebook consista in un mezzo per mantenere delle relazioni sociali virtuali, che tuttavia spesso rispecchiano anche i legami esistenti nella vita reale degli iscritti.

Le stesse modalità di gestione dei dati, furono riscontrate anche nel 2013 da Young e Quan-Haase nella ricerca "Privacy protection strategies on Facebook", fatta su un campione di circa un centinaio di studenti, da cui questa ricerca ha preso alcuni riferimenti per la raccolta dei dati primari. I risultati raccolti dallo studio svolto cinque anni prima, hanno dimostrato come gli utenti non siano disposti a bloccare altri membri iscritti al sito o a falsare le informazioni condivise nel proprio profilo online. Gli utenti campionati allora dichiaravano di preferire l'uso delle impostazioni sulla privacy o l'omissione delle informazioni più sensibili, per la riduzione dei rischi dati dalla condivisione di dati personali online. Gli stessi risultati sono stati riscontrati anche nel corso del campionamento svolto in questa indagine, dimostrando come i trend comportamentali di condivisione dei dati online, siano simili a quelli individuati da Young e Quan-Haase e non abbiano subito particolari cambiamenti a distanza di circa cinque anni.

Infine, per quanto riguarda il controllo della propria cyber security online, dallo studio fatto si evince una completa mancanza di effetti concreti nell'uso di Facebook dopo il caso Cambridge Analytica. L'impatto mediatico dato dalla notizia non è stato uno stimolo sufficiente a sensibilizzare gli utenti in materia di tutela dei dati online. Allo stesso modo neanche l'entrata in vigore del nuovo Regolamento europeo per la protezione dei dati (GDPR) avrebbe sensibilizzato gli utenti sulla

questione della cyber security, spingendoli a verificare lo stato di tutela dei proprio dati caricati all'interno del proprio profilo social.

L'evento traumatico eccezionale subito dall'azienda è stato affrontato con una risposta immediata, centralizzata e trasparente, considerando che lo stesso Zuckerberg è stato chiamato a chiarire la posizione di Facebook davanti al Congresso Statunitense. La gestione della crisi ha permesso all'azienda di superare le prime difficoltà avute in campo economico e finanziario, ciò nonostante il caso non ha effettivamente sensibilizzato gli utenti su un controllo razionale della propria sicurezza online, ma piuttosto, ha suscitato delle reazioni emotive, che nel lungo termine rischiano di rovinare la brand reputation del social, incidendo inevitabilmente sul numero di iscritti.

Capitolo 7
Implicazioni manageriali

7.1
Ipotesi di sviluppo per la domanda

Nello studio del privacy paradox e del caso Facebook e Cambridge Analytica sono stati considerati e approfonditi vari temi, legati alla gestione della comunicazione in caso di crisi e alla necessità che hanno le aziende di dichiarare i propri valori etici di riferimento. La crisi affrontata da Facebook è stata un evento traumatico attribuibile in parte ad azioni delittuose compiute da terzi e in parte a omissioni di controllo sui flussi di informazioni gestite internamente dall'azienda. Secondo quanto dichiarato da Zuckerberg, la sottrazione di dati fatta da Cambridge Analytica sarebbe avvenuta con il consenso del social e grazie al mascheramento della raccolta in ricerche accademiche. Facebook d'altro canto, è responsabile di non aver vigilato abbastanza sulla vicenda all'epoca dei fatti, tanto da esser già stata condannata a luglio 2018, al pagamento di una multa dal l'autorità britannica per la privacy e la protezione dei dati personali (Information Commissioner's Office - Ico). Già nel 2016, l'inchiesta svolta da Carole Cadwalladr e pubblicata nella rivista "The Observer", nell'articolo "The great British Brexit robbery: how our democracy was hijacked" faceva dei riferimenti agli interessi strategici che Cambridge Analytica aveva nei confronti dei database di Facebook.
Nel 2018 la pubblicazione di nuovi articoli sulla vicenda e le reazioni politiche ed economiche sono state prontamente gestite da Facebook. La società è riuscita a superare gradualmente le prime settimane di crisi grazie all'intervento diretto di Mark Zuckerberg che ha una sostenuto una prima ripresa mediatica e finanziaria dell'azienda, chiarendo pubblicamente la sua posizione sui fatti usando lo stesso social network e rispondendo alle accuse davanti al Congresso degli Stati Uniti. La

crisi aziendale è stata così affrontata in modo centralizzato, formale, trasparente e pubblico, ristabilendo in un primo momento la fiducia dei mercati finanziari sulle prospettive economiche della società.

Le prime tensioni mediatiche e finanziarie causate dalla vicenda, sono state seguite da un andamento altalenante dei mercati finanziari e del livello di fiducia degli iscritti al social network. Dopo i risultati incoraggianti del primo trimestre, Facebook ha registrato un calo del numero di utenti presenti in Europa nel corso primo semestre 2018. La vicenda ha dunque avuto dei riflessi negativi, che tuttavia non sono stati riscontrati dall'indagine, svolta immediatamente dopo lo scoppio dello scandalo. Da alcune affermazioni raccolte dai questionari si evince infatti come Facebook rappresenti per gli utenti uno strumento di comunicazione, utile a mantenere vivi i contatti con la propria rete sociale. Ciò nonostante, il calo di iscritti riscontrato in Europa rappresenta comunque una minaccia concreta per lo sviluppo di Facebook nel continente, considerando il fatto che essendo una piattaforma di social network, è caratterizzato da un'economia di rete che si regge sul volume di utilizzatori.

Dopo la pubblicazione dell'inchiesta di Matthew Rosenberg, Nicholas Confessore, Carole Cadwalladr e Emma Graham-Harrison, Facebook ha implementato una strategia di superamento della crisi volta ad affrontare il caso per i suoi effetti temporanei e per quelli a lungo termine. Nell'immediato, Mark Zuckerberg ha chiarito la posizione dell'azienda alle autorità internazionali, mentre gli utenti coinvolti nel caso sono stati contattati personalmente. L'azienda ha inoltre agito per arginare gli effetti del datagate sulla brand reputation, realizzando una campagna di sensibilizzazione sul controllo e la gestione della privacy online. La società si è infatti attivata per svolgere una comunicazione proattiva verso i propri utenti, informandoli sulle modifiche dei termini di privacy tramite dei messaggi postati all'interno delle loro bacheche. La campagna di sensibilizzazione è stata realizzata anche con l'uso di cartellonistica esterna e inserzioni sui quotidiani.

Gli sforzi fatti per il superamento della crisi non hanno comunque avuto degli effetti sulla brand reputation aziendale, la quale deve essere valutata invece su una prospettiva di lungo termine, che non comprenda i soli primi sei mesi successivi alla vicenda. Sempre nella prospettiva di una valutazione futura, l'andamento della

società non può essere descritto considerando il solo caso Cambridge Analytica, ma devono essere presi in considerazione altri fattori quali ad esempio il problema della fake news e la diffusione di nuovi social network, come Instagram.

7.1.1
Scelta dei mezzi di comunicazione

Il caso Facebook e Cambridge Analytica ha avuto un impatto significativo nel mercato dei social media, in quanto ha palesemente dimostrato come anche la piattaforma più popolare al mondo, possa essere coinvolta in una fuga incontrollata di informazioni appartenenti a milioni di utenti. Il sito che nei primi mesi del 2018 raccoglieva oltre due milioni di persone, si è dimostrato vulnerabile a un attacco così diffuso, che ha potenzialmente inciso sulle scelte politiche di 87 milioni di persone. In un primo momento si era iniziato a mettere in discussione l'intero sistema di gestione dei social network, tanto che nelle settimane successive all'uscita della notizia vi fu un crollo in Borsa di tutti i titoli azionari legati ai gestori di piattaforme simili, come ad esempio Snapchat e Twitter.
A oggi Facebook e gli altri social network hanno adottato delle misure per superare la crisi mediatica e finanziaria di marzo 2018, tuttavia il caso Cambridge Analytica resta un esempio dei possibili rischi, relativi alla gestione dei dati condivisi in rete. La notizia ha infatti suscitato un forte clamore mondiale, sensibilizzando gli utenti della rete sul tema della condivisione di informazioni personali online. La raccolta dei dati effettuata nel corso dell'indagine ha dimostrato inoltre, come circa l'80% degli soggetti coinvolti crede che quanto accaduto possa ripetersi anche in futuro.
Uno dei fatti più eclatanti avvenuti a marzo 2018, è stato il boicottaggio di Elon Musk a Facebook, il quale decise nell'immediato di eliminare le pagine di Tesla e Space X dal social network. In un primo momento si credeva che molte altre società potessero unirsi alla sua protesta, sancendo definitivamente la fine della piattaforma. Per quanto questo non sia avvenuto, oggi è rimasta aperta la questione della scelta del social media mix. La decisione di Elon Musk è stata dettata da ragioni

etiche relative al trattamento di informazioni sensibili. Secondo l'imprenditore infatti, Facebook non riesce a garantire la massima tutela dei dati che raccoglie giornalmente dai propri iscritti. Allo stesso modo, le aziende che hanno deciso di aderire alla campagna di boicottaggio al social network, hanno preso una posizione decisiva riguardo quanto accaduto, ribadendo i loro valori di riferimento in tema di data retention e data mining.

Per quanto la protesta mossa contro il social network abbia avuto un forte clamore mediatico, dall'indagine è emersa l'assenza di una reazione concreta degli utenti, che si sono mostrati indifferenti anche alla campagna di boicottaggio. In una valutazione generale dei risultati raccolti dai questionari, si evince infatti come la maggioranza degli utenti non abbia alcuna intenzione di rimuovere il proprio profilo Facebook. Il social network rappresenta dunque un mezzo di comunicazione ancora valido per rimanere in contatto con i membri delle proprie cerchie sociali. Allo stesso modo però gli iscritti sono coscienti dei rischi che corrono nella condivisione di informazioni personali nella piattaforma.

Il punto di vista espresso dagli utenti rappresenta un elemento significativo nello studio delle modalità di utilizzo dei social network e per questo motivo, dev'essere considerato nelle scelte di pianificazione del social media mix. La definizione degli strumenti da impiegare per la comunicazione promozionale online, costituisce un'importante decisione strategica, che incide sull'efficacia complessiva delle azioni di marketing. Le aziende determinano il proprio social media mix, considerando le caratteristiche del proprio target e gli obiettivi che intendono raggiungere. L'analisi di questi elementi permette infatti, di ottimizzare l'efficacia del messaggio, incidendo nel successo complessivo della campagna promozionale.

Secondo quanto analizzato dai dati primari raccolti dai questionari, Facebook rappresenta un mezzo di comunicazione soggetto a possibili attacchi informatici, proprio come altri siti internet. Consapevoli di questo, i membri del social network non rinunciano all'uso della piattaforma, allo scopo di mantenere le relazioni con i propri contatti. L'uso del sito non può dunque riferirsi alle garanzie di sicurezza poste dallo stesso, ma piuttosto alla comunità che raccoglie.

Il boicottaggio di Facebook ha sensibilizzato gli utenti in materia di trattamento dei dati online, tuttavia non ha inciso sulle loro abitudini di utilizzo di Facebook. La

scelta del social media mix deve dunque seguire una linea di valutazione più tradizionale legata all'analisi delle piattaforme esistenti, all'utilizzo che ne viene fatto e agli obiettivi di marketing posti dall'azienda.
Le imprese che intendono dichiarare la loro posizione in materia di trattamento dei dati, hanno il dovere di agire inserendo la questione all'interno del proprio codice etico e pubblicando dei messaggi informativi destinati agli utenti interessati dalle loro attività di data retention. Tale strategia rappresenta la soluzione più efficace per l'affermazione dei valori aziendali in materia di privacy, tanto da essere più significativa di un'azione boicottaggio. Le aziende che descrivono pubblicamente le loro attività di raccolta e gestione dei dati personali, rispettano i canoni di trasparenza richiesti dalle leggi europee e nello stesso tempo trasmettono un senso di fiducia all'interno dell'ambiente in cui operano.

7.1.2
Politiche interne aziendali

Mark Zuckerberg ha apertamente descritto i valori etici di Facebook in modo centralizzato e uniforme, nel corso della sua testimonianza davanti al Congresso statunitense. Le dichiarazioni fatte sono state particolarmente efficaci nel contrastare i primi effetti della crisi economica e finanziaria dovuta allo scandalo, tanto da aver permesso una prima ripresa del titolo azionario in Borsa.
Quanto avvenuto rappresenta tuttavia un fatto eccezionale, realizzato in risposta a un evento traumatico significativo, subito dal social network. Il tema del rispetto della privacy nel trattamento di dati online, rappresenta una questione rilevante nelle relazioni tra aziende e stakeholder. Chi svolge attività di data retention e data mining, ha il dovere di comunicare i principi etici a cui fa riferimento, secondo modalità e tempistiche conformi ai bisogni degli utenti interessati.
Le aziende devono considerare la realizzazione di un il codice etico come uno dei primi passi per la dichiarazione dei propri valori. Il codice etico rappresenta una sorta di carta costituzionale, in cui l'azienda dichiara i principi a cui fa riferimento

nella sua attività di mercato, nel rispetto dei propri stakeholder, della concorrenza e dell'ambiente socio economico in cui opera. Il tema del trattamento dei dati personali deve rientrare negli argomenti considerati dal documento, in quanto rappresenta un fattore di tensione tra principi etici sociali e norme di condotta manageriali. I valori enunciati nel codice etico devono rappresentare un punto di riferimento per tutte le attività svolte dall'azienda, tra cui il controllo dei sistemi produttivi e la gestione dei rapporti con l'ambiente esterno. Il documento rappresenta infatti l'insieme dei valori condivisi da tutti i membri dall'azienda, definiti e comunicati in modo chiaro e coerente alle attività svolte (Felici, 2005).

Il codice etico rappresenta un documento ufficiale, appartenente a un tipo di comunicazione istituzionale e formale, simile a quella adottata da Facebook nelle prime fasi di superamento della crisi causata dal datagate. Il documento costituisce infatti un fattore significativo per di un certo ambiente di mercato, definibile con quello dei soggetti più coinvolti nel ciclo economico e finanziario dell'azienda. I codici di condotta costituiscono infatti una sorta di autocertificazione, che permettono alle aziende di ottenere più fiducia da parte dei propri stakeholder tra cui anche finanziatori e fornitori. Questi ultimi in particolare, sono quelli che hanno bisogno di ottenere più garanzie dalle aziende, in quanto mettono a disposizione delle risorse economiche e finanziarie proprie. Per questa ragione si affidano alla presenza di documenti formali quali appunto i codici etici, in cui le aziende dichiarano in modo pubblico il loro impegno al rispetto di determinati principi.

Nonostante il codice etico rappresenti uno strumento significativo per la dichiarazione dei valori aziendali, dalla letteratura considerata e dallo studio dei dati primari raccolti è possibile affermare che lo stesso sia invece ignorato dagli utenti della rete. Chi naviga online è infatti consapevole dell'attività di data retention svolta dalle aziende, tuttavia non è interessato a conoscere le modalità di gestione e la destinazione delle informazioni raccolte. Rispetto a quanto analizzato nello studio del privacy paradox è infatti evidente come gli utenti condividano le proprie informazioni personali secondo fattori emozionali. Questo incide nella gestione delle loro informazioni online, tanto da impedire l'individuazione dei veri destinatari di quanto condiviso. Per questa ragione, gli iscritti a Facebook sono

molto più attenti alle impostazioni sulla visibilità piuttosto che a quelle sulla sicurezza del loro profilo (Young, Quan-Haase, 2013).

Le aziende possono intervenire nell'affermazione dei propri valori di rispetto dei dati online, svolgendo un tipo di comunicazione più semplificata per gli utenti della rete. Ogni organizzazione deve infatti cercare condividere i principi espressi nel codice etico attraverso un linguaggio adatto ai propri destinatari. La comunicazione a riguardo deve quindi assumere una forma periodica, chiara e concisa, che permetta di sensibilizzare gli utenti in materia di privacy. Le aziende possono così aumentare la consapevolezza dei soggetti coinvolti nelle attività di data retention, migliorando conseguentemente anche le loro decisioni a riguardo.

La dichiarazione dei valori aziendali svolta in modo semplificato e periodico costituisce un'attività del tutto coerente con il nuovo regolamento europeo sulla protezione dei dati (GDPR). Quest'ultimo prevede che i titolari del trattamento comunichino in modo facile e chiaro la destinazione e i termini di utilizzo delle informazioni coinvolte nelle loro attività data retention online. La norma tuttavia differisce dalle strategie di marketing, in quanto svolge un ruolo funzionale ai soli utenti. Questi ultimi infatti devono essere consapevoli della gestione dei loro dati online, allo scopo permettere un'effettiva realizzazione del principio consensuale previsto dalla legge. Le aziende invece, devono condividere con i loro utenti i valori di riferimento adottati per il trattamento dei dati, allo scopo di instaurare con loro una relazione duratura, basata sulla fiducia reciproca.

Le affermazioni fatte dalle aziende costituiscono quindi un impegno assunto nei confronti dell'ambiente, al rispetto di un trattamento etico delle informazioni altrui, al di là della mera osservanza delle norme esistenti. I principi dichiarati devono rappresentare delle effettive convinzioni morali, assunte dalle aziende nella raccolta e nella gestione di dati. Queste hanno inoltre, il dovere di prendere atto dell'esistenza del del privacy paradox e impegnarsi nel ridurlo, fornendo delle note informative chiare, brevi e periodiche, capaci di salvaguardare il principio consensuale degli utenti. Tali comunicazioni migliorano la trasparenza della gestione delle attività di data retention e data mining, trasmettendo agli utenti un senso di consapevolezza e controllo sulle informazioni da loro condivise online. La pubblicazione di brevi aggiornamenti sul trattamento dei dati, permette alle

aziende di migliorare il rapporto con quanti interessati dallo studio della domanda online, trasmettendo loro un senso di fiducia. Il tema della data retention può essere infatti un fattore determinante la definizione della brand equity aziendale.
Una chiara presa di posizione dell'azienda a riguardo, rappresenta infatti un fattore appartenente all'insieme dei vantaggi esperienziali e simbolici che gli utenti attribuiscono alla marca. Un costante aggiornamento sulle attività di data retention svolte dall'azienda permette agli utenti di comprendere e definire in modo chiaro i destinatari delle informazioni da loro pubblicate online. Una costante sensibilizzazione degli utenti a riguardo, migliora il loro senso di controllo e gestione dei dati, incidendo sulle percezioni di utilizzo della rete.
I soggetti che sentono di avere una piena padronanza sulle proprie informazioni online, percepiscono un senso di gratificazione maggiore dall'uso di internet, che si riflette in una maggiore apertura nella condivisione di informazioni personali e in una maggiore interazione con la piattaforma. Allo stesso modo, una dichiarazione obiettiva e concisa dei principi adottati per le attività di data retention e data mining rappresentano per gli utenti un riflesso dei propri valori di rispetto della privacy altrui. Tale senso di reciprocità e trasparenza nella condivisione dei dati costituisce dunque un vantaggio simbolico per i soggetti coinvolti nell'analisi della domanda online. Nel lungo periodo tali vantaggi, costituiscono per gli utenti un più ampio senso di fiducia e coinvolgimento verso la piattaforma online (es. social network) e verso il brand che li utilizza (Aaker, 1997).

7.1.3
Evoluzione del sistema normativo

Nel corso della sua testimonianza davanti al Congresso statunitense, Mark Zuckerberg ha fatto un paragone tra le normative europee in tema di privacy e quelle statunitensi. Il suo intervento oltre a chiarire la posizione della piattaforma, è servito infatti, anche a sensibilizzare il senato americano sul tema delle normative garanti della sicurezza dei dati raccolti e scambiati online, per scopi

economici e politici. Zuckerberg ha infatti auspicato la definizione di normative chiare e corrette nei confronti degli utenti della rete, indicando con favore gli sforzi fatti dall'Unione Europea con il nuovo regolamento generale per la tutela della privacy (Valsania, 2018).

Il trattamento dei dati online è diventato una delle tematiche chiave per aziende appartenenti al settore del digitale, e in particolare quelle statunitensi. La fine del Safe Harbor e l'entrata in vigore del nuovo regolamento europeo ha significativamente ridimensionato il sistema normativo di gestione dei dati tra Stati Uniti e Unione Europea. A fronte di tali cambiamenti, alcune aziende hanno deciso di adottare un modello standard di gestione dei dati, valido per il maggior numero di Paesi in cui sono presenti. Tim Cook, amministratore delegato di Apple ha dichiarato che l'azienda utilizzerà gli standard di sicurezza europei anche al di fuori dell'Europa e lo stesso farà anche Google.

Mark Zuckerberg finora ha affermato di voler migliorare la gestione delle informazioni raccolte all'interno della piattaforma, tuttavia ha negato un possibile utilizzo delle normative europee come standard di condotta anche negli Stati Uniti (Hern, 2018). Lo stesso ha invece invocato insieme a Twitter, la realizzazione del progetto di legge statunitense "Honest Ads Act". Quest'ultimo renderebbe obbligatoria la pubblicazione di costi, autori e target di messaggi politici online, allo scopo di applicare nella divulgazione politica digitale, le stesse norme esistenti per quella realizzata con altri mezzi di comunicazione (Valsania, 2018).

Il caso Cambridge Analytica ha dunque suscitato un dibattito politico, sulla realizzazione di normative uniformi a livello internazionale, capaci di tutelare tutti gli utenti della rete in modo omogeneo. Anche in questo caso le più importanti aziende del digitale hanno dimostrato un loro interesse a riguardo. L'attivismo sorto dalla vicenda è stato tuttavia svolto con azioni autonome, che hanno messo in evidenza il problema legato all'autoregolamentazione adottata dalle aziende in materia di data retention e data mining. Ciascun attore economico si sente infatti autorizzato a gestire i dati appartenenti ai propri utenti, seguendo delle regole proprie, talvolta diverse da quelle applicate da altre organizzazioni.

La stessa questione era già stata posta da Google dieci anni prima, il quale aveva chiesto all'ONU di istituire un Global Privacy Counsel, in risposta all'arresto del

giornalista cinese Shi Tao, che nel 2004 usò Yahoo! Mail per annunciare il boicottaggio del partito comunista alla ricorrenza del massacro di piazza Tienanmen. Allora Yahoo! venne accusata di non aver tutelato il diritto di anonimato, con il quale lo scrittore avrebbe potuto esercitare liberamente la sua professione, senza subire le pesanti conseguenze della censura pubblica. La società non fu imputata giuridicamente nella questione, ma dovette sopportare le accuse mosse da diverse autorità internazionali che protestano contro la sua condotta, incidendo negativamente nella sua brand reputation (Rodotà, 2014).

Le aziende coinvolte in questi scandali sono solitamente attive online come marche ombrello, volte a offrire servizi gratuiti per gli utenti e a pagamento per le aziende. Facebook, come Yahoo! è stata accusata di non rispettare la privacy e i diritti dei suoi iscritti, andando contro un'etica di tutela della dignità altrui. Allo stesso tempo però, i principi morali appartenenti all'ambiente di riferimento sono in tensione con i sistemi manageriali che stanno alla base delle logiche aziendali. La definizione di un codice di condotta è il primo passo per il riconoscimento di questi punti di contrasto. A questa fase deve seguire l'impegno dell'azienda per la realizzazione di un sistema gestionale che rispetti tutti gli stakeholder dell'organizzazione, tra cui anche gli utenti interessati del trattamento dei dati online.

Infine, la realizzazione di politiche adeguate per il rispetto della privacy nelle attività di data retention e data mining online deve essere sostenuta dalla collaborazione dell'azienda con altri attori coinvolti in questo genere di operazioni. Tale uniformazione ha un'utilità bilaterale, sia per gli utenti della rete che per le imprese stesse. I primi infatti possono così far riferimento a un solo modello per la gestione dei dati, che evita loro il rischio di subire dei trattamenti diversi a seconda delle piattaforme e dei siti a cui accedono. La aziende invece possono così adottare un sistema standard, uniforme all'ambiente di riferimento, con il quale definire dei riferimenti per la costituzione di un modello comune che rispetti i principi etici di trattamento dei dati. In questo modo, riuscirebbero a evitare di esser accusate singolarmente per le loro modalità di gestione, nel caso venissero coinvolte in scandali simili a quanto avvenuto nel datagate Facebook e Cambridge Analytica. Le aziende coinvolte nella realizzazione di un sistema di autoregolamentazione condiviso, dovrebbero inevitabilmente individuare i principi più significativi nel

rispetto della tutela dei dati online. Lo sviluppo di codici di condotta privati condivisi tra diversi attori di mercato faciliterebbe inoltre il dialogo tra istituzioni e operatori economici in prospettiva della definizione di un ordinamento comune.

7.2 Risvolti nel lungo termine

Nel corso del 2018, Facebook è stato il social network che più di tutti ha subito un andamento economico e finanziario altalenante e costantemente incerto. A marzo la pubblicazione degli articoli "How Trumps Consultants Exploited the Facebook Data of Millions" e "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach" portarono il titolo di Facebook a perdere in soli due giorni circa 60 miliardi di dollari in Borsa e ad un chiarimento tempestivo della vicenda davanti al Congresso Statunitense da parte dello stesso Mark Zuckerberg. Dopo i primi due mesi successivi allo scoppio dello scandalo il social network riuscì in a recuperare quanto perso, riacquisendo già a maggio un valore di mercato precedente alla crisi e contando l'entrata di 70 milioni di nuovi utenti. Infine tra luglio e settembre vi fu nuovamente un crollo finanziario ed economico, dato dalla pubblicazione dei risultati sull'andamento del sito nel primo semestre dell'anno, in cui si evidenziava un generale calo del numero di iscritti.
Una delle principali questioni emersa dalla vicenda è stata la formulazione di varie ipotesi sul futuro di Facebook. L'appropriazione e l'uso illecito di dati fatto da Cambridge Analytica ha infatti messo fortemente in discussione le misure di tutela e di gestione dei dati caricati in Facebook, facendo sorgere dei dubbi sullo stesso business model dell'azienda. Il datagate del 2018 ha contribuito a segnare la brand reputation del social, già compromessa da altri fattori, quali i rischi sulle fake news, la gestione del cyber bullismo e il controllo di profili falsi coordinati per il raggiungimento di obiettivi comuni.
L'azienda ha comunque deciso di intervenire in modo compatto su tutti questi temi, partendo dal suo stesso business model. Nel corso della sua testimonianza a Capitol Hill, Mark Zuckerberg ha ribadito le sue volontà di non voler intervenire nel modello di business del social network, lasciando che la piattaforma resti un mezzo

di comunicazione e condivisione gratuito, sostenuto dal flusso di dati venduti ad aziende, per lo più per scopi pubblicitari. Oltre al mantenimento del business model Facebook non intende diversificare la propria offerta di valore, a dispetto di quanto realizzato da altre aziende per migliorare la stabilità finanziaria ed economica delle proprie attività (Simonetta, 2018).

L'intervento di Facebook per il mantenimento della brand reputation è stato dunque basato su azioni interne alla piattaforma stessa. Nel corso del 2018 l'azienda ha annunciato una serie di interventi per migliorare la gestione delle informazioni scambiate all'interno della piattaforma. In primo luogo, ha sfruttato il datagate di marzo per affermare i suoi valori sul trattamento dei dati degli utenti, realizzando inoltre una campagna pubblicitaria volta a sensibilizzare gli utenti, servendosi del sito stesso e utilizzando altri mezzi di comunicazione tradizionali, come inserzioni editoriali e cartellonistica. Ad agosto sono state annunciate nuove misure per il controllo delle fake news, insieme alla rimozione di pagine, gruppi e profili aventi una condotta non autentica ma coordinata a obiettivi comuni.

Infine sempre nel 2018, Facebook ha annunciato il lancio di nuovi servizi tra cui la nuova applicazione di incontri chiamata Dating e l'attivazione anche in Italia di Facebook Watch, una piattaforma televisiva realizzata dal social, già presente negli Stati Uniti da agosto 2017. La società si è impegnata a introdurre nuovi strumenti di intrattenimento e comunicazione per i propri utenti con lo scopo di sopperire alle esigenze della domanda e mantenere la propria capacità competitiva nel mercato, rispetto alle innovazioni tecnologiche introdotte dalla concorrenza.

Il processo di crescita e consolidamento di Facebook Inc. nel mercato del digitale negli anni passati è stato supportato in parte anche dall'acquisizione di altre società, quali l'azienda di visori Oculus Rift, la piattaforma di messaggistica WhatsApp e il social network Instagram. In tutti questi casi, l'acquisto era avvenuto con la promessa di Mark Zuckerberg di mantenere indipendenti tali aziende, allo scopo di sviluppare appieno le loro potenzialità tecnologiche. Le difficoltà finanziarie ed economiche avute da Facebook Inc. dopo gli scandali delle fake news e di Cambridge Analytica, hanno tuttavia portato lo stesso fondatore del social a modificare l'assetto strategico della holding. Zuckerberg ha così affidato dei ruoli strategici a propri uomini di fiducia all'interno delle tre aziende acquisite. Tali

scelte strategiche avrebbero causato l'uscita dei fondatori delle aziende acquisite da Facebook Inc., tra cui quelle di Palmer Luckey, a maggio 2017 e di Jan Koum, Brian Acton, Kevin Systrom e Mike Krieger nel 2018.

Le posizioni marginali date agli sviluppatori di Oculus Rifs, WhatsApp e Instagram all'interno delle loro stesse società, sarebbero state la vera causa scatenante la rottura con Facebook Inc.. Mark Zuckerberg starebbe infatti cercando di centralizzare la gestione dell'intera holding, in prospettiva di servirsi delle società acquisite per supportare il proprio social network. Instagram in particolare, rappresenterebbe una buona occasione di crescita per Facebook e per l'intera holding. Nel 2018 infatti l'azienda è riuscita a sostenere le difficoltà finanziarie dell'intera società grazie al successo dimostrato in sei anni dall'acquisizione, tra cui il raggiungimento del miliardo di iscritti e le prospettive di raddoppiamento per i prossimi cinque anni. Instagram costituisce un'innovazione per il mondo dei social, vista da molti come una via di fuga da Facebook, che oltretutto piace alle nuove generazioni per il formato di condivisione veloce delle immagini, in parte simile a quello di Snapchat. Ciò nonostante l'indipendenza di Instagram da Facebook sarebbe solo una questione di brand image, considerando l'ipotesi che in futuro i dati raccolti dalle società potrebbero essere condivisi tra i due social network. Nella holding dunque si verrebbe a creare un sistema di supporto biunivoco e coordinato tra le piattaforme, capace di migliorare anche la profilazione degli utenti, usata a scopi promozionali (Simonetta, 2018).

Nel complesso, il futuro di Facebook rappresenta ancora una questione aperta basata soprattutto sulla capacità che avrà la piattaforma di attrarre nuovi utenti e mantenere quelli attuali. Quest'ultimo dato rappresenta anche una garanzia per i mercati finanziari che tuttavia non hanno dimostrato la loro fiducia al social network dopo quanto avvenuto a marzo 2018. La politica di gestione dei brand di Facebook, Instagram e WhatsApp per quanto possa rappresentare una sicurezza per i mercati finanziari, non costituisce infatti una certezza per il social di Menlo Park- L'azienda dovrà infatti dovrà continuare a migliorare i sistemi di tutela dei dati personali e le funzioni di condivisione offerte, allo scopo di mantenere stabile il numero di membri iscritti alla piattaforma.

Limiti della ricerca

Uno dei principali limiti che ha caratterizzato l'intera ricerca è stato il periodo temporale in cui è stato analizzata la vicenda di Facebook e Cambridge Analytica e in cui sono stati raccolti il questionari. Il caso, scoppiato a marzo del 2018 è stato analizzato valutando gli effetti di quanto avvenuto nei primi sei mesi. Tale limite temporale ha messo in evidenza l'andamento altalenante dei risultati economici e finanziari della società ma tuttavia, non ha fornito alcuna certezza sugli effetti nell'immagine e nella reputazione dell'azienda nel medio e lungo termine.

Allo stesso modo anche le informazioni raccolte dai questionari devono essere contestualizzate a un periodo di tempo immediatamente successivo allo scandalo, considerando che la loro somministrazione è avvenuta tra maggio e giugno 2018, a meno di tre mesi dall'uscita della notizia e parallelamente all'entrata in vigore del nuovo regolamento europeo per il trattamento dei dati (GDPR). Le reazioni raccolte potrebbero esser state influenzate dal caos mediatico delle prime settimane in cui è avvenuta la vicenda. Il punto di vista degli utenti potrebbe inoltre subire dei cambiamenti entro lo stesso anno in cui è stata fatta la ricerca, considerando che non è stata del tutto chiarita la posizione di Facebook sulla vicenda. Tali considerazioni valgono meno per le risposte raccolte nella prima parte del questionario, relative alla gestione della visibilità e della sicurezza dei dati online.

Nel complesso la raccolta di dati primari si è basata sulla somministrazione di 202 questionari, destinati a un campione di studenti nati negli anni Novanta e frequenti un corso di laurea triennale o magistrale presso l'università Ca' Foscari. I risultati raccolti in questo caso devono dunque essere contestualizzati in base all'età, al grado di istruzione e all'attività di studio svolta dagli utenti coinvolti nell'indagine.

Allo stesso modo, lo studio è avvenuto all'interno di un ambiente specifico riferito a un unico ateneo. I risultati ottenuti dall'analisi dei dati primari, raccolti con la somministrazione dei questionari, hanno dunque un'interpretazione legata a una determinata popolazione di riferimento, particolarmente definita. Tale specifica-

zione evita l'estensione degli esisti ottenuti a popolazioni più generiche, come ad esempio l'insieme di studenti universitari italiani oppure gli tutti utenti iscritti a Facebook, nati negli anni Novanta.

Ciò nonostante, vari aspetti comportamentali individuati dalla raccolta dei questionari, sono stati comparati con gli elementi emersi dallo studio della letteratura accademica di riferimento. Nel complesso, uno dei principali riferimenti per l'analisi dei dati primari, relativi al privacy paradox è stata la ricerca "Privacy protection strategies on Facebook", svolta nel 2013 da Young e Quan-Haase, per la quale è stato fatto un confronto diretto tra i risultati ottenuti. Per quanto riguarda invece l'impatto che il datagate Cambridge Analytica ha avuto su Facebook, è stata presa in considerazione un'analisi svolta da Reuters-Ipsos, che tra aprile e maggio 2018, ha analizzato le reazioni di oltre duemila cittadini statunitensi di età compresa tra i 26 e i 30 anni.

Nonostante la raccolta dei dati primari sia avvenuta all'interno di un determinato ateneo, non è possibile contestualizzare la ricerca alla sola regione del Veneto, considerando la possibile presenza di studenti fuori sede e pendolari provenienti da altre regioni limitrofe. Il fattore geografico non è stato preso in considerazione dalla ricerca, in quanto non è stato ritenuto rilevante ai fini dello studio. Infine un ultimo elemento demografico da tenere in considerazione, è stata la forte disparità tra utenti femmine (90%) e maschi (10%). Tale discrepanza è stata del tutto casuale, considerando la raccolta dei dati è avvenuta online senza alcuna distinzione di sesso. I questionari infatti sono stati condivisi in gruppi studenteschi misti, in maggioranza riguardanti dei corsi di laurea triennale o magistrale.

Un ulteriore vincolo che ha condizionato l'interpretazione dei risultati ottenuti dalla raccolta dei dati primari, è stata la focalizzazione della ricerca in un unico social network. Lo studio del datagate Facebook e Cambridge Analytica ha infatti determinato l'approfondimento dei trend comportamentali, dei soli membri iscritti alla piattaforma, rispettando gli obiettivi di ricerca definiti dalla research question. L'indagine non è stata dunque estesa a una valutazione della gestione dei dati personali, nell'utilizzo di altri social network. Dalla ricerca è emerso che la maggioranza degli utenti iscritti a Facebook utilizza anche altri social network, i quali spesso hanno altre politiche di trattamento delle informazioni. Per questo

motivo è ipotizzabile che gli utenti adottino comportamenti diversi da quelli individuati nella ricerca. I risultati ottenuti dalla raccolta di dati primari, relativi alla gestione della visibilità e della privacy delle informazioni caricate nella piattaforma, non sono dunque estendibili ad altri social network.

Un'ultima considerazione relativa al datagate Facebook e Cambridge Analytica, riguarda i risvolti politici che i fatti hanno avuto a livello internazionale. Queste ultime reazioni non sono state considerate nel corso della ricerca, in quanto non attinenti alla research question formulata. L'indagine infatti, è stata realizzata con gli unici obiettivi di verifica della letteratura considerata per lo studio del privacy paradox e di approfondimento delle reazioni avute dagli iscritti al social network. Nel questionario, non è stata fatta alcuna domanda sugli orientamenti e sulle opinioni politiche degli utenti. I riferimenti a quanto accaduto sono stati tratti da articoli di giornale e in particolare da quotidiani. Le testate considerate più attendibili per la ricerca sono state il quotidiano economico "Il sole 24 ore" e i quotidiani esteri direttamente imputati nella pubblicazione della notizia, ovvero il "New York Times" e il "The Guardian".

Conclusioni

La ricerca ha cercato di descrivere l'impatto delle attività di data retention e data mining, all'interno del rapporto tra aziende e utenti, con un particolare focus sul fenomeno del privacy paradox e del caso Facebook e Cambridge Analytica.

Internet è uno strumento fondamentale per la comunicazione, che a oggi soffre di una mancanza norme, volte a regolare il suo funzionamento. Uno dei problemi più frequenti consiste ad esempio nel trasferimento di dati tra Paesi stranieri aventi ordinamenti diversi. Il datagate Facebook e Cambridge Analytica ha messo in evidenza i rischi posti dall'assenza di norme internazionali comuni, utili a individuare e punire casi simili. D'altro canto ha palesemente evidenziato come la mancata adozione di misure per la tutela della cyber security, rappresenti un fattore capace di incidere sull'immagine e la reputazione aziendale. Per questa ragione, tutti gli operatori di mercato sono sempre più chiamati esprimere la loro posizione in materia di trattamento dei dati, tramite la realizzazione di sistemi di autoregolamentazione propri, volti a tutelare quanti interessati al trattamento, al di là degli ordinamenti esistenti.

I codici di condotta costituiscono dei documenti ufficiali nei quali le aziende ribadiscono il proprio impegno nell'uso responsabile delle informazioni raccolte. Ciò nonostante appartengono a una tipologia di comunicazione istituzionale, della quale beneficiano solo i soggetti direttamente in affari con l'azienda quali finanziatori e fornitori. Questi infatti, solitamente hanno bisogno di determinate garanzie che possano essere stabili e giuridicamente valide, allo scopo di avere delle certezze sugli accordi e sugli impegni presi dall'azienda nei rapporti economici e commerciali di lungo e medio periodo.

La maggioranza degli utenti coinvolti nelle attività di data retention e data mining online gestisce invece, le proprie informazioni in modo istintivo, senza valutare i termini di gestione e i codici di condotta forniti dalle aziende. Tale comportamento causa loro una serie di incomprensioni sulla destinazione che hanno le loro

informazioni online, tanto da dar luogo al fenomeno del privacy paradox. Gli utenti infatti, sono consapevoli dei dell'uso commerciale e dei possibili rischi corsi nella condivisione di dati online, tuttavia non intervengono per tutelare la sicurezza degli stessi, ma piuttosto si preoccupano della visibilità che hanno nella rete. Ciò avviene in particolar modo nei social network, dove gli utenti espongono informazioni, opinioni, foto e video con i membri appartenenti alle loro cerchie sociali. In questo contesto, gli iscritti alle piattaforme social si attivano concretamente per controllare la propria immagine nella piattaforma, gestendo in modo consapevole la visibilità delle informazioni condivise. Lo stesso invece, non avviene per la sicurezza dei dati personali contro possibili furti o usi impropri, nonostante gli utenti siano consapevoli della vulnerabilità dei siti di social network. Solo gli utenti che già in passato sono stati personalmente direttamente coinvolti in cyber attacchi dimostrano una maggiore cautela nella condivisione di informazioni personali online, facendo attenzione alla sicurezza degli stessi.

L'indagine ha dimostrato come anche una grave e diffusa appropriazione di dati personali online, non rappresenti per gli utenti un elemento di sensibilizzazione in materia cybersecurity. La ricerca ha infatti analizzato il datagate Facebook e Cambridge Analytica, quale una delle più significative fughe di dati del 2018, fatta ai danni del social network più popolare al mondo. Dall'analisi dei dati primari raccolti nel corso della ricerca, è infatti emerso come gli utenti non abbiano percepito la notizia come un avvertimento sui possibili rischi della condivisione dei dati online, per cui il loro uso di Facebook è rimasto immutato. Questo comportamento sarebbe giustificato dall'economia di rete su cui si regge il sito, tanto che sarebbe stato rilevato un forte legame degli utenti coinvolti nel campione con la loro cerchia sociale virtuale. Ciò nonostante, in molti questionari sono state riscontrate delle affermazioni di insoddisfazione verso la piattaforma, in particolare inerenti all'uso dei dati personali fatto a scopi commerciali.

Ciò nonostante il datagate di marzo 2018, avrebbe comunque inciso sull'immagine aziendale. I dati sull'andamento della piattaforma nel primo semestre dell'anno, avrebbero infatti riscontrato un calo del numero di iscritti negli Stati Uniti e in Europa. Questa flessione, insieme alla multa ricevuta a luglio dall'autorità britannica per la protezione dei dati personali avrebbero causato una seconda fase

di crisi dell'azienda, incidendo sull'andamento del titolo azionario in Borsa. Queste continue tensioni hanno costretto Mark Zuckerberg a intervenire sulle strategie di branding dell'intera holding. Parte delle difficoltà economiche e finanziarie della società sono infatti state superate grazie agli ottimi risultati registrati dai brand di Oculus Rift, WhatsApp e Instagram. Quest'ultima in particolare ha rappresentato per molti utenti di Facebook un'alternativa al social network, essendo del tutto estranea alle vicende delle fake news e di Cambridge Analytica. Mark Zuckerberg ha così deciso cogliere il successo di Instagram per salvaguardare l'intero gruppo, centralizzando il controllo di tutte le altre società acquisite nel corso degli anni. Per fare questo ne ha ridotto la loro indipendenza, mettendo alla guida della "Family Apps" Chris Cox e inserendo Adam Mosseri come capo di sviluppo del prodotto in Instagram. Tali azioni di controllo fatte hanno suscitato dei dissidi con i fondatori delle società, che nel giro di diciotto mesi hanno dato le loro dimissioni.

Dall'analisi dei dati primari è emerso come gli iscritti a Facebook utilizzino uno o più social network, aventi solitamente delle caratteristiche diverse tra loro. Tra questi Instagram è risultata la piattaforma più diffusa (utilizzata dall'87% degli intervistati), dimostrando come il social network delle immagini rappresenti concretamente un punto di forza per Facebook Inc. Per questo motivo, il coordinamento dei brand presenti nel gruppo sta effettivamente permettendo di ridurre i danni reputazionali subiti da Facebook nelle vicende delle fake news e di Cambridge Analytica. L'estraneità di Instagram a tali fatti di cronaca e il formato di condivisione scorrevole della piattaforma potrebbero scaturire crescita futura del social, di cui Facebook potrebbe beneficiarne ulteriormente. Molti infatti hanno ipotizzato la realizzazione di una strategia di condivisione reciproca tra i due social network, nella prospettiva di creare una struttura di supporto condivisa e migliorare la comunicazione promozionale offerta da entrambi (Simonetta, 2018).

Ciò nonostante, dall'analisi della letteratura considerata e dallo studio dei dati primari si evince come le aziende siano chiamate a fare degli sforzi maggiori nella comunicazione verso gli utenti coinvolti nelle attività di data retention online. Il trattamento di dati personali è ritenuto etico quando rispetta il principio consensuale degli utenti. Lo stesso principio è alla base delle attuali leggi riconducibili all'argomento e in particolare, del nuovo regolamento europeo sulla

protezione dei dati. Per far sì che avvenga un'effettiva realizzazione del principio consensuale, gli utenti devono essere in grado di capire a cosa sono sottoposti quanto condividono le loro informazioni in rete . In questo modo possono così fare una scelta consapevole, basata su motivazioni più logiche che emotive.

Nel complesso, la comunicazione aziendale in materia di trattamento dei dati personali deve adattarsi alle esigenze degli utenti, considerando le loro modalità di accesso e utilizzo delle rete, dunque anche la questione del privacy paradox. I codici di etici costituiscono infatti parte della comunicazione istituzionale di un'azienda, che pochi utenti coinvolti nella data retention intendono consultare. Ciò nonostante, le aziende hanno il dovere facilitare la comprensione delle pratiche di raccolta e trattamento dei dati, spiegando in modo chiaro e conciso le modalità in cui viene realizzata l'analisi delle informazioni presenti nella rete. La comunicazione deve avvenire con delle note informative brevi, talvolta accompagnate da supporti grafici, che gradualmente sensibilizzano gli utenti alla tutela della sicurezza dei loro dati e che li aiutano ad assumere delle decisioni a riguardo.

Nel corso del superamento dello scandalo, Facebook ha adottato questo tipo di comunicazione con gli iscritti alla piattaforma, pubblicando dei messaggi mirati all'interno delle bacheche personali. L'azienda ha inoltre inviato un messaggio informativo a quanti hanno effettivamente subito una sottrazione di informazioni da parte di Cambridge Analytica. Tutti gli utenti sono stati avvertiti di quanto avvenuto e aggiornati sugli adattamenti normativi realizzati con l'entrata in vigore del nuovo regolamento europeo sulla protezione dei dati. Gli aggiornamenti e le note informative pubblicate da Facebook stessa sono continuate anche dopo la fine dello scandalo mediatico, arginando i fenomeni di boicottaggio e gli riducendo gli effetti della crisi sulla brand image complessiva.

Una politica di trasparenza simile a quella adottata da Facebook nel corso del primo superamento della crisi di marzo 2018, rappresenta per le aziende una svolta nel rapporto con gli utenti coinvolti nelle attività di data retention. Le imprese hanno il dovere di dichiarare i propri principi di analisi e di gestione delle informazioni in modo facile e rapido, adatto ai ritmi d'uso della rete e alle conoscenze dell'utente medio. La comprensione delle attività di data retention e data mining, permette agli interessati di avere una maggiore conoscenza della

destinazione delle loro informazioni, permettendo la realizzazione del principio consensuale e la maturazione di un senso di controllo consapevole dei propri dati. Quest'ultimo fatto in particolare migliora il senso di gratificazione dato dalla navigazione in internet e incide sul livello di fidelizzazione al sito o al brand aziendale di riferimento.

Il sostegno di politiche di trasparenza nel trattamento dei dati, promosso dalle aziende costituisce inoltre uno dei fattori di miglioramento auspicati dalle recenti leggi promulgate dall'Unione Europea. Il nuovo regolamento per la protezione dei dati (GDPR) in particolare, definisce in modo più stringente il principio consensuale, rispetto a quanto fatto in passato. A oggi tuttavia, esistono ancora delle lacune normative legate al tema della gestione delle informazioni nella rete, soprattutto nello scambio internazionale di dati. Anche per questa ragione, le aziende devono impegnarsi nella realizzazione di politiche di trattamento dati proprie, che rispettino principi etici condivisi anche da altri operatori di mercato. Collaborando con altre organizzazioni, è possibile così definire un modello standard, capace di supportare anche la creazione di nuove norme a riguardo.

Bibliografia

Aaker J., (1997). Dimensions of Brand Personality. Journal of Marketing Research, 34, (3), 347-356.

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

Acquisti A., (2005). Conditioning Prices on Purchase History. Marketing Science. 24, (3), 367 - 381

Acquisti A., Grossklags J. (2005). Privacy and Rationality in Individual Decision Making. IEEE Security & Privacy. 3, (1), 24-30.

Acquisti A, Grossklags J., (2007). What can behavioral economics teach us about privacy. In: Acquisti A, Gritzalis S, Lambrinoudakis C, di Vimercati S, editors. Digital privacy: theory, technology, and practices. Auerbach Publications, 363–77.

Awad N.F., Krishnan M.S., (2006). The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. MIS Quarterly, 30, (19), 13-28.

Baran K., Wolfgang S., (2015). Facebook has Been Smacked Down. The Russian Special way of SNSs: Vkontakte as a Case Study. Proceedings of the 2nd European Conference on Social Media (ECSM 2015), pp. 574-582, 2015.

Barth S., Jong M., (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. Telematics and Informatics. 34, (7), 1038-1058.

Batrinca B.,Treleaven P. C., (2014). Social media analytics: a survey of techniques, tools and platforms. Springerlink, 30, (1), 89–116.

Baumhart, R. (1961), How ethical are businessmen?. Harvard Business Review. (38), 6-31.

Bernardi L., (2005), Percorsi di ricerca sociale, Carocci, Roma.

Blattberg R., Deighton J., (1991). Interactive Marketing: Exploiting the Age of Addressability. Sloan Management Review, 33, 1, 5-14.

Boyd DM., Ellison NB., (2007). Social network sites: Definition, history, and scholarship. Journal of computer-mediated communication. 13, (1), 210-230.

Bondy, K., Matten, D., & Moon, J. (2004). The adoption of voluntary codes of conduct in MNCs: A three-country comparative study. Business and Society Review. 109(4), 449–477.

Brown B., (2001). Studying the internet experience. Report pubblicato il giorno 26/03/2001, da HP Laboratories Bristol. Consultabile al link: http://www.hpl.hp.com / techreports/2001/HPL-2001-49.pdf.

Cadwalladr, (2017). The great British Brexit robbery: how our democracy was hijacked. The Observer. Articolo pubblicato il giorno 07/05/2017. Disponibile al link: https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy (consultato il 10/05/2018).

Cadwalladr C., (2018). I made Steve Bannon's psychological warfare tool': meet the data war whistleblower. The Guardian. Articolo pubblicato il giorno 18/03/2018. Disponibile al link: https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump (consultato il giorno 10/05/2018).

Cadwalladr C., Graham-Harrison E., (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian. Articolo pubblicato il giorno 17/03/2018. Disponibile al link: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (consultato il giorno 11/05/2018).

Camp. J., (2004). Digital identity. IEEE Technology and Society Magazine, 23, (3), 34-41.

Carrascal J. P., Erramilli V., Cherubini M., De Oliveira R., (2013). Your browsing behavior for a Big Mac: Economics of Personal Information Online. Proceedings of the 22nd international conference on World Wide Web, 189-200.

Chellappa R. K, Sin R. G., (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. Information Technology and Management, 2-39, (6), 181-202.

Cheung K. W., Kwok J. T., Law M. H., Tsui K. C. (2003). Mining customer product ratings for personalized marketing. Decision Support Systems, 35, 231– 243.

Chiu CM., Cheng HL., Huang HL., Chen CF., (2013).Exploring individuals' subjective well-being and loyalty towards social network sites from the perspective of network externalities: The Facebook case. International Journal of Information Management, 33, (3), 539-552.

Clarke T., Boersma M., (2017). The Governance of Global Value Chains: Unresolved Human Rights, Environmental and Ethical Dilemmas in the Apple Supply Chain. Journal of Business Ethics. 143, (1), 111-131.

Cohen R. L., (1987). Distributive justice: Theory and research. Soc. Justice Res., 1, (1), 19–40.

Commissione per i diritti e i doveri relativi ad Internet (2015). Dichiarazione dei diritti in Internet, Consultabile al link: http://www.camera.it/application/xmanager/projects/leg17/commissione_internet/dichiarazione_dei_diritti_internet_pubblicata.pdf.

Convenzione n. 108 del 28 gennaio 1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale. Disponibile al link: https://www.garanteprivacy.it/documents/10160/10704/1798208 (consultato a marzo 2018).

Corte di Giustizia Europea, (2014). Comunicato stampa n. 54/14 del 8 aprile 2014. Disponibile al link: https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054it.pdf (consultato a marzo 2018).

Coviello N., Milley R., Marcolin B. (2001). Understanding it-enabled interactivity in contemporary marketing. Journal of Interactive Marketing, 15, (4), 18–33.

Culnan M. J., Armstrong, P. K., (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. Organization Science. 10, (1), 104-115.

D. lgs. del 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali". Disponibile al link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248 (consultato a marzo 2018)

Dawes S. S., (2009). Governance in the digital age: A research and action framework for an uncertain future. Government Information Quarterly, 26 (2) 257-264.

Danezis G., Lewis S., Anderson R., (2005). How Much is Location Privacy Worth? Online Proceedings of the Workshop on the Economics of Information Security Series (WEIS).

De Stefani F., (2018), Le regole della privacy. Guida pratica al nuovo GDPR. Milano, Ulrico Hoepli Editore.

Debatin B., Lovejoy J. P., Horn A. K., Hughes B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. Journal of Computer-Mediated Communication, 15, (1), 83-108.

Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Disponibile al link: http://www.garanteprivacy.it/documents/10160/10704/Direttiva+95+46+CE.pdf (consultato a marzo 2018).

Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche). Disponibile al link: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32002L0058&from=IT (consultato il giorno 16/03/2018).

Donaldson T., (1982). Corporations and morality. Englewood Cliffs, New Jersey: Prentice-Hall.

Éthier J., Hadaya P., Talbot J., Cadieux J., (2006). B2C web site quality and emotions during online shopping episodes: an empirical study, Inform. Manage. 43, (5), 627–639.

Ethier J., Hadaya P., Talbot J., Cadieux J., (2004). Business-to-consumer web site quality and web shoppers' emotions: exploring a research model. Twenty-Fifth International Conference on Information Systems, (ICIS 2004 Proceedings). Association for Information Systems AIS Electronic Library (AISeL). 72, 889-900.

Fan W.,Bifet A., (2013). Mining big data: current status, and forecast to the future. ACM SIGKDD Explorations Newsletter. 14, (2), 1-5.

Felici G., (2005). Dall'etica ai codici etici. Franco Angeli, Milano.

Final results european data market measuring the size and trends of the EU data economy, (2017). Commissione Europea. Consultabile al link: https://ec.europa.eu /digital-single-market/en/news/final-results-european-data-market-study-measu ring-size-and-trends-eu-data-economy (consultato il giorno 21/04/2018).

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

Gevers R., Sprengers M., Van Haaster J., (2016). Cyber Guerilla. Cambridge, Massachusetts, Elsevier, Syngress.

Shim K., Chung M., Kim Y., (2017) Does ethical orientation matter? Determinants of public reaction to CSR communication. Public Relations Review. 43, (4), 817-828.

Glazer R. (1991). Marketing in an Information-Intensive Environment: Strategic Implications of Knowledge as an Asset. 55, (4), 1-19.

Global Digital 2018, (2018). We are social. Consultabile al link: https://www.slide share.net/wearesocial/digital-in-2018-global-overview-86860338 (consultato il giorno 28/04/2018)

Gorla S., Ponti C., (2018). Privacy UE: il vecchio e il nuovo. Confronto tra dlgs 196/2003 codice privacy e regolamento europeo 2016/679 gdpr Copertina flessibile. Milano, Hoepli .

Gubitosa C., (2007). Hacker, scienziati e pionieri. Storia sociale del Ciberspazio e della Comunicazione Elettronica. Roma, Stampa alternativa.

Guida all'applicazione del Regolamento Europeo, (2018). Garante per la protezione dei dati personali. Consultabile al link: http://194.242.234.211/documents/10160/0/Guida+all+applicazione+del+Regolamento+UE+2016+679.pdf (Consultato il giorno 05/04/2018).

Hanna R., Rohm A.,Crittenden V., (2011). We're all connected: The power of the social media ecosystem. Business horizons, 54, (3), 265-273.

Hern A., (2018), Facebook refuses to promise GDPR-style privacy protection for US users. The Guardian. Articolo pubblicato il giorno 04/04/2018. Disponibile al link: https://www.theguardian.com/technology/2018/apr/04/facebook-gdpr-stronger-privacy-protections-eu-data-protection-law-mark-zuckerberg (consultato il giorno 24/06/2018).

Higgins, E. Tory (1997). Beyond Pleasure and Pain. American Psychologist, 52, (12), 1280–300.

Huber G. P., (1984). The Nature and Design of Post- Industrial Organizations. Management Science, 30 (8), 928- 51.

Huberman B. Adar E, Fine L., (2005). Valuating privacy. Browse Journals & Magazines, IEEE security & privacy. 3, (5), 22–5.

Hunt S. D., Chonko L. B., Wilcox J. B. (1984). Ethical Problems of Marketing Researchers. Journal of Marketing Research, 21, (3), 309-324.

Ji F. Y., (2014), Talking Past Each Other: Chinese and Western Discourses on Ethnic Conflict. Procedia - Social and Behavioral Science. 155, 434-441.

Kahn C., Ingram D., (2018). Americans less likely to trust Facebook than rivals on personal data: Reuters/Ipsos poll. The Thomson Reuters Trust Principles. Disponibile al sito:https://www.reuters.com/article/us-usa-facebook-poll/americans-less-likely-to-trust-facebook-than-rivals-on-personal-data-reuters-ipsos-poll-idUSKBN1H10K3 (consultato il giorno 19/06/2018).

Kaplan A M., Haenlein M., (2010). Users of the world, unite! The challenges and opportunities of Social Media. Business horizons. 53, (1), 59-68.

Kim. AJ., Ko E., (2012). Do social media marketing activities enhance customer equity? An empirical study of luxury fashion brand. Elsevier, 65, (10), 1480-1486.

Kirsch L. J. (1996). The Management of Complex Tasks in Organi zations: Controlling the Systems Development Process. Organi zation Science, 7, (1), 1-21.

Klobas J. E., Clyde, L. A., (2000). Adults Learning to Use the Internet: A Longitudinal Study of Attitudes and Other Factors Associated with Intended Internet Use. Library and Information Science Research, 2, (1), 5-34.

Kokolakis S. (2015). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security. 64, 122-134.

L'e-commerce in Italia, (2017). Casaleggio associati. Consultabile al link: https://www.casaleggio.it/focus/rapporto-e-commerce-in-italia-2017/
(consultato a marzo 2018).

Laczniak G. R., Murphy P. E., (2006). Marketing, Consumers and Technology. Business Ethics Quarterly,16, (3), 313-321.

Laibson D., (1997). Golden eggs and hyperbolic discounting. The Quarterly Journal of Economics. 112, (2), 443–478.

Laufer R., Wolfe M., (1977). Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. Journal of social Issues. 33, (3), 22-42.

Lee H., Chang E., (2011). Consumer Attitudes Toward Online Mass Customization: An Application of Extended Technology Acceptance Model. Journal of Computer-Mediated Communication, 16, (2), 171–200.

Leonardi P.M, Huysman M., Steinfield C., (2013). Enterprise social media: Definition, history, and prospects for the study of social technologies in organizations. Journal of Computer-Mediated Communication, 19, (1), 1-19.

Li H. , Luo X., Zhangb J., Xuc H. (2016). Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors. Information & Management, 54, (8), 1012-1022.

Linoff G. S., Berry M.J.A., (2011). Data mining techniques: for marketing, sales, and customer relationship management. John Wiley and Sons Ltd.

Lo Conte M., (2018). Uk e Ue convocano Zuckerberg. Sospeso ceo di Cambridge Analytica. Il sole 24 ore. Articolo pubblicato il giorno 20/03/2018. Disponibile al link: http://www.ilsole24ore.com/art/mondo/2018-03-20/datagate-si-dimette-capo-sicurezza-facebook-070733_PRV.shtml?uuid=AEzVFlJE (consultato il giorno 11/05/2018).

Loidean N., (2016). The End of Safe Harbor: Implications for EU Digital Privacy and Data Protection Law. Journal of Internet Law. 19 (8), 7-14.

Lutz C, Strathoff P., (2014). Privacy concerns and online behavior – not so paradoxical after all? Viewing the privacy paradox through different theoretical lenses. In Brändli, Sandra (ed.), 81-99. Consultabile al link: https://papers.ssrn.com /sol3/papers.cfm?abstract_id=2425132 (consultato a marzo 2018).

Magnini A. (2018). Facebook e Twitter contro l'Europa sui dati flop: «Colpa del Gdpr». Il sole 24 ore. Articolo pubblicato il giorno 27/07/2018. Disponibile al link: http://www.ilsole24ore.com/art/mondo/2018-07-27/facebook-e-twitter-contro-l-europa-dati-flop-colpa-gdpr--162954.shtml?uuid=AEEb6WTF (consultato il giorno 15/09/2018).

Malhotra N. K., Kim S. S., Agarwal J., (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Information system research, 14, (4), 336 - 355.

Masera A., Scorza G., (2016). Internet, i nostri diritti. Bari, Laterza editori.

Matarrese A., Notarangelo E., (2017). Informativa e consenso privacy, in arrivo il cambiamento. Il sole 24 ore. Articolo pubblicato il giorno 05/09/2017. Disponibile al link: http://www.diritto24.ilsole24ore.com/art/dirittoCivile/2017-09-05/informativa-e-consenso-privacy-arrivo-cambiamento-092942.php (consultato il giorno 24/03/2018).

McWilliams A., Siegel D., (2001). Corporate Social Responsibility: A Theory of the Firm Perspective. The Academy of Management Review. 26, (1), 117-127.

Mederois F. A., Bygrave L. A., (2015). Brazil's Marco Civil da Internet: Does it live up to the hype? Computer Law & Security Review. 31, (1), 120-130.

Mensi M., Falletta P., (2015), Il diritto del web. Casi e materiali. Padova, Cedam.

Mikut R., Reischl M., (2001). Data mining tools. Wiley Online Library.

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.

Mozur P., (2016). China's Internet Controls Will Get Stricter, to Dismay of Foreign Busines. New York Times. Articolo pubblicato il giorno 07/11/2016. Disponibile al link: https://www.nytimes.com/2016/11/08/business/international/china-cyber-security-regulations.html (Consultato a maggio 2018).

Murray A., (2016). Information Technology Law: The Law and Society. Oxford, Oxford University Press.

Novak T.P., Hoffman D.L., (2008). The fit of thinking style and situation: new measures of situation-specific experiential and rational cognition. Journal of Consumer Research. 36 (6), 56–72.

Oetzel M.C., Gonja T. (2011), The online privacy paradox: a social representations perspective. Proceeding, CHI EA '11 CHI '11 Extended Abstracts on Human Factors in Computing Systems. 2107-2112.

Pentina I., Zhang L., Bata H., Chen Y., (2016). Exploring privacy paradox in information-sensitive mobile app adoption: a cross-cultural comparison. Comput. Hum. Behav. 65, 409–419.

Petronio S., (1991). Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information between Marital Couples. Communication Theory. 1 (4), 311-335.

Papacharissi Z., (2010). A Networked Self: Identity, Community, and Culture on Social Network Sites. Routledge. 14, (7), 1240-1246.

Pizzetti F. (2016). Privacy e il diritto europeo alla protezione dei dati personali, dalla direttiva 95/46 al nuovo Regolamento europeo. Torino, Giappichelli Editore.

Pötzsch S., (2008). Privacy Awareness: A Means to Solve the Privacy Paradox? IFIP Advances in Information and Communication Technology, 298, 226-236.

Poullet Y., (2006). EU data protection policy. The Directive 95/46/EC: Ten years after. Computer Law & Security Review, 22, (3), 206-217.

Rodotà S., (2014). Il mondo nella rete. Quali i diritti, quali i vincoli. Bari, Laterza editori.

Rodotà S., (2010). Una Costituzione per Internet?. Bologna, Il Mulino.

Rosen J., (2012). The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google. Fordham Law Review, 80 (4), 1525-1538.

Rosenberg M.,Confessore N.,Cadwalladr C. (2018). How Trump Consultants Exploited the Facebook Data of Millions. New York Times. Articolo pubblicato il giorno 17/03/2018. Disponibile al link: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html (consultato il 11/05/2018)

Savioli L. (2018). Facebook crolla in Borsa, deludono conti e stime. Calano gli utenti in Europa. Il sole 24 ore. Articolo pubblicato il giorno 25/07/2018. Disponibile al link: http://www.ilsole24ore.com/art/finanza-e-mercati/2018-07-25/facebook-calano-utenti-europa-conti-sotto-attese-male-titolo-223610.shtml?uuid=AE3dJbSF (consultato il 31/07/2018).

Savioli L., (2018). Zuckerberg prende il controllo di Instagram per salvare Facebook. Il Sole 24 ore. Articolo pubblicato il giorno 25/09/2018. Disponibile al link: https://www.ilsole24ore.com/art/finanza-e-mercati/2018-09-25/instagram-senza-fondatori-ora-zuckerberg-avra-mano-libera-105935.shtml?uuid=AEBQ9r6F (consultato a settembre 2018).

Scafati G., Perelli P., (2016). La "privacy europea", il Regolamento UE 2016/679. Il sole 24 ore. Articolo pubblicato il giorno 16/05/2016. Disponibile al link: http://www.diritto24.ilsole24ore.com/art/dirittoCivile/2016-05-16/la-privacy-europea-regolamento-ue-2016679-125453.php (consultato ad aprile 2018).

Schafer JB., Konstan JA., Riedl J., (2001). E-commerce recommendation applications. Data Mining and Knowledge Discovery, 5, (1-2), 115–153.

Schwepker, C. H., Jr., & Good, D. J. (2011). Moral judgment and its impact on business-to-business sales performance and customer relationships. Journal of Business Ethics, 98 (4), 609–625.

Serrat O., (2017). Social Network Analysis. Springer, (9), 39-43.

Simon H.A., (1982). Models of Bounded Rationality. Cambridge (USA), MIT Press.

Simonetta B., (2018). Facebook: i profili ceduti a Cambridge Analytica sono 87 milioni, 214 mila italiani. Il sole 24 ore. Articolo pubblicato il giorno 04/04/2018. Disponibile a link http://www.ilsole24ore.com/art/tecnologie/2018-04-04/facebook-profili-ceduti-cambridge-analytica-sono-87-milioni-212600.shtml?uuid=AEC1evSE (consultato il 11/05/2018).

Simonetta B., (2018). Da Facebook a Google, perché è impossibile boicottare i big del web. Il sole 24 ore. Articolo pubblicato il giorno 04/04/2018. Disponibile al link: http://www.ilsole24ore.com/art/notizie/2018-04-04/da-facebook-google-perche-e-impossibile-boicottare-big-web-152813.shtml?uuid=AEdN6kSE (consultato il 10/05/2018).

Simonetta B., (2018). Facebook, il peggio è passato: in Borsa torna ai livelli pre-datagate. Il sole 24 ore. Articolo pubblicato il giorno 11/05/2018. Disponibile al link http://www.ilsole24ore.com/art/finanza-e-mercati/2018-05-11/facebook

-peggio-e-passato-borsa-torna-livelli-pre-datagate-095122.shtml?uuid=AErTXmmE&refresh_ce=1 (consultato il giorno 11/05/2018).

Simonetta B., (2018). Così Instagram ha centuplicato il suo valore e oggi può salvare Facebook. Il sole 24 ore. Articolo pubblicato il 29/06/2018. Disponibile al link: https://www.ilsole24ore.com/art/tecnologie/2018-06-29/cosi-instagram-ha-centuplicato-suo-valore-e-oggi-puo-salvare-facebook-115359.shtml?uuid=AEHPNXEF (consultato a settembre 2018).

Simonetta B., (2018). Facebook, la privacy costa cara. Ecco perché sta crollando in Borsa. Il sole 24 ore. Articolo pubblicato il 26/07/2018. Disponibile a link: http://www.ilsole24ore.com/art/tecnologie/2018-07-26/facebook-si-riscopre-fragile-privacy-e-scandali-presentano-loro-conto-172659.shtml?uuid=AEjPU2SF (consultato a settembre 2018).

Smith D. (2018). Zuckerberg put on back foot as House grills Facebook CEO over user tracking. The Guardian. Articolo pubblicato il giorno 21/04/2018. Disponibile al link: https://www.theguardian.com/technology/2018/apr/11/zuckerberg-hearing-facebook-tracking-questions-house-back-foot (consultato il 11/05/2018).

Smith, E.J., Kollars, N.A., (2015). QR panopticism: user behavior triangulation and barcode-scanning applications. Inf. Secur. J. Global Perspect. 24 (4–6), 157–163.

Smith H. J., Milberg S. J., Burke S. J., (1996). Information privacy: Measuring individuals' concerns about organizational practices. MIS Quart. 20, (2), 167-196.

Smith M., Kawasaki G., (2014). The New Relationship Marketing : How to Build a Large, Loyal, Profitable Network Using the Social Web. New York, John Wiley & Sons.

Soro A., (2016). Liberi e connessi. Torino, Codice Edizione.

Ståhlberg M., Maila V., (2013). Multichannel Marketing Ecosystems. Londra, Kogan Page.

Sutanto J., Palme e., Tan C. H., Phang C. W., (2013). Addressing the Personalization Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users. MIS Quarterly, 37, (4), 1141-1164.

Tezinde T., Smith B., Murphy J., (2002). Getting Permission: Exploring Factors Affecting Permission Marketing. Journal of Interactive Marketing. 16, (4), 28-36.

Tönnies F., Loomis CP. (2003). Community and society. New York, Routledge.

Tracol X., (2016), EU–U.S. Privacy Shield: The saga continues. Computer Law & Security Review, 32, (5), 775-777

Trasferimento dei dati personali verso Paesi terzi (2018) Garante della protezione dei dati personali. Consultabile al link: http://www.garanteprivacy.it/home/provvedimenti-normativa/normativa/normativa-comunitaria-e-intenazionale/trasferimento-dei-dati-verso-paesi-terzi (consultato il 09/04/2018).

Tre L., (2018). Agli americani Facebook non piace più. Uno su quattro cancella l'app. Il sole 24 ore. Articolo pubblicato il 06/09/2018. Disponibile al link: http://www.ilsole24ore.com/art/tecnologie/2018-09-06/agli-americani-facebook-non-piace-piu-su-quattro-cancella-l-app--085533.shtml?uuid=AEPIVWkF (consultato a settembre 2018).

Tremolada L., (2017). Quanto vale il mercato europeo dei dati? L'economia crescerà del 15%. Il sole 24 ore. Articolo pubblicato il giorno 04/05/2017. Consultabile al link: http://www.infodata.ilsole24ore.com/2017/05/04/quanto-vale-mercato-europeo-dei-dati/ (consultato ad aprile 2018).

Tufekci Z., (2008). Can you see me now? Audience and disclosure regulation in online social network sites. Bulletin of Science, Technology & Society. 28, (1), 20-36

Understanding Facebook Business Model, (2012). BMIMATTERS - Business Model Innovation Matters. Disponibile al link: http://bmimatters.com/ (consultato il giornno 09/05/2018).

Valsania M., (2018). Cambridge Analytica travolta dal Datagate: bancarotta e chiusura immediata. Il sole 24 ore. Articolo pubblicato il giorno 02/05/2018. Disponibile al link http://www.ilsole24ore.com/art/mondo/2018-05-02/datagate-cambridge-analytica-annuncia--chiusura-immediata-205429_PRV.shtml?uuid=AEAKYxhE&fromSearch (consultato il 11/05/2018).

Valsania M., (2018). Mea culpa Zuckerberg: «Sì a nuove norme sulla privacy ma non siamo un monopolio». Il sole 24 ore. Articolo pubblicato il giorno 10/04/2018. Disponibile al link: http://www.ilsole24ore.com/art/mondo/2018-04-10/mea-culpa-zuckerberg-si-nuoven-norme-privacy-ma-non-siamo-monopolio-222651.shtml?uuid=AEScqJWE&refresh_ce=1. (consultato il giorno 24/06/2018).

Waterson J. (2018). Five things we learned from Mark Zuckerberg's European parliament appearance. The Guardian. Articolo pubblicato il giorno 22/05/2018. Disponibile al link: https://www.theguardian.com/technology/2018/may/22/five-things-we-learned-from-mark-zuckerbergs-european-parliament-appearance (cosultato a settembre 2018)

Weiss M. A., Archick K. (2016). U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield. Consultabile al link: https://epic.org/crs/R44257.pdf (consultato a marzo 2018)

Westin A., (1967). Privacy and Freedom. Administrative Law Review, 22, (1), 101-106

Wilson D.W., Valacich J.S., (2012). Unpacking the privacy paradox: Irrational decision-making within the privacy calculus. AIS Electronic Library (AISeL). Thirty Third International Conference on Information Systems, Orlando, Florida, 1-11.

Wong J. C., (2018). Facebook's privacy practices are under investigation, FTC confirms. The Guardian. Articolo pubblicato il giorno 26/03/2018. Disponibile al link https://www.theguardian.com/technology/2018/mar/26/facebook-data-privacy-cambridge-analytica-investigation-ftc-latest (consultato a maggio 2018).

Xia L., Bechwati N., (2008). Word of mouse: the role of cognitive personalization in online consumer reviews. Journal of interactive Advertising, 9, (1), 3-13.

Young A. L., Quan-Haase A., (2013). Privacy protection strategies on Facebook. Information, communication & society, 16, (4), 479-500.

Zafeiropoulou A. M., Millard D. E., Webber C., O'Hara K. (2013), Unpicking the privacy paradox: can structuration theory help to explain location-based privacy decisions? In: Proceedings of the 5th Annual ACM Web Science Conference, May 2-4, Paris, France. 463-472.

Zeng D., Chen H., Lusch R., Li S., (2010). Social media analytics and intelligence. IEEE Intelligent Systems, 25, (6), 13-16.

Zhao S., Grasmuck S., Martin J., (2008). Identity construction on Facebook: Digital empowerment in anchored relationships. Computers in Human Behavior, 24, (5), 1816-1836.

Zuckerberg M. (2018). Post del Profilo di Mark Zuckerberg pubblicato il giorno 21/03/2018 da Menlo Park, USA. Disponibile al link: https://www.facebook.com /zuck/posts/10104712037900071 (consultato il giorno 11/05/2018).