Università
Ca'Foscari
Venezia

Corso di Laurea Magistrale
in Marketing e Comunicazione

Tesi di Laurea Magistrale

LA PRIVACY E LA CONDIVISIONE DELLE PROPRIE INFORMAZIONI PERSONALI ONLINE. IMPLICAZIONI DELLA TRASFORMAZIONE DIGITALE.

Relatore
Ch. Prof. Andreas Hinterhuber

Correlatrice
Ch.ma Prof.ssa Anna Moretti

Laureando
Alberto Colangelo
Matricola 851191

Anno Accademico
2019 / 2020

Sommario

ABSTRACT

Il tema della digitalizzazione è un tema ricorrente, se ne parla ormai da diverso tempo. Letteralmente, fa riferimento alla semplice trasposizione dei formati tradizionali di dati in uno che ne consente l'archiviazione sugli strumenti tecnologici in continuo sviluppo. Tuttavia, in linea generale, riguarda le trasformazioni innescate dall'adozione massiccia di tecnologie digitali che generano, elaborano, condividono e trasferiscono informazioni. Non è un evento una tantum ma segue le ondate del progresso tecnologico e la diffusione delle innovazioni che ne derivano. Negli ultimi anni si stanno man mano scoprendo gli effetti della terza ondata della digitalizzazione, ampiamente discussa nell'ultimo decennio grazie all'adozione di tecnologie digitali come le AI, gli algoritmi decisionali, l'automazione, i sensori e i Big Data. La terza ondata avrà effetti sulla crescita economica, sulla forza lavoro e, a differenza delle altre, avrà un notevole impatto sulla nostra società e il suo benessere portando, in determinate situazioni, ad una trasformazione digitale.

Inoltre, aziende, governi e istituzioni insistono sul concetto di "big data". L'idea che il progresso tecnologico consenta finalmente di utilizzare il patrimonio di dati stoccato nelle *data warehouse* ha preso sempre più piede. Le tecnologie digitali (smartphone e IoT) hanno trasformato miliardi di persone connesse in fonti e produttori di contenuti. Non è chiaro come questi contenuti vengano utilizzati perché, infatti, c'è un lato oscuro della datificazione che le persone sembrano accettare in quanto i benefici che possono trarne sono superiori agli svantaggi. Si tende a fornire una maggiore quantità di dati personali in quanto la comodità è più importante della privacy. Infatti, c'è una tendenza a voler tutto e subito, istantaneamente. Risulta, pertanto, necessario un algoritmo che diminuisca i tempi di risposta dei motori di ricerca, che conosca e sappia già cosa gli individui vogliono. Attraverso diversi approcci è possibile comprendere e allinearsi a queste tendenze.

Il primo capitolo, dunque, verterà sull'argomento della digitalizzazione, dove verranno analizzate le ondate dell'innovazione tecnologica e verrà descritta la trasformazione digitale.

Il capitolo successivo spiegherà la natura dei *data* e le tecniche di raccolta dati. Successivamente, l'elaborato intende spiegare, sulla base della letteratura, i maggiori risvolti sociali associati all'utilizzo dei *data* e le relazioni tra gli stakeholder interessati (individui, organizzazioni e società), nonché i maggiori tradeoff derivanti da queste tecnologie e che gli individui tendono a adottare.

In ultima analisi, la presente ricerca cercherà di capire quali siano le variabili che influiscono sulle intenzioni degli individui nel rilasciare le proprie informazioni personali online, partendo dall'analisi di un questionario. Inoltre, la ricerca intende analizzare quali siano gli effetti della componente ottimistica delle persone relativamente ai loro comportamenti online e alla gestione e condivisione delle loro informazioni personali online.

INTRODUZIONE

Lo scopo di questa ricerca è analizzare i comportamenti, i sentimenti e gli atteggiamenti delle persone quando si tratta della loro privacy, fornendo un quadro generico della situazione circa le tecnologie riguardanti la raccolta dati e i comportamenti dei soggetti interessati. Questa tesi indaga le intenzioni degli individui nel rilasciare le proprie informazioni personali online.

L'elaborato si concentrerà sulla natura dei dati presenti online e che si possono ricavare da tutti i sistemi connessi a Internet (IoT, AI, sensori), nonché sulle tecnologie adottate dai soggetti competenti per raccogliere tali dati online. Inoltre, verranno analizzati i comportamenti e i risvolti degli individui coinvolti (successivamente "stakeholder"), ovvero le singole persone, le organizzazioni e le società (di persone, comunità), per capire quali siano le interazioni tra loro e quali siano le implicazioni in tali relazioni.

La letteratura sostiene che la raccolta e l'utilizzo dei dati dei clienti sia un modo efficace per migliorare i ritorni di marketing (McAfee & Brynjolfsson, 2012). Le aziende, infatti, arrivano a spendere molto per acquisire e sfruttare i dati dei clienti (Columbus, 2014). Tuttavia, maggiori sono tali sforzi, maggiore è anche la vulnerabilità dei dati dei clienti e la percezione del rischio ai danni dovuti a usi indesiderati dei dati personali. Pertanto, la raccolta dei dati ha sì molti vantaggi per le aziende ma, dai consumatori, tale pratica viene spesso fatta oggetto di critiche o pareri negativi, specialemente sul tema della privacy (Marcus & Davis, 2014). Come già visto, le organizzazioni dovrebbero sviluppare pratiche decisionali che rispettino la libertà di scelta degli individui per migliorare ulteriormente la fiducia e reputazione

Quando le aziende hanno accesso ai dati personali di un cliente significa che hanno in loro possesso un dossier digitale dettagliato sulle persone e possono impegnarsi in un "trasferimento diffuso di informazioni tra una varietà di entità" (Solove, 2003). I clienti limitano il modo e con chi condividono le informazioni sensibili per ridurre questo scambio, utilizzando processi di gestione della divulgazione come il consenso o il rifiuto (Acquisti, et al., 2012). Tuttavia, le aziende già possiedono e continuano a cercare attivamente volumi crescenti di informazioni sui clienti, con la conseguenza che la protezione dei propri dati sia fonte di una preoccupazione crescente e sempre più diffusa negli individui (Tucker, 2014)

Lo studio, inoltre, intende analizzare i driver che spingono gli individui a condividere consapevolmente i propri dati, sulla base anche di caratteristiche personali come, ad esempio,

l'essere più o meno delle persone ottimiste. L'ottimismo, come verrà spiegato più avanti, gioca un ruolo fondamentale sugli individui e sui loro comportamenti. Infatti, come risulterà dall'analisi effettuata, le persone che tendono ad essere più ottimiste sono anche quelle più propense a lasciare le proprie tracce sul web e hanno una minore paura che le loro informazioni possano essere raccolte, archiviate e usate in modi illeciti.

La letteratura, a riguardo, non è ampia, se non addirittura assente. Le teorie affrontate nel documento partono, innanzitutto, dal paradosso della privacy, ovvero quella dicotomia tra attitudine/comportamento effettivo dove gli individui sono disposti a scambiare le loro informazioni personali per ricompense relativamente piccole. Le teorie della *Communication Privacy Management* (CPM) e della Vulnerabilità dei dati verranno analizzate e utilizzate per lo sviluppo delle ipotesi e la costruzione del questionario per l'indagine volta a conoscere le intenzioni degli individui nel rilasciare le proprie informazioni personali online. Infine, l'analisi dell'ottimismo come moderatore potrà essere un punto di partenza per le aziende e gli enti in generale che raccolgono i dati per capire come migliorare queste tecniche rendendole più sicure e trasparenti e stabilire una maggiore affidabilità agli occhi degli individui.

Capitolo 1 – DIGITALIZZAZIONE

1.1 – INTRODUZIONE

Di digitalizzazione se ne parla ormai da diverso tempo essendo un tema ricorrente. Letteralmente fa riferimento alla semplice trasposizione dei formati tradizionali di dati in uno che ne consente l'archiviazione sugli strumenti tecnologici in continuo sviluppo. Tuttavia, in linea generale, riguarda le trasformazioni innescate dall'adozione massiccia di tecnologie digitali che generano, elaborano, condividono e trasferiscono informazioni. Non è un evento una tantum ma segue le ondate del progresso tecnologico e la diffusione delle innovazioni che ne derivano.

La prima ondata della digitalizzazione si configura con l'introduzione e adozione delle cosiddette tecnologie "mature", ovvero tutti i sistemi informativi gestionali finalizzati all'automazione del trattamento dei dati e applicati al monitoraggio e rendicontazione dell'andamento aziendale, tecnologie di telecomunicazioni quali la banda larga (fissa e mobile) e le telecomunicazioni vocali (fisse e mobili) che consentono l'accesso remoto delle informazioni.

La seconda ondata di digitalizzazione ha comportato la diffusione di Internet e delle sue piattaforme corrispondenti (motori di ricerca, mercati), che hanno consentito il collegamento in rete delle imprese ai consumatori e delle imprese tra loro per l'acquisto di forniture e la distribuzione della produzione.

La terza ondata di digitalizzazione ha portato l'adozione di una serie di tecnologie avanzate, come big data / analytics, Internet of Things, robotica, sensori e intelligenza artificiale, con l'intento di migliorare l'elaborazione delle informazioni e la qualità del processo decisionale, automatizzando ulteriormente le attività di routine all'interno di aziende e governi.

Ogni ondata di digitalizzazione ha una serie specifica di impatti sociali ed economici. Le reti informatiche, a banda larga e di telefonia mobile sono state migliorare la scalabilità del settore (ovvero la capacità di una società di sostenere o migliorare le sue prestazioni in termini di redditività e di efficienza quando aumenta il suo raggio d'azione o il suo volume di vendite), consentendo così ai settori tradizionali dell'economia di crescere più rapidamente. L'attenuazione del vincolo di risorse (risorse reperibili più facilmente) ha portato a un aumento della domanda di manodopera nelle industrie dei servizi (ad es. Servizi finanziari,

istruzione, assistenza sanitaria, ecc.), Sebbene abbia avuto anche un effetto positivo nella produzione, infine, la prima ondata sembra aver avuto un impatto sulla crescita del reddito familiare e sulla facilitazione dell'inclusione sociale, come per esempio un maggiore accesso alle informazioni, un miglioramento nei servizi governativi e una maggiore offerta nei contenuti di intrattenimento grazie al collegamento e al cablaggio della rete.

La seconda ondata di digitalizzazione ha portato all'introduzione di nuovi servizi e applicazioni come la ricerca di informazioni su Internet, il commercio elettronico, l'istruzione a distanza e tutta una serie di attività collaborative che caratterizzano l'economia digitale (Uber, airbnb, ecc.). Questo "effetto innovazione" ha prodotto una maggiore domanda di manodopera in alcune occupazioni legate allo sviluppo di servizi digitali o all'emergere di modelli di business collaborativi, insieme alla scomparsa di lavori ripetitivi a bassa e media qualifica derivanti dall'automazione delle attività.

La terza ondata di digitalizzazione ha implicazioni significative per i miglioramenti della produttività, come vedremo successivamente. Promette inoltre di avere benefici significativi sul benessere sociale, in particolare su diversi obiettivi di sviluppo sostenibile, associati alla fornitura di servizi pubblici.

Le prove finora per quanto riguarda gli effetti dirompenti sul lavoro della terza ondata sono piuttosto speculative (Raul L. Katz, 2017), a meno che non si creda che l'interruzione della terza ondata sia semplicemente la fine di alcuni effetti della seconda ondata di digitalizzazione.

1.2 – IMPATTI SOCIO-ECONOMICI DELLE TRE ONDATE DIGITALI

È già stato anticipato prima come si caratterizzano le tre ondate digitali.

La prima ondata della digitalizzazione si configura con l’introduzione e adozione delle cosiddette tecnologie “mature”, ovvero tutti i sistemi informativi gestionali finalizzati all'automazione del trattamento dei dati e applicati al monitoraggio e rendicontazione dell'andamento aziendale, tecnologie di telecomunicazioni quali la banda larga (fissa e mobile) e le telecomunicazioni vocali (fisse e mobili) che consentono l'accesso remoto delle informazioni.

La seconda ondata di digitalizzazione ha comportato la diffusione di Internet e delle sue piattaforme corrispondenti (motori di ricerca, mercati). In aggiunta all'adozione di Internet, questa ondata ha portato alla diffusione del cosiddetto "cloud computing", ovvero quella "tecnologia informatica che consente la distribuzione di servizi di calcolo, come server, risorse di archiviazione, database, rete, software, analisi e intelligence, tramite Internet ("il cloud"), per offrire innovazione rapida, risorse flessibili ed economie di scala" (Anon., s.d.)

La terza ondata di digitalizzazione ha portato l'adozione di una serie di tecnologie avanzate, con l'intento di migliorare l'elaborazione delle informazioni e la qualità del processo decisionale, automatizzando ulteriormente le attività di routine all'interno di aziende e governi. Queste comprendono:

- Big data/analytics: definiti come la capacità di elaborare una serie (set) di dati estremamente grandi per estrarre informazioni e identificare modelli di relazione (correlazione, causalità) tra i dati. I campi di applicazione più comuni vanno dal marketing e dalla progettazione dei processi aziendali (privato) , alla ricerca epidemiologica e sui cambiamenti climatici (pubblico)
- Internet of things (IoT): ovvero la "connessione fra tutti gli oggetti grazie alla tecnologia digitale, quindi la capacità degli oggetti di essere connessi e di poter scambiare dati e informazioni fra di loro" (Mele, 2020). Prevede piattaforme che collegano più sensori e dispositivi di dati al fine di generare una visione completa del comportamento di un'organizzazione, un sistema, un'operazione aziendale o un fenomeno. Le applicazioni più comuni sono l'agricoltura di precisione (che controlla i fertilizzanti, monitora la pioggia e determina il raccolto più appropriato), le città intelligenti (che consentono il controllo dei flussi di traffico o gestiscono l'uso di energia nei luoghi pubblici) e la telemedicina (che monitora la salute dei pazienti ospedalieri).
- Robotica: implica l'applicazione della tecnologia digitale all'esecuzione di compiti manuali ripetitivi, come quelli richiesti per l'assemblaggio di automobili, la raccolta agricola e l'esplorazione in ambienti pericolosi.
- Stampanti 3D: è una tecnologia che permette la creazione di oggetti mediante stampa successiva di materiali adesivi come i polimeri. Sebbene le applicazioni della stampa 3D siano molto diffuse, il suo utilizzo è abbastanza comune nella progettazione di prodotti (protesi medicinali, modelli architettonici, design tessile)

e nello sviluppo di parti di ricambio (nell'elettronica di consumo e nei prodotti industriali)

- Intelligenza artificiale (AI) / apprendimento automatico: queste due tecnologie non sono equivalenti, sebbene condividano alcuni concetti comuni. L'apprendimento automatico è un'applicazione di intelligenza artificiale che consiste nello sviluppo di programmi che consentono a un computer di apprendere routine senza essere necessariamente precedentemente programmato. In questo senso, il programma di apprendimento automatico si trasforma una volta che inizia a elaborare le informazioni. Le applicazioni di machine learning più comuni sono auto a guida autonoma, consigli sui prodotti online, piattaforme Internet come Amazon e Netflix, rilevamento di frodi nell'utilizzo della carta di credito e calcolo del profilo di credito al consumo.

Queste tecnologie non vengono utilizzate in maniera autonoma ma sono integrate con le tecnologie "mature" della prima e seconda ondata. Pertanto, la cosiddetta "industria 4.0" viene ricercata attraverso l'assemblaggio delle tecnologie mature con quelle innovative per rispondere ai cambiamenti aziendali. L'avanzamento della terza ondata è rallentato dal necessario incorporamento delle tecnologie più avanzate, come AI e apprendimento automatico. Parte di questo ritardo è dovuto alla difficoltà di far comunicare tra loro due o più tecnologie sviluppate diversamente e, inoltre, anche agli elevati investimenti necessari per lo sviluppo e l'attuazione in più campi di queste tecnologie. Importante è notare come lo sviluppo in alcune aree (sociali, lavorative. Governative) è correlato a problemi etici e/o di privacy laddove l'industria e le organizzazioni sono sempre un passo avanti rispetto alla società e agli individui per quanto riguarda lo sviluppo di regolamenti e linee guida su un piano etico. (Newell & Marabelli, 2014).

Di seguito una tabella per riassumere le tre ondate delle tecnologie digitali mostrando la tipologia di innovazione, quando è stata sviluppata, quando è stata adottata in larga scala e quando si sono manifestati gli effetti socioeconomici

Tabella 1 - Ondate tecnologiche

Innovazione tecnologica	**Sviluppo**	**Adozione**	**Impatti socioeconomici**
Computer, banda larga, telecomunicazioni	1950-1975	1960 – 2000	1990 – 2010
Internet, piattaforme online, cloud computing	1970 – 1990	1995 – presente	2005 – presente
IoT, Robotics, AI, autoapprendimento	1980 – presente	2010 – presente	2020 - presente

Stabilito quanto mostrato, risulta pertinente anche mostrare gli impatti socioeconomici di ciascuna ondata. Verranno analizzate le conseguenze sulla crescita economica, sulla creazione di posti di lavoro e sul benessere sociale

1.2.1 – Conseguenze socioeconomiche della prima ondata

La digitalizzazione basata sulle tecnologie mature ha fornito un modo per consentire alle imprese di espandersi riuscendo a soddisfare la domanda finale aggiuntiva e creando una maggiore necessità di lavoro. I fattori positivi che hanno contribuito alla crescita economica sono molteplici. Innanzitutto, l'introduzione nei processi aziendali di tecnologie più efficienti supportate da quelle ICT ha portato a una maggiore produttività (Atkinson, et al., 2009). Di conseguenza c'è stata una crescita dei ricavi dovuta ad una maggiore copertura del mercato (Gillet, et al., 2006) che ha impattato fortemente sulla composizione e diffusione delle catene del valore per l'industria. Infatti, le tecnologie digitali di questa ondata hanno potuto attrarre posti di lavoro da altre regioni grazie anche alla possibilità di offrire servizi a distanza come l'outsourcing e i centri di assistenza clienti virtuali (Greenstein & Prince, 2006). Tutto questo è avvenuto mentre crescevano parallelamente le industrie nel settore dei servizi come quelle per lo sviluppo di software e di outsourcing dei processi aziendali (Crandall, et al., 2007).

La prima ondata ha apportato un altrettanto e significativo contributo all'occupazione grazie alla creazione di posti di lavoro dovuti alla costruzione e allo sviluppo delle reti di

telecomunicazione. Secondo Crandall, et al. (2007) si è visto come ci sia stata una concentrazione di nuovi posti di lavoro nel settore dei servizi riguardanti la banda larga specialmente negli ambiti di servizi finanziari, istruzione e assistenza sanitaria. Inoltre, si è riscontrato un effetto positivo anche nel settore manifatturiero, in quello del commercio all'ingrosso e in quello della sanità, dovuto al trasferimento delle imprese dalle grandi città in zone degli Stati Uniti più urbane e locali o di periferia, creando delle piccole comunità o migliorando la qualità della vita di quelle già esistenti, dando lavoro ai residenti (Katz, et al., 2011). A livello mondiale, tra il 2004 e il 2015, si è verificato un aumento dell'1% nell'indice di digitalizzazione che si è tradotto in una riduzione dello 0,07% del tasso di disoccupazione (Katz, & Callorda,, 2014). In Europa, nello stesso periodo, il moltiplicatore per nuovi posti di lavoro in zone locali nel ramo high-tech era intorno al cinque (Goos,, et al., 2015). Ciò nonostante, alcune industrie come quella dei servizi di alloggio o quella di ristorazione, in fase di adozione della banda larga hanno ridotto i il numero di posti di lavoro portando quindi un processo di sostituzione capitale/lavoro (Katz, et al., 2011). Su alcuni settori (manifatturiero, agricolo, servizi), quindi, la digitalizzazione ha creato nuovi posti di lavoro mentre su una piccola parte delle attività nel terziario ha impattato negativamente in quanto la forza lavoro umana è stata sostituita da quella digitale.

Negli ultimi anni, l'implementazione di indagini su scale nazionali sulle famiglie in possesso di sistemi ICT ha permesso di ricercare l'impatto sul benessere sociale della prima ondata di digitalizzazione: L'adozione della tecnologia a banda larga ha avuto il boom intorno all'anno 2000, con un tasso di crescita del 3.67% mensile (5.01% nelle famiglie con un PC). (Katz, & Callorda,, 2014).
La banda larga sembra aver avuto un impatto sulla crescita del reddito familiare attraverso quattro effetti. In primo luogo, l'implementazione della banda larga richiedeva la costruzione di infrastrutture per fornire il servizio (l'effetto "costruzione" di cui sopra), lavoratori aggiuntivi per i nuovi uffici commerciali di ciascun operatore e personale tecnico per l'installazione e la manutenzione della nuova infrastruttura. Una maggiore occupazione si traduceva in un aumento di reddito. Una seconda spiegazione per l'aumento del reddito è che, come si vede in Katz (2012) la banda larga ha un effetto positivo sulla produttività dei lavoratori e, pertanto, una maggiore produttività del lavoro produce salari più elevati.
In terzo luogo, i risultati della ricerca di Katz hanno mostrato anche che l'effetto della diffusione della banda larga è stata maggiore per chi possedeva un computer che permetteva la connessione a Internet. In questo senso, l'introduzione della banda larga ha consentito ai

lavoratori con competenze digitali e informatiche di segnalarsi più facilmente a potenziali datori di lavoro e poter richiedere salari più elevati. Infine, l'introduzione delle ICT ha aiutato a ridurre il tempo altrimenti richiesto per una ricerca efficace di lavoro, consentendo ai lavoratori sottoccupati di cercare lavoro a tempo pieno utilizzando i servizi a banda larga. Questo aumento dell'efficienza ha portato inevitabilmente a una riduzione dei periodi di disoccupazione individuale e ha conseguentemente generato un aumento della migrazione dei lavoratori sottoimpiegati verso posizioni a tempo pieno, ovviamente a reddito più elevato. In altre parole, la riduzione dei costi di transazione relativi alla ricerca di un impiego ha portato alla fine a un reddito più elevato (con meno tempo dedicato alla ricerca, i sottoccupati hanno potuto trovare un lavoro a tempo pieno).

1.2.2 – Conseguenze socioeconomiche della seconda ondata

Gli impatti socioeconomici della seconda ondata possono essere riassunti in tre categorie: 1) crescita economica dovuta alle combinazioni di tecnologie innovative; 2) impatto sulla forza lavoro; 3) effetti negativi sul benessere sociale.

La seconda ondata è stata caratterizzata dall'introduzione di nuovi servizi e applicazioni come la ricerca di informazioni su internet (il "search" di Google), il commercio elettronico (EBay, Amazon, Alibaba etc.…) l'istruzione telematica e l'avvento dei social networks. Il risultato più rilevante di questa seconda ondata è stata l'adozione combinata di piattaforme, banda larga e cloud computing, che ha posto le basi per un ampio mercato di creazione di contenuti e applicativi internet, di attività collaborative, che hanno caratterizzano l'economia digitale attuale. Congiuntamente, le piattaforme B2B (Business to Business) e B2C (Business to Consumer) per le vendite online hanno consentito alle imprese di allargarsi su scala internazionale rivolgendosi più facilmente ai mercati esteri, producendo a loro volta una maggiore occupazione.

Tuttavia, questo maggiore utilizzo delle tecnologie digitali ha creato una dipendenza da Internet e i suoi servizi, che, come conseguenza, si è tradotta in un potenziale effetto economico negativo dovuto alla sua possibile interruzione. A titolo esemplificativo, Howard, et al., (2011), nel loro studio di ricerca, hanno identificato 606 chiusure di internet imposte dal governo tra il 1995 e la prima metà del 2011 in 99 paesi. Solo nel 2010, 111 sono stati gli

arresti causati da errori umani. Dalla seconda metà del 2010 e fino al 2016 sono state identificate 81 interruzioni imposte solo dal governo americano (West, 2016). Internet risulta ormai vitale per lo sviluppo economico. Pertanto, è ragionevole pensare a quali possano essere gli impatti negativi di un suo blocco a seguito di un'emergenza naturale, di criminalità informatica, fallimento tecnologico oppure di un blackout per motivi politici.

Riguardo alla forza lavoro la seconda ondata ha impattato in tre modi. Il primo, negativo, eliminando e modificando alcuni lavori in seguito all'automazione di determinate mansioni soprattutto nel settore agricolo e manifatturiero (Brynjolfsson, & McAfee, 2014). In ogni caso, i lavori manuali specifici difficilmente vengono eliminati perché secondo Sachs & Lawrence, (2012), gli effetti negativi dell'automazione si riscontrano su livelli di occupazione di bassa competenza e, inoltre, perché la creazione di posti di lavoro dovuta alla seconda ondata non può eliminare completamente i posti di lavoro ma, tutt'al più, modificarli.
In modo positivo, invece, creando nuovi posti di lavoro specifici come ingegneri informatici specializzati o tecnici/operatori dedicati. La letteratura tuttavia riporta pareri contrastanti a riguardo, anche se il consenso è quello per cui l'effetto della creazione di posti di lavoro derivanti dalla seconda ondata di digitalizzazione, nonostante appunto le nuove occupazioni, non sia stato sufficiente da sopperire la scomparsa di posti di lavoro come discusso prima. (Berger & Frey, 2016; Hlatshwayo, & Hlatshwayo, 2012). Lin, (2011) sostiene invece che la creazione di posti di lavoro è stata forte come nel caso della prima ondata ma si è successivamente affievolita, scemando un po' alla volta. Attraverso l'analisi della seconda ondata sono stati identificati anche determinati cluster dell'occupazione. Le tecnologie digitali si sono diffuse in larga scala tra professioni e industrie e la domanda di lavoratori con capacità analitiche e di risoluzione di problemi è aumentata (Katz, et al., 2003). Inoltre, l'offerta di capitale umano altamente specializzato non è riuscita a stare al passo con la domanda innescata dal cambiamento tecnologico; questo ha portato ad un aumento dei salari delle professioni altamente specializzate (Acemoglu & Katz, 2011). Parallelamente, le attività manuali non di routine prevalenti nelle professioni del settore dei servizi, non essendo sostituibili dai computer e combinate con la domanda di occupazioni a reddito elevato, hanno determinato l'aumento dei lavori a bassa qualifica. Infatti, nuovi posti di lavoro in ambito tecnologico creano comunque una domanda aggiuntiva di servizi locali in quanto le aziende, una volta digitalizzate, si ampliano e necessitano comunque di personale (Katz & Dorn, 2013) (Moretti, 2010).

In sostanza, la scomparsa dei lavori di media qualificazione e la crescita dell'occupazione nella fascia alta insieme alla fine dei lavori più di routine viene definita come "polarizzazione del lavoro". La riduzione dei lavori di routine è stata registrata in tutte le economie appartenenti all'OECD ("Organization for Economic Co-operation and Development", trad. "Organizzazione per la cooperazione e lo sviluppo economico") (Goos, et al., 2014). Secondo Akerman, et al., (2015), i principali motori di questa polarizzazione del lavoro nei paesi sviluppati sono stati, per l'appunto, le tecnologie digitali e l'automazione.

La letteratura asserisce che gli effetti dell'automazione modificheranno sempre di più, come precedentemente visto, i settori ad alta intensità di lavoro dove le mansioni sono ripetitive e avranno un grande impatto sui lavori a bassa qualifica. Questi effetti saranno sempre più frequenti e si verificheranno sempre più velocemente grazie alla richiesta di capitale intangibile (cambiamenti organizzativi, innovazione dei processi aziendali) da parte delle imprese e dal crescente potenziale delle tecnologie digitali legate alla terza ondata di digitalizzazione come vedremo in seguito.

Per quanto riguarda gli impatti sul benessere sociale, questi sono stati riscontrati prevalentemente negativi. Prima fra tutti una degenerazione delle relazioni umane risultante dall'utilizzo massiccio delle tecnologie digitali (smartphone, gaming console, pc) soprattutto nei giovani (Turkle, 2016). Sempre tra i giovani, un secondo effetto negativo è stato riscontrato nel lento declino di altre attività parallele alla formazione culturale e personale come, per esempio, la lettura. Un terzo effetto negativo che è stato studiato nei paesi in via di sviluppo è quello che si può definire "sradicamento culturale". (Katz, et al., 2014). Come risultato della ricerca, è stato dimostrato come nei paesi maggiormente sviluppati una grande percentuale dei siti Internet navigati appare essere locale (creati, sviluppati su base nazionale) e con contenuti internazionali e nelle aree con specificità linguistiche (ad esempio la Russia) sia siti e sia contenuti tendono a essere locali. D'altro canto, le regioni in via di sviluppo che hanno una lingua di quelle maggiormente usate (America Latina con lo spagnolo, il sud dell'Asia con l'inglese e infine sia inglese che francese per l'Africa e l'area MENA) tendono ad avere meno contenuti di tipo locale. Così facendo, il rischio in cui si incorrono questi paesi è quello di uno sradicamento culturale dovuto appunto da una produzione limitata di contenuti locali con una maggiore influenza di culture estere.

1.2.3 – Conseguenze socioeconomiche della terza ondata

La terza ondata di digitalizzazione ha implicazioni significative per i miglioramenti della produttività. I progressi della robotica, dell'analisi dei big data e dell'apprendimento automatico hanno già prodotto applicazioni che, se adottate su larga scala, dovrebbero avere un impatto positivo riducendo significativamente i costi operativi.

Poiché queste applicazioni sono ancora in fase di sviluppo, non è ancora possibile quantificare il loro impatto a livello macroeconomico, anche se cominciano a manifestarsi le prime adozioni, specialmente in campo manifatturiero e sanitario con notevoli riduzioni dei costi operativi. Inoltre, tornando alla distinzione tra innovazione tecnologica, diffusione e impatto economico, è abbastanza difficile prevedere la velocità con cui verranno adottati. Ad esempio, è probabile che alcune di queste piattaforme saranno adottate solo da alcune grandi aziende in settori con costi operativi elevati con l'intento di ridurli. Pertanto, al di là di aziende come Amazon che ha già iniziato ad adoperare queste tecnologie e con alti costi di adempimento (vedi il fenomeno "AmazonGo" analizzato da Polacco & Backes, 2018) e grandi operatori di telecomunicazioni (colpiti dagli alti costi dei call center) (Ismagilova, et al., 2017), è improbabile che l'adozione proceda a un ritmo rapido. La letteratura è concorde sul fatto che sia necessario, al fine di adottare tali piattaforme, un cambiamento nei processi e negli aspetti organizzativi (Matt, et al., 2015), come verrà spiegato in seguito . Infine, molte di queste piattaforme pongono questioni fondamentali riguardanti la resistenza dei dipendenti, la mancanza di consapevolezza del management e persino considerazioni etiche (Greenwald, 2017).

Gli effetti di questa ondata si verificheranno entro un decennio o due e avranno impatti significativi. In primo luogo, ci si aspetta che le nuove infrastrutture digitali possano dare il via ad una nuova potenziale creazione di valore da parte delle imprese in quanto una diminuzione del costo medio di produzione dovuta all'automazione potrebbe consentire maggiori esportazioni (Maknkopf, 2019) . Di conseguenza, un aumento nella domanda e nell'offerta di prodotti e servizi nonché un aumento nella domanda di lavoro. In secondo luogo, le aziende si aspettano che la digitalizzazione dei processi produttivi e aziendali riduca i costi grazie alla riduzione di manodopera, di energia e materie prime. Questo porterebbe alla scomparsa dei posti di lavoro a meno che il ritmo, la portata e l'impatto di tale cambiamento non vengano accompagnata da investimenti nella formazione (Figueroa, 2018). Infatti,

nell’attuale fase iniziale di sviluppo della digitalizzazione è difficile stimare gli effetti sul mercato del lavoro.

Nonostante i fattori relativi al tempo di adozione, la terza ondata di digitalizzazione promette di avere un impatto positivo sull'occupazione. La ricerca è raggruppata attorno a due argomenti di sviluppo futuri: uno che prevede una drammatica scomparsa di posti di lavoro a causa dell'automazione, e un secondo che stabilisce che gli effetti negativi sull’occupazione sono sopravvalutati.

L'assunto principale a sostegno del primo corpo di ricerca è che l'automazione di mansioni ripetitive, collegata alla robotica e combinata con una maggiore potenza della tecnologia in settori come l'intelligenza artificiale e il riconoscimento vocale, è collegata alla scomparsa dei posti di lavoro. Ad esempio, Frey & Osborne, (2013) stimano che quasi la metà dei posti di lavoro negli Stati Uniti sarà a rischio a causa dell'automazione nei prossimi decenni, mentre i lavori che richiedono creatività e complesse interazioni sociali sono a basso rischio di essere sostituiti. Per coincidenza, McKinsey (2015) stima che il 45% delle attività svolte dai lavoratori statunitensi sia automatizzabile con la tecnologia esistente. Allo stesso modo, Bruegel (2014) stima che il 45% dei posti di lavoro nell'UE è a rischio di automazione, dal 40% al 60% in Romania, Bulgaria, Grecia, Portogallo e Svezia. Queste ricerche trovano un riscontro in quanto uno studio condotto sempre dal McKinsey Global Institute, (2017), ha stimato che nel futuro prossimo la maggior parte delle vendite di automi sarà concentrato nei cinque mercati di Cina, Corea del Sud, Giappone, USA e UE, ovvero le aree maggiormente sviluppate tecnologicamente

La premessa principale del secondo corpo di ricerca è che non tutti i posti di lavoro possono essere sostituiti dall'automazione e che la creazione di posti di lavoro derivata da nuove innovazioni e/o aumento della produttività e della spesa può effettivamente annullare qualsiasi effetto di interruzione. Alcune ricerche riconoscono che la creazione di posti di lavoro guidata dall'innovazione non compenserà mai la perdita di posti di lavoro guidata dall'automazione, ma che i nuovi posti di lavoro saranno innescati da un aumento del potere d'acquisto dei consumatori che comporterà una domanda maggiore di beni e servizi e quindi un’offerta maggiore di posti di lavoro (Atkinson e Wu, 2017) (Figueroa, 2018). In questo senso, la preoccupazione di questi ricercatori è che se la produttività non aumenta, il tenore di vita non migliorerà.

La terza ondata di digitalizzazione promette di avere benefici significativi sul benessere sociale, in particolare su diversi obiettivi di sviluppo sostenibile, come una migliore sanità un miglior benessere sociale, energia accessibile e pulita, lavoro dignitoso, crescita economica e città sostenibili. Ad esempio, i Big data saranno fondamentali nei settori relativi alla sanità e ai servizi di pubblica amministrazione, basti pensare all'immenso lavoro di datificazione fatto per monitorare la diffusione del virus durante la pandemia causata dal Covid-19 (Fahey & Hino, 2020). Allo stesso modo, le applicazioni di e - Government riducono i tempi di viaggio necessari per condurre transazioni nelle pubbliche amministrazioni (Purwanto, et al., 2020). Inoltre, si sostiene che le tecnologie digitali offrano un incentivo per la trasformazione a basse emissioni dei sistemi energetici e di mobilità (trasporti) e che abbiano infatti un notevole impatto sull'economia circolare e sulla salvaguardia dei sistemi ecologici. L'impatto ambientale sembra essere il tema più discusso, in parte grazie agli studi relativi alla Green Economy (Loiseau, et al., 2016) e sul benessere della società gli impatti sono apparentemente positivi. Tuttavia, l'altro lato della medaglia rivela degli effetti tutt'altro che positivi. Se le auto elettriche alimentate a batteria (BEV) e quelle a celle combustibile (FCEV) sembrano essere la migliore soluzione possibile per la mobilità del futuro con quasi il 30% sulle vendite totali nel 2030 (50% in Cina) (Gao, 2016) è altresì vero che per la loro produzione, le auto elettriche hanno bisogno di quattro volte tanto il materiale necessario rispetto alle auto tradizionali con motore endotermico (benzina, diesel, gas) e hanno bisogno anche di materiali come il cobalto o litio e altri materiali rari (DERA, 2016). Per definizione, tali metalli sono rari in quanto, oltre alla scarsità di reperimento, il processo metallurgico per separarli risulta complesso. Questo significa che per far fronte a una sempre più maggiore richiesta di auto elettriche, il reperimento di tali materiali impatterà sulla deforestazione generata dagli scavi delle miniere, generando maggiori danni ecologici e sempre più frequenti conflitti con le popolazioni locali. Le tecnologie "smart" dentro le nostre case sembrano avere un impatto positivo in termini di risparmio di energia. Ma è anche vero che bisogna considerare un maggiore uso di elettricità per i sempre più frequenti dispositivi "smart" e per le crescenti infrastrutture ICT su cui si basa il sistema (Gossart, 2015). Per quanto riguarda il mondo AI e IoT, il "cloud"è diventato uno snodo centrale e fondamentale. Questa tecnologia, dove le persone acquistano, socializzano, prestano, votano e fanno operazioni di banca, è a tutti gli effetti un'infrastrutture fisica composta da cavi telefonici e in fibra ottica, satelliti, cavi sul fondo degli oceani e depositi colmi di computer che consumano una grande quantità di metalli, acqua ed energia (Delforte, 2016). Questi depositi, più grandi di portaerei, posseduti dalle Big Tech quali

Alphabet, Amazon, Apple, Facebook, Google e Microsoft (Ba Alibaba, Baidu, Tencent in Cina), sono chiamati “Data center”. Grazie all’avvento dei contenuti digitali, dell’e-commerce e del traffico dei *data* su Internet, questi centri sono diventati l’ossatura portante dell’economia digitale e stanno diventando i più grandi consumatori di elettricità nei paesi sviluppati e una dei fattori chiavi nella costruzione di centrali elettriche. Vidal (2017) sostiene che questi centri arriveranno a consumare un quinto dell’energia globale nel 2025, diventando così uno dei più grandi fattori di inquinamento.

Riassumendo, con l’esplosione dell’intelligenza artificiale e i dispositivi connessi a Internet aumenterà il consumo di energia di tutta l’infrastruttura CIT, La grande industria ICT acquisterà sempre più elettricità da fonti energetiche rinnovabili ma questa non è affatto una buona notizia perché la capacità di energia rinnovabile non è più disponibile per altri scopi (Jones, 2018).

Inoltre, come già detto, l'infrastruttura digitale necessita anche di un'enorme quantità di metalli, che devono essere estratti (di solito con un enorme impatto ecologico e sociale) e quindi trasportati dai luoghi di origine ai luoghi in cui verranno elaborati e consumati. Diversi metalli e minerali sono considerati 'critici' perché sono necessari per molti scopi diversi come la produzione di energia rinnovabile, la trasmissione di sistemi militari di energia e la digitalizzazione (DERA, 2016). Secondo lo studio promosso dalla DERA, comparando la domanda globale di materie prime necessarie allo sviluppo di tecnologie digitali nel 2013 e nel 2035, entro tale data dovranno essere disponibili quattro volte la quantità di litio, tre volte la quantità di materie rare pesanti, una volta e mezza la quantità di materie rare leggere e tantalio. La domanda globale di rame potrebbe persino aumentare tra il 300 e il 400 percento nei prossimi decenni.

Oltre ad aspettarsi `` opportunità di business multimiliardarie '' grazie all'elettrificazione e alla guida autonoma nei prossimi anni, la banca d'investimento svizzera UBS calcola che i soli veicoli elettrici potrebbero decuplicare il mercato delle batterie entro il 2025, il che determinerebbe un aumento di oltre il 40% del consumo di nichel e più del doppio dell'uso del cobalto; ma si stima che anche la domanda di grafite si moltiplichi da sole 13.000 tonnellate nel 2015 a oltre 800.000 tonnellate nel 2030 (Maler, 2012).

Risulta chiaro come i benefici sulla società e sulle persone dovuti alla digitalizzazione siano prettamente positivi. Tuttavia, i risvolti ecologici e ambientali previsti e che impattano anche

a livello geopolitico sui paesi ricchi di materie prime necessarie al continuo sviluppo sono assolutamente allarmanti.

1.3 – TRASFORMAZIONE DIGITALE

1.3.1 – Trasformazione digitale, definizione

Analizzando la letteratura esistente, 282 lavori sul tema della "digital transformation" derivanti dalla letteratura sull'IS (information system), Vial (2019) definisce la trasformazione digitale (in seguito DT) come "*un processo che mira a migliorare un'entità innescando modifiche significative alla sua proprietà attraverso combinazione di tecnologie di informazione, elaborazione, comunicazione e connettività"* mentre Verhoef, et al., (2021) danno la seguente definizione: *"un cambiamento nel modo in cui un'azienda impiega le tecnologie digitali per sviluppare un nuovo modello di business digitale che aiuti a creare e ad appropriarsi di più valore per l'azienda"*.
Quest'ultima definizione è più specifica poiché fornisce informazioni dettagliate riguardo il soggetto interessato (*azienda*), l'oggetto (*cambiamento*) e il motivo dell'oggetto (*creazione e appropriamento del valore*). Inoltre, specifica anche come questo cambiamento avvenga (*sviluppando un modello di business*) e tramite quale mezzo (*tecnologie digitali*). Per la definizione proposta da Vial, invece, è necessario fare tre importanti osservazione. La prima è quella per cui, riferendosi al soggetto come "*entità*", l'attenzione non è incentrata sull'azienda ma è correlato al concetto di *digitalizzazione* che include quello di individuo in senso ampio, le organizzazioni e il contesto sociale. La seconda osservazione si focalizza sul termine "*miglioramento",* inteso come un risultato previsto della DT ma non necessariamente garantito. In ultima analisi, il mezzo attraverso cui viene ricercato tale miglioramento non viene definito come "tecnologia digitale" ma attraverso un insieme (*combinazione*) di diverse tecnologie. Tale uso risulta un valido compromesso poiché fa sì che questa definizione sia valida e applicabile nel tempo, a seguito del cambiamento delle varie tecnologie.

La DT è un approccio multidisciplinare per sua stessa natura in quanto comprende cambiamenti relativi a diversi ambiti come la strategia e l'organizzazione aziendale, il comparto IT, il marketing e tutti i servizi di logistica. Inoltre, racchiude tutte le tecnologie

sotto l'acronimo SMACIT (Sebastian, et al., 2017), ovvero "*social, mobile, analytics, cloud, IoT".* Tutte queste tecnologie (*"platform"* incluse) risultano rilevanti nel contesto della DT solo se combinate (Gunther, et al., 2017).

1.3.2 – Digital transformation, perché?

I motivi per cui si è giunti alla DT hanno carattere esogeno rispetto ai soggetti interessati (tali soggetti saranno analizzati in seguito). Verhoef, et al., (2021) identificano tre fattori che hanno portato alla DT. Un primo fattore è relativo al cambiamento del comportamento dei consumatori e delle loro abitudini d'acquisto in risposta alla rivoluzione digitale. Grazie all'utilizzo di strumenti sempre più evoluti come gli strumenti di ricerca e i social media, i consumatori sono diventati sempre più connessi, informati e attivi (Lamberton & Stephen, 2016). Sono cambiati i punti d'accesso anche per reperire le informazioni, tant'è che nelle nostre vite sono entrate le AI, come Amazon Alexa o Google Home ma, in linea generale, si è notato il passaggio a touchpoint digitali anche per gli acquisti (Kannan & Li, 2017). Queste tecnologie continueranno a modificare il comportamento dei consumatori e l'uso di tali tecnologie diventerà sempre più un *modus operandi* standard (Hoffman & Novak, 2017).
Un secondo fattore fa riferimento allo sviluppo di un gran numero di tecnologie, già dall'avvento del World Wide Web e della sua adozione, a supporto dell'e-commerce. Come già detto precedentemente, Big Data, AI, IoT e automazione avranno un forte impatto sull'economia (Ng & Wakenshaw, 2017), soprattutto sulla struttura dei costi attraverso la sostituzione della forza lavoro con quella automatica o l'ottimizzazione dei flussi logistici con la riduzione dei costi della *supply chain* grazie all'uso dell'intelligenza artificiale.
Infine, è cambiato anche il livello competitivo generale grazie all'uso di queste tecnologie. Nel retail, le "*disruptive Technologies"* ("tecnologie dirompenti") hanno imposto cambiamenti e adattamenti a favore delle giovani imprese nate già con un animo digitale. Oltre che ad essere globale, il grado di competitività è anche aumentato. Basti pensare ai big tech americani (Alphabet, Amazon, Google, Facebook, Apple e Microsoft) e cinesi (Ba Alibaba, Baidu, Tencent) che negli ultimi anni si sono imposti sul mercato mondiale.

1.3.3 – Digital transformation, i soggetti interessati

La DT è diversa da soggetto a soggetto. Secondo Verhoef, infatti, il cambiamento riguarda specificatamente l'azienda. Ci sono tre tipologie di aziende, quelle orientate al prodotto, quelle che offrono prevalentemente servizi e quelle incentrate esclusivamente su prodotti e servizi tecnologici (Saarikko, et al., 2020). A prescindere dalle dimensioni, tali aziende hanno aspettative, ambizioni e interessi differenti verso il fenomeno della DT ma, tuttavia, si scontrano inequivocabilmente con gli stessi problemi. Le differenze sostanziali tra le tre tipologie di aziende riguardano i ruoli e le *business units* coinvolte. Per quanto riguarda le aziende manifatturiere (orientate al prodotto), vengono interessati i reparti produttivi (automazione, soluzioni Iot) e di assistenza post vendita. Per le imprese nel settore dei servizi sono coinvolte tutte le unità che beneficiano da un passaggio alle tecnologie digitali, vale a dirsi, tutte. Il maggior problema che affrontano, però, risiede nella difficoltà del diffondersi e creare sinergie tra le loro *business units.* Inoltre, le imprese hanno dovuto adattarsi. alla grande diffusione e adozione dei prodotti connessi ad Internet (IoT), In ultima analisi, e imprese a carattere digitale sono quelle che offrono prodotti e servizi alle altre due tipologie di azienda. Esse provvedono alla fornitura sia delle infrastrutture necessarie che dei prodotti stessi. A differenze delle altre due non hanno interesse nel conoscere o possedere i *data* ma rimangono imparziali nonostante possano fornire i servizi di immagazzinaggio dei dati generati dai consumatori. Il loro ruolo è solo quello di elaborare e inoltrare i dati nel modo richiesto dal cliente.

1.3.4 – Fasi della digital transformation

Abbiamo già dato la definizione di "digitalizzazione" e "trasformazione digitale" ma la letteratura in lingua inglese utilizza tre termini per identificare tre diverse situazioni.
La prima è "*digitization"* è fa riferimento alla semplice trasposizione su formati digitali di contenuti e informazioni in formato analogico (0 , 1 – codice binario) (Loebbecke & Picot, 2015) e anche il cambiamento delle mansioni dall'analogico sempre al digitale (Vendrell-Herrero, et al., 2017) In linea di massima, *"digitization"* descrive l'azione di conversione dell'analogico in digitale.

La seconda è *"digitalization"* , di cui abbiamo parlato prima. Attraverso la *"digitalization"* le imprese utilizzano determinate tecnologie digitali per ottimizzare il lavoro e permettendo un miglior coordinamento dei processi e, a volte, creando valore aggiunto per il cliente migliorando le esperienze degli utenti (Pagani & Pardo, 2017). Pertanto, la digitalizzazione in questo senso non è incentrata solo sulla riduzione dei costi ma anche ai processi che porterebbero a migliorare le esperienze dei consumatori.
Infine, la *"digital transformation"* descrive un cambiamento a livello aziendale che porta allo sviluppo di nuovi modelli di business (Pagani & Pardo, 2017) implementando una nuova logica di business per creare e catturare valore (Gölzer & Fritzsche, 2017). Inoltre, influenza l'intera azienda e il suo modo di lavorare riorganizzando anche l'intero processo, la struttura organizzativa (Li, et al., 2018) e il processo di creazione del valore (Matarazzo, et al., 2021).

Riassumendo, nel tempo, un primo inizio di DT fa riferimento a quello del semplice passaggio dall'analogico al digitale interessando solamente gli asset e gli strumenti che un'azienda possedeva (entità). Questo ha portato a un notevole risparmio in termini di costi e tempo e una miglior allocazione delle risorse nelle mansioni già esistenti. Successivamente, con l'avvento delle nuove tecnologie, si ha avuto anche qui un risparmio nei costi e un incremento nei ricavi dovuto a una più efficiente produzione grazie alla riorganizzazione dei processi aziendali. In questa fase sono state introdotte tecnologie a supporto della produzione come l'automazione e, introducendo nuovi canali di distribuzione e di comunicazione digitali, si è iniziato a guardare miglioramento dell'esperienza degli utenti
Infine, con la DT, vengono introdotti nuovi modelli di business come le piattaforme digitali e modelli basasti sui *data*. In questa fase risulta appunto enorme l'apporto dei sistemi di analisi dei dati (*big data analytcs)* che migliorano sempre più l'impatto sui costi di gestione.

NATURA DELLE TECNOLOGIE DIGITALI
La letterature definisce le tecnologie digitali come *"disruptive"* per tre motivi:

1. Hanno alterato il comportamento d'acquisto dei consumatori, soprattutto di quelli che hanno accesso alle informazioni in qualsiasi momento e in qualsiasi modo. L'uso di queste tecnologie ha creato una nuova figura del consumatore, quella del *"prosumer"*, nel momento in cui i consumatori stessi sono diventati partecipanti attivi nel processo produttivo (Yeow, et al., 2018). Questo ha fatto sì che i consumatori non si sentissero più fortemente legati alle imprese e che le loro aspettative rispetto ai servizi a loro forniti fossero maggiori (Sia, et al., 2016). Da qui la risposta delle aziende che hanno

cominciato ad anticipare piuttosto che rispondere ai cambiamenti nelle aspettative dei consumatori.

2. Poiché hanno modificato il panorama competitivo attraverso al combinazione di prodotti e di servizi esistenti generando nuove forme di offerte digitali, abbassando le barriere all'entrata e ostacolando il vantaggio competitivo delle aziende già presenti (Barret, et al., 2015) (Kahre, et al., 2017). Ad esempio, le piattaforme digitali hanno facilitato lo scambio di beni e servizi digitali e, così facendo, le barriere all'ingresso si sono drasticamente ridotte.
3. Hanno aumentato la disponibilità dei *data*. Analizzando i *data*, le imprese hanno la possibilità di offrire servizi che meglio rispondono ai bisogni dei consumatori e/o rendono i processi più efficienti (tramite l'algoritmo decisionale, per esempio) e possono aumentare il proprio vantaggio competitivo (Gunther, et al., 2017). Inoltre, la raccolta dei *data* va a favore delle aziende per il loro interesse anche perché, vendendoli a terzi, forniscono la possibilità di avere dei profitti (Loebbecke & Picot, 2017)

1.3.5 – Digital transformation, risposte strategiche

Nonostante i possibili problemi causati dalle tecnologie digitali, le imprese devono continuare a essere competitivi sul mercato. Le tecnologie digitali, infatti, offrono sì grandi opportunità ma sono anche fonte di una grandi minacce a livello competitivo che gravano sulle imprese (Sebastian, et al., 2017). Data la natura multidisciplinare della DT, la letteratura fornisce due concetti strategici da poter intraprendere. Il primo è quello denominato *"digital business strategy"* (d'ora in avanti "DBS), e si riferisce ad una "strategia formulata e applicata utilizzando le risorse digitali disponibili al fine migliorare il processo di creazione del valore" (Holotiuk & Beimborn, 2017) (Leischnig, et al., 2017). Il secondo concetto si focalizza più sulla trasformazione dei prodotti, dei processi produttivi e degli aspetti organizzativi che derivano dall'utilizzo di determinate tecnologie digitali e viene denominata *"digital transformation strategy"* (DTS) (Matt, et al., 2015). La DTS è vista come " un progetto che supporta le aziende nel governare le trasformazioni che derivano dall'integrazione delle tecnologie digitali, così come nelle loro operazioni dopo una trasformazione". La DTS si distacca dalle strategie finalizzate alla creazione del valore della DBS perché si concentra sui cambiamenti strutturali

che, impattando sull'azienda, vanno a modificarne l'organizzazione intera. Questi cambiamenti sono postumi e devono essere accuratamente pianificati prima di essere attuati per sfruttare le tecnologie digitali senza che queste nuocciano negativamente a livello finanziario e vengono attuati a seconda degli effetti previsti. La struttura organizzativa risulterà flessibile, composta da *business units* autonome (Venkatraman, 2017) e separate dalla centrale operativa, dove poter sperimentare e imparare velocemente evitando il rischio di cannibalizzazione delle mansioni e possibili conflitti tra le unità. Per rispondere velocemente ai costanti cambi digitali, l'organizzazione deve risultare *agile* e flessibile nella sua organizzazione (Robertson, 2015). La tecnica "*agile"* è un approccio che enfatizza un modo di lavorare fatto di brevi periodi alla fine dei quali avviene un confronto tra gli operatori e dove vengono discusse di volta in volta possibili strategie sulla base di quanto fatto. Infine, oltre a una separazione delle unità di business, vengono identificate anche le aree funzionali con carattere digitale. Lo stesso reparto IT necessita di prendere parte attiva nel processo di creazione del valore digitale attraverso risposte sempre più repentine e precise (Leonhardt, et al., 2017). Gli stessi dipendenti devono ricevere un upgrade nelle competenze digitali, soprattutto in ambiti come il marketing e i servizi, per aumentare al più presto la creazione del valore (Lemon & Verhoef, 2016). La DT, come appunto detto, rischia di far sostituire la forza lavoro esistente con una maggiormente qualificata a livello digitale e analitico

1.3.6 – Digital business strategy

CREAZIONE DEL VALORE – RISORSE CHIAVE

Per quanto riguarda la DBS, in ottica del miglioramento del processo di creazione del valore vengono identificate alcune risorse, nonché alcuni cambiamenti, necessari alla trasformazione digitale:

- *Digital assets:* le aziende necessitano di alcune risorse tecnologiche per poter compere nell'era digitale. Ne sono un esempio tutta l'infrastruttura relativa alle comunicazioni, interne ed esterne all'azienda, le tecnologie che immagazzinano i dati e le informazioni e tutte le tecnologie (hardware e software) che consentono il lavoro delle AI, dell'automazione, dell'IoT e dei meccanismi di apprendimento automatico (Verhoef, et al., 2021). I progressi fatti attraverso queste tecnologie forniscono gli ingredienti base per sfruttare le conoscenze aziendali già esistenti per creare più valore per i clienti. Ad

esempio, tutti i dati raccolti riguardo i movimenti di un cliente sul sito dell'impresa, uniti alle competenze di analisi (automatiche e non) dei dati, danno la possibilità di personalizzare l'offerta e il servizio entrambi rivolti al consumatore. Infatti, le tecnologie digitali consentono la creazione di nuove proposte di valore che si basano sempre più sulla fornitura di servizi (Barret, et al., 2015). Le organizzazioni utilizzano le tecnologie digitali per passare da o aumentare le vendite di prodotti fisici contestualmente alla vendita di servizi a complemento della loro proposta di valore per soddisfare le esigenze dei clienti offrendo soluzioni innovative e per raccogliere dati sulle loro interazioni con prodotti e servizi (Wulf, et al., 2017). Netflix ne è un esempio interessante. Dal noleggio di film è passato a offrire un servizio streaming di video diventandone il maggiore provider. La raccolta di dati derivanti dall'utilizzo degli utenti ha permesso, negli ultimi anni, di personalizzare l'offerta e sviluppare al meglio i propri contenuti (Gunther, et al., 2017)

- *Digital agility:* la *digital agility* fa riferimento alla capacità di cogliere le opportunità del mercato derivanti dalle tecnologie digitali e adattarsi velocemente. Infatti, le imprese devono essere flessibili per consentire il cambio ripetuto dei ruoli organizzativi, per rispondere ai cambi nelle esigenze dei consumatori e all'introduzione di nuove tecnologie e per rispondere all'intensificarsi della concorrenza dovuta all'eliminazione di barriere all'ingresso. Essere agili vuol dire essere in grado di modificare e riconfigurare gli asset e le capacità digitali, anche con implicazioni sulla struttura organizzativa.

  Per giungere a un DT, infatti, è necessario ricombinare le risorse digitali con quelle strutturali e organizzative dell'azienda per modificare il processo lavorativo. Inoltre, si utilizza il termine "ambidestrismo" per indicare quell'abilità delle imprese di combinare con successo l'esplorazione di nuove risorse digitali innovative con l'utilizzo delle risorse già esistenti (Li, et al., 2018) (Svahn, et al., 2017).
- *Digital networking capability:* ovvero la capacità di creare una rete digitale dove viene selezionato, inserito e, infine, collegato un gruppo eterogeneo di stakeholder come ad esempio consumatori, fornitori e figure terze che stimolano fortemente il processo di creazione del valore e la crescita di piattaforme. Ne è un esempio il Technoweb 2.0 di Siemens, un social network interno aziendale globale che metteva in contatto i dipendenti stessi in parti diverse del mondo per ricevere assistenza su problemi che l'hub di riferimento non era in grado di risolvere (Wiener, et al., 2012). Le imprese

possono utilizzare le tecnologie digitali per migliorare una delle tre principali strategie di mediazione. In una strategie di "disintermediazione", le tecnologie bypassano gli intermediari e consentono gli scambi diretti tra i partecipanti di un network, come ad esempio i consumatori (Hansen & Sia, 2015). In una strategia di "riparazione", gli scambi tra i partecipanti di un network sono rafforzati poiché le tecnologie digitali consentono una stretta collaborazione e coordinamento tra i diretti interessati, ad esempio utilizzando una piattaforma per coordinare gli scambi all'interno di una catena di fornitura (Klötzer & Pflaum, 2017). Nella mediazione basata sulla rete, vengono create relazioni complesse tra più parti interessate con interessi potenzialmente concorrenti a vantaggio dei clienti. Le tecnologie digitali hanno, infatti, anche concesso ai clienti la possibilità di diventare co-creatori di valore (prosumer) all'interno di questi network. (Tan, et al., 2015). Per esempio, i social media e le comunità online dipendono quasi esclusivamente dai contributi attivi degli utenti che utilizzano queste tecnologie. Pertanto, le imprese sono invogliate anche loro a utilizzare queste tecnologie per connettersi ai consumatori e creare valore anche insieme a loro

- *Digital channels:* le aziende utilizzano le tecnologie digitali per implementare i cambiamenti relativi ai canali di distribuzione e di vendita. Questo può avvenire in due modi. Il primo, diretto, permette di raggiungere i consumatori e intrattenere dei rapporti con loro attraverso la creazione di nuovi canali (es. social media). Vista in ottica di omnicanalità, un canale di comunicazione permette all'azienda un confronto continuo con i propri consumatori. I social media, in questo caso, riescono a colmare velocemente il vuoto tra il fisico e il digitale. Un secondo modo, indiretto, è quello per cui, potenzialmente, l'azienda ha la possibilità di coordinare le attività di tutta l'azienda stessa. Questo è reso possibile dai meccanismi dell'algoritmo decisionale che viene applicato nelle sue tecnologie, come per esempio i sensori associati ai dispositivi IoT che nel manifatturiero lavorano automaticamente per rendere più efficiente i processi della *supply chain* (Klötzer & Pflaum, 2017).
- *Big data analytics capability:* l'acquisizione e l'analisi dei *big data* risulta cruciale e funzionale in quanto, oltre ad avere informazioni riguardo ai consumatori, le altre tecnologie digitali (AI, Iot) si basano sui dati raccolti.

CREAZIONE DEL VALORE – MODIFICHE NECESSARIE ALLA STRUTTURA ORGANIZZATIVA

Per quanto riguarda i cambiamenti questi fanno riferimento ai cambiamenti strutturali necessari per il processo di creazione del valore e che impattano su diversi aspetti dell'organizzazione. Un primo aspetto da considerare è quello relativo alla struttura organizzativa e consiste nel considerare l'agilità e l'ambidestrismo come requisiti necessari per poter competere in un mondo digitale. Un modo per poter raggiungere queste due capacità è quella, già definita, della creazione di unità separate con un livello di indipendenza dal resto dell'organizzazione (Sia, et al., 2016) tale per cui siano in grado di agire in maniera abbastanza flessibile a livello innovativo mantenendo, allo stesso tempo, l'accesso alle risorse già esistenti. Un altro modo è quello di creare dei team cross-funzionali di dipendenti e professionisti esterni che rimangono però sotto l'organizzazione aziendale (Svahn, et al., 2017).

Un secondo aspetto da considerare fa riferimento alla cultura aziendale e come essa possa variare nel tempo, adattandosi a cambiamenti necessari per rispondere alla DT. La domanda che maggiormente sorge nella letteratura riguarda " come una cultura digitale possa apparire" (Kane, et al., 2016) poiché, l'idea di base, è che le aziende, adattandosi ai cambiamenti, imparano attraverso piccole e incrementali interazioni. Tali interazioni, tuttavia, possono avere effetti negativi andando a modificare i piani sul lungo termine. Ciò è spesso dovuto al fatto che tali modifiche hanno cause esogene (Jöhnk, et al., 2017).

Importante è anche il fattore umano all'interno dell'azienda. La leadership deve assicurarsi che la propria azienda sviluppi un approccio e una mentalità digitale tale da poter rispondere alla DT e ai problemi associati all'uso di tecnologie digitali (Benlian & Haffke, 2016). A tal proposito ecco svilupparsi nuove figure dirigenziali. È il caso del CDO, il "*Chief Digital Officer*", figura che deve assicurarsi che le nuove tecnologie vengano introdotte senza alcun danno e che, una volta inserite, tali tecnologie siano allineate con gli obiettivi strategici dell'impresa (Sign & Hess, 2017). Il CDO agisce come mezzo per migliorare le strategie e attuarle in una serie di azioni concrete con il supporto del reparto IT. Tuttavia, il CDO è allo stesso visto come una figura temporanea, data la natura transitoria della DT (Matt, et al., 2015).

Inoltre, la letteratura evidenzia l'idea che la DT promuove situazioni in cui i dipendenti che non fanno parte della funzione IT assumono la guida di progetti ad alta intensità di tecnologia dove i membri dell'IT diventano partecipanti attivi nella realizzazione di tali progetti (Yeow, et al., 2017). Poiché le tecnologie digitali consentono nuove forme di automazione e processi

decisionali (Neumeier, et al., 2017) le domande sulla necessità di sviluppare le competenze dei lavoratori esistenti e anche le competenze richieste per i futuri lavoratori che formeranno la forza lavoro digitale stanno diventando sempre più rilevanti (Hess, et al., 2016) (Watson, 2017). Lungi dal rimuovere la necessità per le organizzazioni di dipendere dal capitale umano, la DT richiede ai dipendenti di sviluppare maggiormente le loro capacità analitiche per risolvere problemi aziendali sempre più complessi.

C*REAZIONE DEL VALORE – BARRIERE*

In linea con la letteratura, vi sono delle barriere al cambiamento del processo di creazione del valore. Queste possono essere sintetizzate in due concetti.

Il primo viene definito "inerzia" e viene rilevato laddove le risorse e le capacità esistenti fungono da barriere allo sviluppo. (Svahn, et al., 2017). Viene così evidenziato l'attaccamento delle organizzazione ai processi di produzione e, più in generale, al modo di fare business che risulta obsoleto poiché accentuato dalle relazioni esistenti con clienti e fornitori che si sono evoluti tecnologicamente. Famoso è il caso Kodak che pur avendo le capacità e le possibilità, non è riuscita a rispondere prontamente ai cambiamenti tecnologi in essere al tempo. Il rischio, come successo in questo caso, è che tutta la struttura organizzativa si irrigidisca a tal punto da impedire una trasformazione anche radicale offerta dalle tecnologie digitali. La cultura organizzativa, l'identità e la legittimità possono formare forti barriere istituzionali che ostacolano lo sviluppo di nuovi servizi e processi. Le componenti strutturali dell'organizzazione, sia tangibili (ad esempio, mezzi di produzione) che intangibili (ad esempio, cultura organizzativa), sono così incorporate nelle pratiche quotidiane da soffocare il potere innovativo e "*disruptive"* delle tecnologie digitali (Töytäri, et al., 2017).

Una seconda barriera è quella della "resistenza" dimostrata dagli impiegati quando una nuova tecnologia viene introdotta all'interno dell'organizzazione. In questo caso risulta fondamentale la figura del CDO che ha la possibilità di allineare l'uso della nuova tecnologia con la cultura aziendale (Sign & Hess, 2017). Tuttavia, Svahn, et al., (2017) mostrano come più semplicemente questa resistenza altro non sia che una mancanza nel vedere i benefici potenziali derivanti dalle nuove tecnologie digitali.

CREAZIONE DEL VALORE – STRATEGIE DI CRESCITA

La letteratura è concorde sul fatto che la maggior parte delle strategie di crescita in risposta alla DT riguardino l'adozione delle piattaforme digitali (Parker, et al., 2017). Dal 1999 al 2020, le ricerche effettuate su Google sono passate da 3,5 milioni a 2780 miliardi all'anno, un tasso di crescita del 50% circa annuo mentre il numero di utenti Facebook è aumentato da 100 milioni fino a 2740 milioni tra il 2008 e la fine del 2020, circa il 25% all'anno (Stats, 2020), Le piattaforme possono crescere velocemente e riescono a gestire un grande numero di utenti grazie ai bassi di costi per servire un cliente addizionale che, nel caso di imprese digitali, sono irrisori. Un secondo fattore di crescita delle piattaforme riguarda l'utilità massimizzata dell'utilizzo di queste quando una serie di figure (ad es. clienti) utilizza una piattaforma attraendo la propria controparte (ad es. fornitori), Così facendo, entrambi gli utenti danno vita ad una serie di virtuosismi che tendono a ripetersi e ad attrarre altri utenti. Infatti, secondo Zhu & Furr, (2016), il passaggio è quello tra una strategia incentrata sul prodotto a una basata sull'utilizzo della piattaforme e, di conseguenza, tra le relazioni con i partner come clienti e/o fornitori.

Per capire come le imprese digitali possano adottare delle strategie basate sulle piattaforme digitali vengono identificate alcune strategie: penetrazione del mercato, sviluppo del prodotto, sviluppo del mercato e diversificazione.

La penetrazione del mercato e lo sviluppo del mercato (basato sul prodotto) si basano sul concetto che le piattaforme possano far leva sulle tecnologie digitali per crescere ulteriormente attirando nuovi consumatori che non hanno mai provato il prodotto o ne utilizzavano un sostituto. È il caso di Netflix che ha attirato utenti non abituati a guardare la TV ma contenuti online in streaming utilizzando telefoni, tablet, laptop creando così un nuovo mercato, quello dello streaming. Anche l'introduzione dell'Apple Watch è stato un trampolino per il mercato degli *smartwatch* mentre "*Alexa"* e "*Google Home"* hanno dato il via al mercato degli assistenti vocali e degli smart speaker per la casa (Newman, 2020).

Data la grande sinergia che si crea tra i prodotti, le imprese digitali sono spesso interessate a sviluppare e lanciare nuovi prodotti in un ambiente composto da piattaforme. Infatti, le aziende possono perseguire una terza strategia, incentrata sulla penetrazione in nuovi mercati attraverso le piattaforme composte da diversi prodotti già esistenti e offerti da terze parti. È il caso di Apple che ha creato un ecosistema accessibile e compatibile per tutti i suoi prodotti (smartphones, tablet, PC, TV e dispositivi indossabili come Smartwatch e auricolari).

Anche la co-creazione delle piattaforme può essere una soluzione vantaggiosa. Così facendo, le aziende permettono agli utenti terzi di lavorare attivamente sulle piattaforme e creare valore insieme (Cui & Wu, 2016). È il caso di piattaforme digitali che permettono agli utenti di scrivere recensioni (Booking, Trip Advisor) o di condividere idee innovative su piattaforme di crowdsourcing (Dell IdeaStorm). Ci sono anche piattaforme che permettono lo scambio dei ruoli come Ebay o Airbnb dove l'utente, da acquirente, può diventare anche venditore. Questo scambio di ruoli negli utenti che diventano fornitori o venditori è riscontrabile nelle imprese che si sono già trasformate digitalmente piuttosto che in quelle che i ritrovano ad affrontare i primi cambiamenti in risposta alla DT.

In ultima analisi, alcune imprese possono intraprendere la strategia attraverso cui le piattaforme vengono diversificate. Questa strategia di crescita riguarda le aziende che hanno già sviluppato con successo delle piattaforme e intendono crescere maggiormente in nuovi mercati con nuovi prodotti. Per far questo, le aziende devono espandere le loro piattaforme per servire nuovi mercati, migliorare l'offerta dei prodotti e l'assortimento dei servizi oppure appoggiarsi a provider di servizi terzi (ad esempi Google, Android).

Qualunque strategia ha bisogno di essere controllata e misurata attraverso degli indicatori (KPIs). Nella DT è importante considerare anche le metriche digitali. Infatti, per molte aziende può essere utile monitorare i risultati intermedi tramite metriche relative al processo per valutare quanto bene il nuovo modello di business digitale sta creando valore (Libert, et al., 2016). Soprattutto nella fase di trasformazione digitale, le metriche "digitali" intermedie sono preziose, poiché forniscono informazioni più dettagliate. Per molte piattaforme digitali, ciò può includere l'ottenimento di misure del sentiment e del coinvolgimento online, nonché la creazione di reti e la condivisione del valore. Mentre molte aziende si concentrano sulla profittabilità, le imprese digitali si concentrano di più su valori di crescita. L'obiettivo principale di molte aziende digitali è raggiungere la crescita del numero di utenti dell'ecosistema digitale (ad es. Fornitori, clienti, terze parti) per creare effetti di rete di rinforzo che consentano un'ulteriore crescita della piattaforma. Una base di clienti in rapida crescita consente loro di accumulare dati preziosi su larga scala, che possono essere sfruttati sia internamente (all'interno dell'azienda) che esternamente.
Per gli operatori storici che si trasformano digitalmente, è importante anche raggiungere una crescita elevata, ma non a scapito della redditività. Pertanto, tali operatori affrontano un forte svantaggio quando competono con i concorrenti digitali. Gli operatori storici che vogliono trasformarsi digitalmente devono raggiungere contemporaneamente due obiettivi principali:

ridurre i costi attraverso l'automazione e aumentare i ricavi attraverso una migliore esperienza del cliente (Lemon & Verhoef, 2016). Data la possibile incompatibilità di realizzare entrambi gli obiettivi, alcuni ricercatori suggeriscono che gli operatori storici che si trasformano digitalmente dovrebbero sviluppare iniziative digitali in nuove iniziative separate che funzionerebbero in modo simile a una start-up digitale al fine di giustificare un focus primario sulla crescita.

1.3.7 – Valutazione degli impatti della digital transformation

La digital transformation impatta su diversi fronti, inclusi quelli della società in cui viviamo. Tuttavia, per prima cosa, verranno analizzati quelli sulle aziende a livello organizzativo poiché tali impatti inficiano sull'efficienza dell'operatività e sulle performance in generale dell'organizzazione.

Per quanto riguarda l'operatività, la DT ha notevoli impatti positivi, non solo in quanto le tecnologie digitali hanno il potenziale per trasformare un'organizzazione nella sua struttura, ma proprio perché a livello operativo, attraverso l'introduzione e adozione di tali tecnologie, viene migliorato il processo di creazione del valore con un notevole risparmio nei costi (Gust, et al., 2017). L'utilizzo del "*cloud computing"* fornisce risorse on-demand sempre reperibili e che non necessitano di essere lavorate, revisionate e mantenuto dal reparto IT. Anche l'utilizzo dei big data e degli analytics velocizzano, quando adottati, i processi decisionali dando risposte sempre più veloci e pertinenti mentre i prodotti e i servizi connessi con le AI e che utilizzano i *data* attivano automaticamente queste processo decisionale.

La DT viene spesso associata con l'incremento in diversi ambiti delle performance aziendali come l'innovazione, gli aspetti finanziari, la crescita aziendale, la reputazione e anche il vantaggio competitivo (Svahn, et al., 2017). A livello concettuale, la letteratura propone l'idea che le tecnologie digitali supportino le imprese nel percepire la complessità dell'ambiente in cui operano per poter, quindi, modellare le sue attività principali (*core activities)* in risposta ai continui cambiamenti (Tanriverdi & Lim, 2017).

Come detto, gli impatti della DT sulla società sono molteplici. La ricerca è concorde sul fatto che le tecnologie digitali offrano un potenziale enorme per migliorare la qualità della vita delle persone (Vial, 2019). Ne è un esempio il settore medico dove diverse tipologie di tecnologie

come l'automazione, i *big data* e gli *analytics* come anche le tecnologie VR e a realtà aumentata sono state recepite come un possibile contributo per il miglioramento delle cure, soprattutto in aree dove è presente una forte disparità sociale e una grande povertà (Kane, et al., 2016) (Srivastava & Shainesh, 2017).

Infine, la letteratura riferisce anche di potenziali problemi legati all'uso pervasivo delle tecnologie digitali, in primis riguardanti la sicurezza e la privacy (Newell & Marabelli, 2015). Questi effetti saranno analizzati nel capitolo successivo.

Capitolo 2 – BIG DATA

2.1 – INTRODUZIONE

Il termine "*big data"* fa riferimento a un grande set di dati inseriti in una grande, complessa e multiforme struttura. La struttura è complessa in quanto vi è una difficoltà intrinseca nell'archiviare, analizzare e visualizzare i dati per utilizzi o risultati futuri.

I dati vengono generati da qualunque movimento venga fatto online, che siano essi transazioni, e-mail, video, immagini, ogni interazione sui social media, accessi ai siti oppure anche i dati scientifici, medici, dati riguardanti l'utilizzo delle tecnologie, smartphones e app in primis. Qualunque flusso di clic è un dato. Anche il tempo di permanenza su un sito e la velocità con cui l'utente scorre una pagina web diventa un dato.

Questi dati vengono stipati in un database e crescono talmente tanto massivamente che risultano difficili da ordinare, gestire, condividere visualizzare e, soprattutto, analizzare, anche attraverso i software e gli strumenti di analisi.
Le tracce di dati lasciate vengono usate ampiamente dalle aziende con l'obiettivo di gestire al meglio il personale (efficienza nell'organizzazione) e il target di riferimento, nonché per offrire prodotti e servizi personalizzati ai clienti e ai consumatori. Tutto questo si basa sullo sviluppo di algoritmi che possono individuare le informazioni necessarie estrapolandole dai set di dati e analizzarle con successo.

2.1.1 – Natura dei data

Secondo Beyer & Laney, (2012), il concetto dei *big data* viene descritto secondo cinque V:

- Varietà *(high variety)* delle informazioni che richiedono costanti e innovativi metodi per analizzare i dati e ottimizzare il processo decisionale al fine di massimizzare i risultati. I *data* hanno molteplici origini e generalmente possono essere suddivisi in tre tipologie: strutturati, non strutturati, semi strutturati. I *data* strutturati sono dati già inseriti in un database, già catalogati e ordinati mentre quelli non strutturati sono difficili da analizzare in quanto randomici. I *data* semi strutturati non vengono ordinati

né catalogati ma possiedono elementi di distinzione dalle altre due tipologie (Singh & Singh, 2012).

- Volume (*high volume)*, quantità di dati che ne determina il valore (Madden, 2012). La quantità massima mai archiviata è dell'ordine di grandezza dello "ZETTABYTE" (10^{21} bytes). Per dare un'idea della quantità di dati archiviati, un Notebook medio ha la capacità di Rom (la "memoria" del computer) di 1 Terabyte, 1000 Gigabytes, ovvero 10^{12} bytes. Nel 2015 sono stati raggiunti 8 Zettabytes, viene stimato un raddoppio ogni due anni circa
- Velocità (*high velocity)*, non è connessa soltanto alla generazione dei dati ma anche alla velocità con cui vengono processati. I *data* dovrebbero essere presi inizialmente come una serie di flussi di informazioni differenti per poi essere categorizzati a seconda delle loro informazioni (Madden, 2012).
- Veridicità (*veracity)*, che rappresenta i requisiti di bontà, fiducia e incertezza relativi ai dati e al risultato dell'analisi dei dati (Zakir, et al., 2015).
- Valore (*value)*, acquisito solo se i dati vengono processati per ottenere informazioni, altrimenti è nullo. La grande quantità dei dati rende questo processo difficoltoso ma le tecnologie di analisi e di immagazzinaggio, necessarie al processo dei dati, continuano a migliorare . (Rajaraman, 2016)

Secondo Manovich, (2011), la grande quantità di dati presenti al giorno d'oggi ha delineato tre modelli tra le persone: persone che creano i dati, persone con le abilità per raccogliere i dati e persone esperte nell'analizzare i dati. Tutte queste caratteristiche, secondo Manovich, si ricongiungono nella figura del Data Scientist. Infatti, non solo le tecnologie sono importanti ma per padroneggiare i *big data* sono necessarie delle capacità ben precise nell'utilizzare queste tecnologie e dare un significato alle informazioni analizzate (Davenport & Patil, 2012)

2.1.2 – Analytics

I Big Data Analytics riflettono le sfide dei dati che risultano troppo vasti, troppo non strutturati e troppo veloci per essere gestiti con metodi tradizionali. Raccogliere informazioni significative è sinonimo di vantaggio competitivo poiché le enormi quantità di dati ricavabili

sono diventate sempre più importanti per le organizzazioni a livello globale. Cercare di estrarre in modo efficiente le informazioni significative da tali fonti di dati in modo rapido e semplice è impegnativo. Pertanto, l'analisi è diventata inestricabilmente vitale per realizzare il pieno valore dei Big Data per migliorare le loro prestazioni aziendali e aumentare la loro quota di mercato. Gli strumenti disponibili per gestire il volume, la velocità e la varietà dei big data sono migliorati notevolmente negli ultimi anni. Tuttavia, queste tecnologie richiedono un set di competenze che è nuovo per la maggior parte dei reparti IT, che devono lavorare sodo per integrare tutte le fonti di dati interne ed esterne rilevanti. Sebbene l'attenzione alla tecnologia non sia sufficiente, è sempre una componente necessaria di una strategia per i big data (Zakir, et al., 2015).

Il processo di analisi dei dati viene fatto formulando un'ipotesi spesso basata su congetture che derivano dall'esperienza o da risultati in provenienti dalla ricerca scientifica. Ci sono quattro tipi di *data analytics.*

L'analisi predittiva è l'uso di dati storici per prevedere il comportamento e le tendenze dei consumatori (Mosavi & Vaezipour, 2013). È l'uso di dati passati / storici per prevedere le tendenze future. Questa analisi fa uso di modelli statistici e algoritmi di apprendimento automatico per identificare modelli e apprendere dai dati storici (Shmueli & Koppius, 2011). L'analisi predittiva può anche essere definita come un processo che utilizza l'apprendimento automatico per analizzare i dati e fare previsioni (Puri, 2013).

L'analisi descrittiva essenzialmente spiega cosa è successo in eventi passati e presenti. Solitamente, i dati vengono organizzati in maniera semplice tramite grafici. scale, diagrammi per agevolarne la comprensione (Rajaraman, 2016). Un esempio è quello della rappresentazione dei censimenti che descrivono la popolazione campionata a tramite parametri come genere, età, educazione, reddito e altri.

L'analisi esplorativa, invece, trova delle relazioni all'interno dei dati raccolti. La maggiore applicazione di questa tipologia di analisi si ritrova, ad esempio, nella scoperta di andamenti nel comportamento dei consumatori. Le aziende, per esempio, basandosi su feedback, consigli, tweets, dati Facebook, dati di vendita etc., possono prevedere le loro azioni (Russom, 2011). I dati, infatti, vengono ricavati da molteplici fonti e questo permette una conoscenza generale e maggiori opportunità. C'è differenza rispetto all'analisi predittiva perché quest'ultima utilizza metodi statistici o i cosiddetti "*machine learning"* per la comprensione e la previsione nel

comportamento dei consumatori mentre l'analisi esplorativa trova le relazioni tra i parametri individuati

L'ultima tipologia è l'analisi prescrittiva che identifica le opportunità e le soluzioni migliori a problemi esistenti. Analizza i dati e dice cosa fare per raggiungere l'obiettivo (Kasturi, et al., 2016). Un uso comune, ad esempio, è quello delle compagnie aree che si basano su dati storici nei comportamenti dei passeggeri, analizzando le maggiori città di partenza e di arrivo, quando ci sono eventi o festività etc. per dare i prezzi ai posti a sedere e massimizzare i profitti.

2.1.3 – Algoritmo decisionale

data, una volta raccolti, categorizzati e infine analizzati sono fine a sé stessi se, successivamente, non vengono utilizzati per sviluppare strategie.

Al giorno d'oggi, è impensabile che ci siano una o più persone che, con i dati alla mano, sviluppino una strategia per ogni singolo consumatore. Infatti, sempre più spesso gli algoritmi vengono utilizzati per prendere decisioni in tutta la società. I sistemi sviluppati come gli algoritmi automatizzati o le AI, aiutano le persone a prendere decisioni al posto loro in diversi momenti.

Viene definito "*algorithmic decsion-making*" (algoritmo decisionale) o semplicemente "algoritmo", come "l'elaborazione dei dati di input per produrre un punteggio o una scelta che viene utilizzata per supportare decisioni come classificazione, associazione e filtraggio" (Diakopoulos, 2016). In alcuni contesti, sono stati utilizzati sistemi decisionali algoritmici per sostituire completamente le decisioni umane. Tuttavia, nella maggior parte degli scenari del mondo reale, c'è sempre un coinvolgimento umano nella decisione finale, influenzato dai suggerimenti e dalle sollecitazioni dell'algoritmo.

L'utilizzo degli algoritmi aiuta a prevedere cosa una persona farà e penserà o cosa a una persona piacerà, sulla base del suo attuale (o anche passato) comportamento. Mentre l'essere umano deve decidere cosa misurare e creare gli algoritmi che analizzano i dati raccolti, le decisioni prese non necessariamente implicano la comprensione dei comportamenti analizzati (Newell & Marabelli, 2015). Le decisioni sono sempre state prese dall'essere umano

basandosi sull'attività di analisi. Vi è sempre stata, pertanto, una sorta di discriminazione dovuta ad una comprensione (o incomprensione) della teoria o del contesto. L'uomo, infatti, analizza i dati, i comportamenti, basandosi solo su di essi e, in minima parte, sul contesto in cui tali comportamenti si sono verificati. Oggi, l'utilizzo degli algoritmi (che analizzano oggettivamente i dati raccolti) ha portato ad un aumento di una discriminazione, con soli pochi individui che riescono a capire cosa effettivamente sia stato incluso nell'algoritmo e perché.

In altre parole, è sufficiente che l'algoritmo abbia successo, non importa come. Il rischio che questo possa portare a problemi è alto quando nessuno all'interno di un'azienda sa come vengono prese determinati decisioni, ovvero quando nessuno sa come realmente lavori e funzioni l'algoritmo utilizzato. Secondo Clark & Newell, (2013), la crisi finanziari del 2008 negli U.S.A. è stata almeno parzialmente un prodotto di questo problema, con gli algoritmi facevano delle previsioni su determinati prodotti chiaramente non tenendo conto di tutti i rischi e allo stesso tempo non essendo soggetti a domande da parte né dei senior manager delle istituzioni finanziarie in cui venivano utilizzati gli algoritmi, né dalle agenzie di rating del credito che stavano valutando questi prodotti perché la base dell'algoritmo non era né chiara né facilmente accessibile.

2.2 – RACCOLTA DEI DATI

Le tecnologie digitali stanno diffondendosi sempre più frequentemente al punto da pervadere gli oggetti che usiamo tanto nella vita privata quanto in quella lavorativa. Questi oggetti sono quasi sempre connessi a Internet, un fenomeno denominato "ubiquitous computing" coniato per la prima volta dal Mark Weiser nel '88, che ha posto le basi delle tecnologie IoT. Ciò vuol dire che noi (e gli oggetti che usiamo quotidianamente) siamo sempre connessi in maniera esplicita oppure implicita. Una connessione esplicita avviene quando il fattore umano crea o usa esplicitamente dei contenuti online, ad esempio tramite l'utilizzo dei social media come Facebook e Twitter per mandare messaggi agli "amici" o al pubblico. Una connessione implicita, al contrario, basata utilizzando i dati (come tracce digitali) prodotti dall'uso degli oggetti digitali che usiamo costantemente. La differenza sostanziale risiede nel momento in cui si guarda ai contenuti creati dagli utenti oppure alle tracce che i frequenti utilizzi lasciano. Riprendendo come esempio Twitter, se le persone creano e leggono i commenti o i tweet,

questa è connessione esplicita poiché le azioni di lettura e creazione del contenuto sono l'oggetto dell'indagine. Al contrario, una connessione è implicita se i dati scaturiti dalla creazione dei contenuti vengono usati come modelli per prevedere qualcosa di diverso dai contenuti stessi.
Prendendo ad esempio l'utilizzo degli smartphone e della geolocalizzazione, è connessione implicita se si inviano offerte personalizzate basandosi sui suoi spostamenti e i suoi interessi ma è esplicita se l'utente invia la sua posizione agli amici per fargli vedere dove si trova.

È essenziale comprendere come questi dati vengono raccolti e le possibili implicazioni. Saranno escluse le modalità classiche di raccolta dati come i sondaggi, le interviste etc. in quanto non pertinenti. Infatti, la pratica di effettuare sondaggi sta pian piano scomparendo perché le persone decidono liberamente di non sottoporvisi (Michael & Miller, 2013). I progressi tecnologici nella raccolta e archiviazione dei dati ne hanno reso possibile l'acquisizione in grandi quantità generate direttamente (esplicitamente) o indirettamente (implicitamente) dagli utenti di Internet. Allo stesso modo, con la capacità di raccogliere dati attraverso l'IoT e da altri del mondo reale, la quantità di dati disponibili e raccolti è immensa.

2.2.1 – Web crawling

La rapida crescita di Internet ha posto le basi per i cosiddetti "*web crawlers"* ovvero dei "programmi che, dati i relativi codici URL, scaricano le pagine contenute in questi URL e ne estraggono ogni *hyperlink* (collegamento ipertestuale). Successivamente, continuano ricorsivamente ad analizzare gli elementi identificati dagli *hyperlinks* e così via", siano esse altre pagine o altri tipi di dati. Il Web Crawler è fondamentale per il recupero delle informazioni che attraversano il Web. Sono progettati, quindi, per recuperare i dati e le pagine Web e inserirli in un magazzino di dati locale.

Ci sono tre diverse tecniche di *crawling* (Abu Kausar, et al., 2013):

- Crawlig generico: un web crawler generico raccoglie il maggior numero di pagine possibile da un particolare insieme di URL e i relativi collegamenti. In questo modo, il crawler è in grado di recuperare un gran numero di pagine da posizioni diverse. La scansione generica può rallentare la velocità e la larghezza di banda della rete perché sta recuperando tutte le pagine.

- Crawling focalizzato: un crawler mirato è progettato per raccogliere documenti solo su un argomento specifico che può ridurre la quantità di traffico di rete e download. Lo scopo del crawler focalizzato è cercare in modo selettivo le pagine appropriate a un insieme predefinito di argomenti. Esegue la scansione solo delle aree rilevanti del Web e porta a risparmi significativi in termini di hardware e risorse di rete.
- Crawling distribuito: nel crawling distribuito vengono utilizzati più processi per eseguire la scansione e scaricare pagine dal Web.

Allo stato attuale i motori di ricerca non dipendono da un singolo ma da più web crawler che vengono eseguiti in parallelo per completare il target. Pur funzionando in parallelo, i crawler affrontano molte difficoltà come la sovrapposizione delle pagine, la qualità e i funzionamenti di rete.

2.2.2 – Web tracking

Il web tracking è la pratica attraverso cui ogni sito web identifica e raccoglie informazioni sui suoi utenti. Per tracciare queste informazioni, molti siti salvano dei piccoli pezzi di dati, incorporano degli oggetti invisibili o utilizzano gli account degli utenti e la loro configurazione hardware. I meccanismi più utilizzati sono i cookies, Browser fingerprints (impronta digitale dei browser), i web beacon:

- I cookie sono il metodo più conosciuto per identificare un utente. Utilizzano piccole porzioni di dati (ciascuna limitata a quattro KB) collocate in un archivio del browser dal server web. Quando un utente visita un sito web per la prima volta, un file cookie con un identificatore utente univoco (potrebbe essere generato in modo casuale) viene memorizzato sul computer dell'utente.
  Ad esempio, le successive visite ad una stessa pagina non richiedono l'accesso perché i dati dell'utente saranno ricordati dal browser tramite un cookie memorizzato al primo login.
- L'impronta digitale del browser è un modo estremamente accurato per identificare e monitorare gli utenti ogni volta che sono online. Le informazioni raccolte sono abbastanza complete e spesso includono il tipo e la versione del browser, il sistema

operativo e la versione, la risoluzione dello schermo, i caratteri supportati, i plug-in, il fuso orario, la lingua e le preferenze dei caratteri e persino le configurazioni hardware. Questi identificatori possono sembrare generici e per nulla come identificativi personali. Tuttavia, in genere solo due persona su diversi milioni di persone hanno esattamente le stesse specifiche.

- I web beacon sono oggetti molto piccoli, solitamente invisibili, incorporati in una pagina web o in un'e-mail. I web beacon sono anche chiamati "web bug", che vanno anche con i nomi "tag", "tag di pagina", "bug di tracciamento", "pixel tracker" o "pixel gif". Nella loro forma più semplice, sono immagini minuscole e chiare, spesso delle dimensioni di un singolo pixel. Vengono scaricati come immagine quando viene caricata la pagina Web o viene aperta l'e-mail, effettuando una chiamata a un server remoto per l'immagine. La chiamata al server avvisa l'azienda che la sua e-mail è stata appena aperta o la sua pagina web è stata visitata. I web beacon vengono utilizzati anche dagli inserzionisti online che li incorporano nei loro annunci in modo che possano monitorare in modo indipendente la frequenza con cui vengono visualizzati i loro annunci.

Il web tracking può essere di due tipi; *First-Party*, quando la raccolta dati viene effettuata dal sito web stesso, oppure *Third-Party* che si riferisce alla pratica con cui un'entità (il tracker), diversa dal sito web visitato direttamente dall'utente, tiene traccia o aiuta a monitorare la visita dell'utente al sito. Il *first-party web tracking* ("terze parti")non è particolarmente preoccupante perché le informazioni e le tracce lasciate vengono lasciate direttamente al sito stesso, Al contrario, un *third-party web tracking* può raccogliere informazioni e farne ciò che vuole. Oltretutto, quando su una pagina web sono presenti delle terze parti, queste hanno la possibilità di invitare altri *third-party* sul sito. Tale monitoraggio consente di raccogliere grandi quantità di dati personali degli utenti da una varietà di fonti provenienti dall'ambiente online e da diversi dispositivi come smartphone, tablet, laptop e PC. Ciò consente la compilazione di profili utente completi che restano nelle mani di poche società con ampie capacità di dati (Binns, et al., 2018). I dati raccolti possono includere località geografiche in cui l'utente è stato, articoli che l'utente ha acquistato o per cui ha mostrato interesse, comunicazioni personali che l'utente ha postato (inserito, sui social), foto o messaggi che ha pubblicato e siti web che l'utente ha visitato e con cui ha interagito. Contrariamente a quanto si crede, questi dati personali dell'utente non sono anonimi, le tracce lasciate sui siti sono facilmente riconducibili alla fonte In effetti, uno studio ha rilevato che nel 75% dei casi le

terze parti, a un certo punto, vengono a conoscenza dell'identità dell'utente (Krishnamurthy, et al., 2011)

Il tracciamento avviene sia sul web che nelle applicazioni (app) per dispositivi elettronici. Sul Web, il 95% dei 10.000 siti Web più popolari in tutto il mondo contiene almeno un tracker di terze parti. Oltre il 90 percento delle app gratuite trovate su Google Play Store contiene tracker di terze parti (Binns, et al., 2018). Questa capacità di monitoraggio è concentrata nelle mani di un piccolo gruppo di aziende: per i tracker basati su app, Alphabet / Google è il tracker più diffuso, seguito da Microsoft (incluso LinkedIn), Facebook e Twitter. L'immagine è solo leggermente diversa per i tracker basati sul web, dove Alphabet / Google è il tracker di maggior successo, seguito da Facebook e Twitter (Purra & Carlsson, 2016). Una manciata di aziende è quindi impegnata nella stragrande maggioranza del monitoraggio tramite *third-party* che avviene sul web o tramite app. Queste aziende fungono da grandi magazzini di dati e sono piattaforme che essenzialmente dominano l'ambiente del tracciamento tramite *third-party* in molti paesi sviluppati, sebbene esistano anche tracker locali più piccoli (Falahrastegar, et al., 2014).

La raccolta dei dati personali ha molteplici finalità nell'ambiente online. Il *third-party web tracking* è essenziale per fornire servizi apparentemente gratuitamente a un lato del mercato, mentre, dall'altro lato, monetizza questi dati gratuiti dell'utente. Ad esempio, le informazioni sugli utenti acquisite gratuitamente vengono vendute alle aziende interessate che li utilizzano per attività di marketing, promozione e personalizzazione delle esperienze online.

I servizi online sovvenzionati in questo modo includono giochi, streaming di musica e video, ricerca online e il social networking (Montes, et al., 2017). Questa pubblicità mirata, tuttavia, è possibile solo se la piattaforma che la vende ha accesso a una quantità considerevole di informazioni (cioè dati) sugli utenti da prendere di mira. Ulteriori usi a cui vengono destinati i dati personali includono la fornitura di servizi personalizzati, la discriminazione di prezzo e la vendita di set di dati a terzi. Inoltre, le aziende possono anche fare affidamento sui dati degli utenti per analizzare e migliorare i beni o servizi che vendono (Trabucchi, et al., 2017),

I vasti flussi di dati personali che vengono raccolti attraverso danno luogo a una serie di problemi legati alla concorrenza, al benessere dei consumatori, alla sicurezza e alla privacy. Il tracciamento consente la profilazione dell'utente e fornisce un campo di applicazione molto più ampio rispetto alla semplice pubblicità mirata come ad esempio l'analisi sulla salute delle persone, gli interessi personali e professionali, le opinioni politiche e la classe socio-

economica di una persona (Binns, et al., 2018). Consente inoltre il micro-targeting, il che significa la creazione di messaggi su misura per uno specifico individuo.

La crescente dipendenza dai dispositivi IoT (Internet of things) e dai dati dei sensori (come vedremo successivamente) da essi derivati, può consentire la raccolta di un volume di dati senza precedenti in tempo reale.

2.2.3 – Sensori

Oltre al passaggio dall'analogico al digitale, negli ultimi anni c'è stata un'altra importante rivoluzione tecnologica, quella dal cavo (sistemi cablati e centralizzati) a sistemi wireless (lett. "senza fili"), distribuiti in ogni dove e pervasivi. In particolare, l'evoluzione tecnologica ha reso possibile l'avvento dei sensori e delle reti wireless ad essi associati. I sensori sono piccoli apparecchi a bassa potenza e dai costi contenuti, multifunzionali e capaci di comunicare tra loro tramite tecnologia wireless a raggio limitato. trovano applicazione nel campo dell'Iot, ovvero la capacità di connettere ogni possibile dispositivo al web, generando una grande mole di informazioni.

Una rete di sensori wireless (d'ora in avanti WSN - *"Wireless Sensor Network"*) può essere definita approssimativamente come "l'insieme di sensori autonomi e indipendenti (chiamati "nodi") distribuiti nello spazio, in grado di rilevare grandezze fisiche (sensori di posizione, temperatura, umidità etc.) e di elaborare dati" (Akyildiz, et al., 2002).

Originariamente sviluppati per applicazioni militari, come la sorveglianza nei campi di battaglia e i sensori termici, le WSN sono ora ampiamente diffuse in molti scenari più civili, tra cui l'automazione domestica (domotica) e degli edifici, il monitoraggio della salute, il monitoraggio dell'ambiente e degli habitat, il controllo del traffico e molti altri. Anche un mondo come quello dell'automazione industriale, tradizionalmente più conservatore, è stato influenzato dalle WSN.

Ogni nodo in una rete di sensori wireless è solitamente dotato di un sensore (che traduce la quantità fisica di interesse in un segnale elettrico), di un piccolo microcontrollore (che fornisce la conversione da analogico a digitale e capacità di calcolo e archiviazione), di un dispositivo ricetrasmettitore radio (che fornisce capacità di comunicazione wireless) e di una

fonte di energia / elemento di immagazzinamento locale (solitamente sotto forma di una batteria elettrochimica). Può essere presente anche un "*Energy Harvesting"* ovvero un processo il cui scopo è convertire l'energia da una fonte esterna (es. Solare, termica, eolica e cinetica, reazioni chimiche) in energia elettrica che affianca / ricarica il tradizionale elemento di accumulo di energia .

Lo sviluppo di queste reti di sensori wireless richiede tecnologie provenienti da tre aree di ricerca molto diverse, ovvero tecnologie relative allo sviluppo del sensore, del dispositivo di comunicazione e del dispositivo informatico (non limitato all'hardware, ma anche software e algoritmi). I progressi combinati e separati in ciascuna di queste aree hanno guidato la ricerca in questo campo. A seconda dell'effettiva implementazione, la dimensione di un nodo sensore può variare da una scatola da scarpe a un granello di polvere. Allo stesso modo, il costo di un dispositivo sensore può variare da centinaia di euro a pochi centesimi, principalmente a seconda della complessità del sensore integrato e dei requisiti di calcolo / archiviazione. Viceversa, i vincoli di dimensione e costo sui nodi del sensore dettati dall'applicazione considerata e dalla sua funzionalità, si traducono in vincoli corrispondenti sulle risorse come l'energia, la potenza di calcolo e la larghezza di banda e la capacità di memorizzazione (Kay & Mattern, 2004). Formalmente parlando, un numero elevato di tali nodi di sensori wireless che possono interagire tra loro costituisce una rete di sensori, una WSN. In linea generale, in una rete possono essere adottati sensori che rilevano ciascuno grandezze diverse, come per esempio pressione o vibrazione, sensori ottici, termici, acustici, etc. in grado di monitorare simultaneamente le condizioni ambientali in luoghi differenti. Le informazioni estratte localmente possono quindi essere inoltrate a un altro nodo per un'ulteriore elaborazione. Per quello interessa la ricerca di questo elaborato, le capacità di rilevamento degli *smart device* continuano ad essere migliorate. Ad esempio, uno smartphone include sensori come accelerometri e GPS (Global Positioning System) e può comunicare queste informazioni per un'ulteriore aggregazione ed elaborazione dei dati. Grazie a questi dispositivi, un essere umano può comunicare le sue sensazioni, i suoi bisogni, i suoi desideri, fungendo anche da sensore (es. segnalando guasti nell'illuminazione stradale).

2.2.4 – Cloud computing

Il discorso sui sensori apre le porte per un approfondimento sul “cloud computing” e la loro relazione.
Il cloud computing viene definito come “un modello per consentire un accesso di rete conveniente e su richiesta a un network condiviso di risorse di elaborazione configurabili (ad esempio, reti, server, archiviazione, applicazioni e servizi) che possono essere rapidamente forniti e rilasciati con uno sforzo di gestione minimo o interazione con il fornitore di servizi" (Mell & Grance, 2011). Nel cloud computing non sono necessari dei server locali per raccogliere e organizzare le informazioni derivanti dai dispositivi smart o dai sensori circostanti ma vengono forniti molteplici server remoti che vengono revisionati costantemente. In poche parole, il cloud computing è la distribuzione di servizi di calcolo, come server, risorse di archiviazione, database, rete, software, analisi e intelligence, tramite Internet ("il cloud")

Il cloud computing può fornire diversi servizi che rientrano in tre categorie (Flammini & Sisinni, 2014):

- IaaS (Infrastructure as a Service): l’”infrastruttura distribuita come servizio” fa parte della categoria di base dei servizi di cloud computing. Con una soluzione IaaS, si ha la possibilità di affittare liberamente e in base alla necessità l'infrastruttura IT, ovvero server e macchine virtuali (VM), risorse di archiviazione, reti e sistemi operativi, da un provider di servizi cloud con pagamento in base al consumo delle sole risorse utilizzate. Un esempio può essere il servizio di Amazon, Amazon EC2 che permette agli utenti di affittare computer virtuali sui quali eseguire le loro applicazioni;
- PaaS (Platform as a Service): una “piattaforma distribuita come servizio” si riferisce a servizi di cloud computing che forniscono un ambiente su richiesta per lo sviluppo, il test, la distribuzione e la gestione di applicazioni software. Una soluzione PaaS è progettata per consentire agli sviluppatori di creare in modo più semplice e rapido app Web o per dispositivi mobili, senza doversi preoccupare della configurazione o della gestione dell'infrastruttura di server sottostante, della rete di archiviazione e dei database necessari per lo sviluppo. Sono un esempio di PaaS Google App Engine oppure Microsoft Azure;

- Saas (Software as a Service): un “software come un servizio” è un metodo per la distribuzione di applicazioni software tramite Internet, su richiesta e in genere in base a una sottoscrizione. Con una soluzione SaaS, i provider di servizi cloud ospitano e gestiscono l'applicazione software e l'infrastruttura sottostante e si occupano delle attività di manutenzione, come gli aggiornamenti software e l'applicazione di patch di protezione. Gli utenti si connettono all'applicazione tramite Internet, in genere con un Web browser nel telefono, tablet o PC. Ad esempio, possono essere citati il pacchetto Office 365 di Microsoft o le suite di Google o Adobe come fornitori tipici di Saas.

Vien fornita una quarta categoria, in sovrapposizione al modello PaaS, ovvero l’elaborazione serverless. Questa permette agli sviluppatori di creare più rapidamente applicazioni, eliminando la necessità di gestire l'infrastruttura. Le applicazioni serverless consentono ai provider di servizi cloud di effettuare il provisioning (preparazione della rete), ridimensionare e gestire automaticamente l'infrastruttura necessaria per l'esecuzione del codice. Per comprendere la definizione di elaborazione serverless, è importante notare che i server eseguono ancora il codice. Il nome serverless deriva dal fatto che le attività associate al provisioning e alla gestione dell'infrastruttura sono invisibili allo sviluppatore. Questo approccio permette agli sviluppatori di concentrarsi principalmente sulla logica di business e di offrire maggiore valore al core del business.

A seconda dell’architettura definita, esistono diversi modelli di cloud:

- Cloud Privato: si riferisce alle risorse di cloud computing usate esclusivamente da una singola azienda o organizzazione. Un cloud privato può trovarsi fisicamente nel centro dati locale della società. Un cloud privato è un cloud in cui servizi e infrastruttura sono gestiti in una rete privata. L’obiettivo dell’azienda che nell’utilizzare questa tipologia di cloud è quello di massimizzare l’efficienza delle risorse interne. I vantaggi, inoltre, ricadono nel ramo della sicurezza e nei minori costi di trasferimento dei *data*;
- Cloud Pubblico: I cloud pubblici sono di proprietà di un provider di servizi cloud di terze parti, che rende disponibili le risorse al pubblico.. I maggiori benefit ricadono nel contenimento dei costi perché l'hardware, il software e l'infrastruttura di supporto appartengono al provider di servizi cloud, che li gestisce. In aggiunta, viene migliorata anche l’efficienza e la scalabilità in quanto il pagamento avviene a seconda dell’uso. Per scalabilità si intende la capacità del server di incrementare le proprie prestazioni. Pertanto, il vantaggio, ricade sia sulle imprese ma anche sul provider dei servizi.

- Cloud Ibrido: combinando cloud privato e pubblico, un cloud ibrido permette di spostare dati e applicazioni tra cloud pubblici e privati. Offre all'azienda maggiore flessibilità e più opzioni di distribuzione e aiuta a ottimizzare l'infrastruttura esistente, la sicurezza e la conformità.
- Community Cloud: un community cloud è un'infrastruttura "multi-tenant" dove un software è fruito e condiviso da diverse organizzazioni di un gruppo specifico, con problemi di elaborazione comuni. Il principio organizzativo per il cloud della comunità sarà diverso, ma i membri della comunità generalmente condividono requisiti di sicurezza, privacy, prestazioni e conformità simili

WSN E CLOUD COMPUTING

Flammini & Sisinni, (2014) coniano i termini "*Sensor as a Service"* e *"Sensor Event as a Service"* per descrivere rispettivamente il processo di messa a disposizione dei dati derivanti dai sensori ai clienti attraverso il cloud, e gli eventi di interesse forniti dalle infrastrutture del cloud. Il WSN e il cloud computing, quando utilizzati contestualmente, danno la possibilità di condividere e analizzare i dati provenienti dai sensori in tempo reale (Dash, et al., 2010). Infatti, insieme, consentono di fornire i dati/eventi dei sensori come servizi su internet in modo che i questi possano essere facilmente analizzati anche da qualsiasi parte del mondo. L'unione di queste due tecnologie trova applicabilità in molteplici campi come quello militare, quello logistico, quello meteorologico o quello sanitario

I sensori trovano, pertanto, un notevole campo di applicazione soprattutto nell'IoT. I sistemi di pagamento tramite sensori NFC ("*near field communications")* o le esperienze di shopping tramite sensori RFDI (*"radio-frequency identification"*) associati alle AI, ad esempio, sono ormai all'ordine del giorno. Oltre che a velocizzare e migliorare le esperienze, queste due tecnologie permettono di raccogliere e analizzare dati riguardo ai consumatori (Tu & Piramuthu, 2020). L'utilizzo di tecnologie basate sui sensori hanno molteplici aspetti positivi sia per quanto riguarda l'individuo che per quanto riguarda le aziende. Ad esempio, un genitore può sentirsi al sicuro se i propri figli vengono monitorati e se nel caso in cui possa esserci un'emergenza possa venire prontamente avvertito. Oppure l'utilizzo ripetuto degli smartphones e del GPS permette ai provider dei servizi di navigazione di avere informazioni sul traffico in tempo reale così da offrire all'utente il percorso migliore.

2.3 – PROBLEMI SOCIALI LEGATI ALL'UTILIZZO DEI DATI

2.3.1 – Potenziale discriminazione associata all'uso dell'algoritmo decisionale

La letteratura è concorde sul fatto che vi è sempre stata una discriminazione in termini offerta di prodotti e servizi. Il motivo è semplice, prodotti e servizi hanno target e acquirenti diversi. Attraverso l'utilizzo dell'algoritmo, questa discriminazione è resa più marcata. Infatti, oggi l'offerta e la comunicazione sono ancor più mirate e personalizzate per i consumatori e potenziali nuovi acquirenti. Ad esempio, nel mercato delle polizze assicurative, l'utilizzo di dati derivanti dai sistemi di sorveglianza nelle auto come ad esempio la velocità media, l'usura dei freni, delle luci etc. permette alle compagnie assicurative, una volta raccolti i dati, di offrire prodotti basandosi sul comportamento alla guida del cliente stesso (Fang, et al., 2016). Tuttavia, tali decisioni prese secondo l'algoritmo sono spesso oggetto di questioni riguardanti i principi di equità e uguaglianza. Ad esempio, in Europa, dal dicembre 2012, sempre nel mercato delle assicurazioni è stato considerato discriminatorio offrire prodotti e servizi assicurativi differenti a seconda del genere solo perché le donne avevano un tasso di vita media superiore rispetto agli uomini. Infatti, le aziende diversificavano l'offerta basandosi su evidenze statistiche per stabilire i premi assicurativi e non su dati realmente raccolti. L'utilizzo dei *big data* e dell'algoritmo al fine di osservare le tendenze sui comportamenti e quindi discriminare i diversi gruppi che risultano dalle analisi può avere delle conseguenze sociali differenti. Tuttavia, i dati e l'algoritmo vengono utilizzati per prevedere il comportamento di ogni singolo individuo, non per prevedere le tendenze nei vari gruppi. Questo viene descritto attraverso il termine *"little data"* riferendosi ai dati ricavati assieme ai *big data* ma che vengono utilizzati in maniera più specifica. Infatti, i *little data* si focalizzano su ogni minimo particolare quotidiano di ogni specifico individuo e derivano dall'utilizzo di ogni strumento personale (Smartphone, PC, auto). Tuttavia, come verrà affrontato i seguito, ci sono dei risvolti sociali derivanti dalle modalità attraverso cui questi dati vengono raccolti, in primis in termini di sicurezza e privacy.

Secondo Newell & Marabelli, (2015), in termini di *big* e *little data*, l'utilizzo dell'algoritmo decisionale pone due importanti questioni. La prima è che i dati permettono alle aziende di sviluppare e utilizzare l'algoritmo che, a detta di Brynjolfsson, & McAfee, (2014) è superiore rispetto al giudizio umano, pervaso di pregiudizi intrinseci. Tuttavia, l'utilizzo dei dati può

portare a una discriminazione ingiusta. La seconda questione riguarda il monitoraggio del comportamento delle persone attraverso le tecnologie digitali e, soprattutto, come questo spesso avvenga nell'inconsapevolezza delle persone

Dopo aver esposto i risvolti etici nell'utilizzo dei big data verrà analizzata la seconda questione dove vengono esposti alcuni tradeoff che riguardano alcuni problemi legati all'uso da parte delle aziende nell'uso dei dati raccolti attraverso i dispositivi tecnologici.

I *big data* sono un arma a doppio taglio. Possono essere comodi e utili per l'individuo in quanto tendono ad agevolarlo nella vita quotidiana ma può portare, altresì, ad alcuni rischi. C'è una lunga storia di discussioni sull'etica e la tecnologia dell'informazione, che risale ai primi giorni della moderna tecnologia informatica. Le questioni etiche sono spesso complesse con conseguenze non intenzionali (Stahl & Wright, 2018). Ad esempio, gli algoritmi predittivi usati dalla polizia si concentrano sui "zone calde". Identificano dove si sono verificati i crimini e in che momento, in modo che le forze di polizia possano schierare agenti in quelle aree in quei momenti nel tentativo di prevenire i crimini prima che si verifichino. L'uso di tali algoritmi solleva diversi problemi etici. Uno è che rinforzano una spirale esistente, ovvero la polizia arresta più persone da quelle zone perché più polizia è stata dispiegata in quelle aree piuttosto che in altre aree. Una preoccupazione più ampia è che tali approcci alle attività di polizia possono modificare l'uso complessivo delle risorse delle forze dell'ordine in modi che potrebbero essere indesiderabili o subottimali. Molti esperti hanno notato che gli algoritmi riflettono i pregiudizi e le mentalità dei loro creatori, anche se tali pregiudizi e mentalità non erano intenzionali. Facebook ha condotto un noto esperimento manipolando i feed di notizie dei suoi utenti alimentando alcune notizie prevalentemente negative e altre prevalentemente positive, per vedere come ha influenzato il contenuto che gli utenti hanno poi condiviso in risposta. È stato giustamente criticato per non aver informato in anticipo i suoi utenti (Flick, 2016).

Una revisione completa dell'etica nell'ICT ha rilevato numerosi problemi discussi in letteratura (Stahl, et al., 2016). In questa revisione gran parte dei documenti affrontano la questione della privacy e della protezione dei dati, il che renderebbe questo l'argomento più importante. Anche Someh, et al., (2016) concordano come la privacy sia il concetto più importante dal punto di vista dell'individuo quando si parla di big data e aspetti etici. Tuttavia, vengono spesso discusse anche numerose altre questioni, come l'indipendenza degli utenti, il loro agire, fiducia, consenso, identità, inclusione e divisioni digitali, sicurezza, uso improprio e

inganno, per citarne solo alcuni.
I risvolti etici relativi ai big data impattano sia sull'individuo ma al contempo anche sulle aziende e sulla società.

2.3.2 – Risvolti etici dei big data per l'individuo

PRIVACY e SICUREZZA

Per definizione, la privacy è "la vita personale, privata, dell'individuo o della famiglia, in quanto costituisce un diritto e va perciò rispettata e tutelata" (Treccani, s.d.) ma in questa sede intendiamo privacy come "la misura in cui un individuo può limitare e controllare il modo in cui le organizzazioni utilizzano e divulgano le proprie informazioni personali" (Bélanger & Crossler, 2011). Alla base delle questioni etiche associate alla privacy ci sono tre aspetti in questo contesto e riguardano il modo in cui le aziende possono raccogliere, modificare e analizzare i dati personali. Secondo Barocas & Nissembaum, (2014), gli individui devono essere in grado di controllare quali dati vengono raccolti dalle aziende e chi vi avrà accesso anche quando sono loro stessi a dare il consenso per la raccolta e l'uso. Di nuovo, argomentano che anche se i database in cui vengono immagazzinati i dati potrebbero essere anonimi, il processo di aggregazione potrebbe rendere i dati disponibili ad altre parti all'insaputa dell'individuo. In secondo luogo Gli individui devono poter validare l'utilizzo dei propri dati alle aziende, verificano come e per quali scopi le altre parti vi accedono o possono sfruttarli (Tene & Polonetsky, 2013). Infine, gli utenti devono poter modificare i dati su sé stessi, aggiornando o eliminando i dati qualora volessero rimediare a informazioni errate, incomplete o non aggiornate (Halavais, 2015).
L'analisi dei dati potrebbe portare le aziende a creare e condividere nuove e maggiori informazioni sugli utenti. Tuttavia, la nuova conoscenza potrebbe rivelare informazioni sensibili sugli utenti, creare disagio e avere conseguenze non intenzionali come la discriminazione (Barocas & Nissembaum, 2014)

FIDUCIA

La fiducia riguarda il rapporto che gli individui hanno con le organizzazioni. Queste, secondo loro, dovranno comportarsi in modo prevedibile senza atteggiamenti opportunistici. Dovranno, pertanto, adempire ai loro obblighi nell'utilizzo dei dati degli utenti. Un frequente problema di fiducia riscontrato nella letteratura riguarda il monitoraggio non autorizzato. Le persone devono essere sicure di non venire osservate e registrate nella loro quotidianità. Se questo non dovesse accadere, potrebbero ritenere che un'organizzazione li stia sfruttando con il fine ultimo di estrarre dei dati causando così la perdita di fiducia nelle organizzazioni stesse (Richard & King, 2014). Gli individui devono avere la certezza che i dati vengano raccolti solo dietro un consenso informato e che verranno utilizzati solo per scopi chiaramente specificati (Barocas & Nissembaum, 2014). In secondo luogo, la sicurezza dei propri dati deve essere garantita dalle organizzazioni con le quali gli individui interagiscono, soprattutto a seconda del grado di condivisione dei dati e dell'archiviazione nel cloud dove i dati vengono inseriti (Goes, 2014). Infine, il problema della ricezione di pubblicità, offerte promozionali o e-mail non richieste (che spesso appunto finiscono in spam), spesso deriva dalla vendita e distribuzione dei dati aggregati da parte delle aziende che li hanno raccolti (Zuboff, 2015). Gli individui devono essere certi che le aziende non trarranno vantaggio in alcun modo dall'analisi dei *data* per profilarli scorrettamente o utilizzarsi i modi che possano danneggiarli (Martin, 2015)

CONSAPEVOLEZZA

Per consapevolezza si intende la conoscenza da parte delle persone riguardo le pratiche di analisi dei big data e relativa comprensione, come per esempio le modalità di analisi dati delle imprese per l'offerta di prodotti e servizi personalizzati. I risvolti etici nascono nel momento in cui le persone non conoscono i motivi per cui tali imprese utilizzino i dati (Newell & Marabelli, 2015). Secondo Crawford & Schultz, (2014), le persone devono possedere delle conoscenze anche basilari dell'argomento, come funzionano i big data e come quest possano influenzarli su scelte e comportamenti. Gli aspetti di consapevolezza, infatti, riguardano la comprensione di cosa siano i big data, la conoscenza e comprensione dei diritti (protezione dati in primis) e, infine, conoscere chi detiene i dati e con quale scopo. In questo modo riescono a capire i vantaggi derivanti dall'analisi dei big data (Newell & Marabelli, 2015). Oltre ai propri diritti, le persone dovrebbero essere a conoscenza anche delle politiche e delle leggi

esistenti in tema di protezione dei dati (es, GDPR – Regolamento generale europeo sulla protezione dei dati), nonché dei regolamenti e delle potenziali conseguenze negative dell'analisi dei big data. Questo permetterbbe agli individui di interagire con le istitutizioni che stabiliscono le normative vigenti. Infine, come già detto, le organizzazioni raccolgono dati anche in modo implicito senza informare chiaramente l'utente e nascondendogli l'uso secondario di tale raccolta (Barocas & Nissembaum, 2014). Le persone, quindi, devono essere consapevoli di quali dati vengono raccolti, chi li possiede e controlla e quali terze parti ne hanno accesso (Markus, 2015). Infatti, sovente le persone non leggono neanche i termini e le condizioni perché lunghi e di difficile compresione, accettandoli ad occhi chiusi

SCELTA

I risvolti etici nell'aspetto della scelta da parte del consumatore vanno di pari passo con la questione della discriminazione. L'analisi dei dati può limitare le scelte delle persone manipolandone ingiustamente il comportamento (Metcalf & Crawford, 2016) (Zuboff, 2015). Infatti, l'analisi tende a discriminare le persone perché basata, ad esempio, sul comportamento passato, sesso, età, posizione etc. Le imprese profilano e classificano gli individui in base ai loro dati personali e offrono servizi e prodotti personalizzati (Ananny, 2016). Non sempre, poi, i dati raccolti sono anche veritieri. Se la qualità dei dati raccolti è bassa o gli algoritmi utilizzati sono inappropriati, i profili che vengono creati non corrispondono alla realtà e non rappresentare correttamente gli individui (Clarke, 2016). Inoltre, sulla base di questi dati errati, gli individui continuano a essere discriminati ingiustamente.
Infine, le organizzazioni possono analizzare e manipolare il comportamento degli individui per personalizzare, ad esempio, determinati premi assicurativi che non vengono concessi a meno che tale comportamento non venga attuato (Zuboff, 2015)

2.3.3 – Risvolti etici dei big data per le organizzazioni

DATA TRADING

Per *data trading* si intende la "pratica con cui le aziende raccolgono, acquistano, aggregano, condividono i dati da molteplici fonti attraverso metodi che rispettano i diritti degli individui". Le organizzazioni possono acquisire dati interagendo direttamente con gli individui tramite l'utilizzo delle risorse digitali oppure, indirettamente, attraverso l'acquisizione e l'aggregazione dei dati da più fonti (Martin, 2015). Dopodiché possono condividere i dati raccolti oppure venderli ad altre aziende per ricavarne qualcosa (Wixom & Ross, 2017). Appunto per questo, i dati sono diventati una risorsa di valore e negoziabile nel mercato dei big data. Tuttavia, le pratiche attraverso cui le organizzazioni possono avere dei risvolti etici non indifferenti. Secondo Abbasi, et al., (2016), la raccolta dei dati spesso avviene in assenza del consenso esplicito informato degli individui e anche nella loro più totale inconsapevolezza. Esemplare il caso Snowden nel 2013, dove è stato scoperto che la NSA (National Security Agency – agenzia di sicurezza nazionale negli U.S.A.) sorvegliava e raccoglieva dati all'insaputa dei cittadini. Anche Google è finita sotto accusa nel 2010 per aver raccolto dati illegalmente dalle connessioni wi-fi non protette. Le organizzazioni fanno sì che i propri prodotti e servizi abbiano all'interno delle funzionalità che tengano traccia del comportamento degli utenti (Davenport & Kudyba, 2016). I prodotti sono quelli di uso quotidiano, dalle auto agli smartphones, e raccolgono una grande quantità di dati sulla vita delle persone senza però che queste siano informate esplicitamente riguardo ai dati raccolti e con quali scopi. Un altro fatto ricorrente riguarda i termini e le condizioni che sono spesso vaghi, scritti in maniera non comprensibile ai più e non specificano specificatamente la destinazione dei dati una volta raccolti (Abbasi, et al., 2016). Le persone, la maggior parte delle volte, vengono infomate sul fatto che i dati potranno essere condivisi con terze parti ma senza sapere quali dati, quali siano le terze parti e come questi verranno utilizzati. Infatti, spesso le aziende non sono propriamente trasparenti a riguardo (Martin, 2015). Un ulteriore problema riguarda la protezione dell'identità dell'individuo. Infatti, una volta che i dati vengono raccolti e aggregati, la loro condivisione può portare a una nuova identificazione delle persone che avevano l'anonimato nel punto inziale di raccolta (Barocas & Nissembaum, 2014). Infine, l'organizzazione che per prima ha raccolto i dati può avere un controllo limitandone l'accesso, la qualità e la condivisione con il rischio di diffondere dati inesatti (Martin, 2015).

GOVERNANCE ETICA

In questo contesto, la governance etica viene definita come " la misura in cui le organizzazioni hanno valori, norme e convinzioni condivise (governance informale) insieme a standard, diritti decisionali e responsabilità (governance formale) che promuovono pratiche etiche di analisi dei big data". La governance formale riguarda le politiche, gli standard a cui attenersi e le responsabilità formali a cui le aziende devono attenersi. La governance informale, invece, fa riferimento alla cultura dell'organizzazione e viene determinata da ciò che gli attori interni alle aziende credono e fanno sulla base di norme, valori e convinzioni condivisi (Wixom & Markus, 2017). A questo riguardo, i possibili risvolti etici si riferiscono alle norme e alle regole che vengono definite, nonché alle procedure di vendita dei dati raccolti. Secondo Wixom & Markus, (2017), le organizzazioni possono anche accettare determinate pratiche non etiche e venire legittimate nella loro cultura. Per prevenire questo problema devono intervenire i governi sanzioando tali pratiche adottate o istruendo e formando le organizzazioni riguardo le pratiche sui dati. L'istruzione, infatti, è indirizzata agli attori interni affinché condividino insieme un sistema di valori, convinzioni, norme e regole corretto. Sono le organizzazioni stesse che devono poi stabilire una base di regole e procedure che i dipendenti che possano seguire. Le regole, infine, possono rendere trasparenti i flussi i dati per i clienti e le altre organizzazioni (Metcalf & Crawford, 2016) perché nel momento in cui un'organizzazione condivide i dati, un uso non consono da parte di un'altra organizzazione puà avere effetti negativi su tutte le altre nella catena (Martin, 2015). Le regole, talvolta, possono anche riguardare le politiche per il trattamento e la sicurezza dei dati laddove, a livello legislativo, ci siano regolamenti in conflitto, ad esempio perché in paesi differenti.
Günther, et al., (2017) sostengono che le organizzazioni dovrebbero anche bilanciare i costi/benefici tra individui e organizzazioni nell'analisi dei big data a livello etico. L'analisi genera notevoli vantaggi finanziari e di mercato per le organizzazioni. Ciò potrebbe portare le aziende a monitorare e manipolare gli individui nelle loro scelte e nei loro comportamenti, anche se, attualmente, le aziende si concentrano sulla creazione di valore per sé stesse (Martin, 2015)

REPUTAZIONE

La reputazione intesa come "la misura in cui gli stakeholders, in particolare i clienti, credono che un'organizzazione gestirà e utilizzerà i dati su di loro in modo etico" può essere associata

alla definizione di rischio di reputazione promossa da (Scott & Walsham, 2005), ovvero "il potenziale che azioni o eventi associano negativamente un'organizzazione a conseguenze che influenzano aspetti del valore degli esseri umani". In questo caso, la reputazione di un'azienda viene a crearsi sulla base delle percezioni degli stakeholder riguardo l'integrazione di concetti etici nelle pratiche di analisi dei big data. Come già detto nel paragrafo precedente, sviluppare una cultura etica e formare poi i dipendenti non è immediato. Infatti, le organizzazioni che vantano una scarsa, se non pessima, reputazione riguardo l'analisi dei big data possono trovarsi in difficoltà a sviluppare internamente una cultura etica. Oppure, d'altra parte, le aziende che invece vantano una buona reputazione in tal senso possono incorrere nel rischi per cui dipendenti disonesti si servano di tale reputazione per sfruttare la fiducia delle persone, viste anche le innovazioni tecnologiche nell'analisi dati e sempre maggiori nuove fonti per raccoglierli. Anche il fattore competitivo può essere controproducente al fine di instaurare una cultura etica. Per avere maggior successo, un'azienda potrebbe seguire pratiche non etiche nella raccolta e nell'analisi dei dati con il fine di monetizzare e superare i concorrenti. Una valida alternativa risiede appunto nel perseguire queste pratiche etiche nel momento in cui la maggior parte dei concorrenti ha una cattiva reputazione (Martin, 2015)

QUALITÀ DEI DATA

La qualità dei dati viene definita come "la misura in cui le organizzazioni garantiscono la qualità dei big data in maniera tale che rispettino i diritti degli individui". Pertanto, in questo contesto, non si guarda alla bontà dei dati fine a sé stessa ma alla loro qualità per un uso corretto nelle decisioni che vengono prese utilizzando i risultanti derivanti dall'analisi (Clarke, 2016). I dati strutturati hanno caratteristiche di accuratezza, tempestività e completezza (le caratteristiche dei dati sono state definite precedentemente). Tuttavia, spesso, le organizzazioni forniscono diversi formati di big data, solitamente in forma non strutturata, in quanto comprendono dati sociali complessi. E non ci sono linee guida per gestire adeguatamente i big data non strutturati (Clarke, 2016). In aggiunta, il significato dei dati potrebbe cambiare nel tempo attraverso i molteplici processi di condivisione e aggregazione. Questo porta a una qualità dei dati diversa da quelli raccolti inizialmente, con il rischio di un utilizzo non etico da parte delle organizzazioni (Martin, 2015). Inoltre, il problema delle aggregazioni e condivisioni successive al momento di raccolta iniziale può portare alla creazione di dati che non sono una rappresentazione reale degli individui a cui

fanno riferimento (Crawford & Schultz, 2014), nonché al problema già riferito della scomparsa dell'anonimato.

ALGORITMO DECISIONALE

Dell'algoritmo decisionale è stato ampiamente già discusso. In questo contesto verrà definito come la "misura in cui l'analisi dei big data e le conseguenti decisioni organizzative rispettano i diritti degli individui." Le decisioni prese solitamente si basano su modelli statistici e modelli computazionali complessi. Le dimensioni, la velocità e la complessità dei dati aumentano. Contestualmente gli algoritmi diventano più importante per dare significato ai dati e fare previsioni (ad esempio sul comportamento dei consumatori) (Newell & Marabelli, 2015). Per l'appunto, le aziende ,utilizzando gli algoritmi, fanno previsioni che si basano su dati storici e soggettivi e, nella maggior parte dei casi, sulla loro correlazione, senza stabilire un effetto causale (Ananny, 2016). Il problema è riscontrabile nel fatto che le aziende non hanno mezzi per garantire la correttezza delle decisioni prese anche dal punto di vista etico. Per esempio, la profilazione, sempre tenendo conto della qualità dei dati, secondo Günther, et al., (2017) può portare a profilazioni razziali o altre tipologie di discriminazioni sociali (non relative all'offerta di prodotti e servizi) perché non c'è alcuna teoria che spiega le relazioni tra i dati raccolti. L'analisi dei big data, infatti, si basa principalmente sull'induzione di intuizioni che tendono a spiegare i comportamenti analizzati. Un altro problema risiede, per esempio, nel momento in cui l'algoritmo prende una decisione ma basandosi su dati di scarsa qualità. Gli individui che poi sono chiamati a prendere decisioni su quanto stabilito dall'algoritmo rischiano di prendere decisioni non etiche o discriminatorie. Vale anche nel caso di algoritmi complessi o inadeguati, per i quali i risultati finali non sono chiari (Ekbia, et al., 2015). Infine, le decisioni prese dall'algoritmo non comprendono il coinvolgimento umano e il problema è che il decisore umano che subentra nel processo successivamente all'algoritmo non ha i mezzi per capire in base a quali criteri la decisione è stata presa. La conseguenza è che il decisore si ritrova limitato nell'interpretazione dei dati, visto che i risultati non mostrano eventuali presupposti, limitazioni, pregiudizi o problemi di qualità dei dati stessi (Ekbia, et al., 2015)

2.3.4 – Risvolti etici dei big data per la società

Anche la società non è esente dagli impatti sociali dei big data. Di seguito vengono analizzati gli argomenti relativi all'etica dei big data dal punto di vista della società

DISEQUILIBRIO DI POTERE

Si intende disequilibrio di potere la "misura in cui un gruppo, un'organizzazione o un governo dominante utilizza l'analisi dei big data in un modo da sbilanciare il potere nella società". Riguarda il potere, il controllo e le relazioni che derivano dall'utilizzo delle analisi dei big data nelle società. Lo squilibrio si verifica perché solo pochi enti hanno accesso ai big data e secondo (Crawford, et al., 2014) questo influisce sull'uguaglianza degli individui e i loro diritti alla libertà di scelta. Lo squilibrio è appunto tra le organizzazioni, le agenzie governative e i paesi che, avendo accesso illimitato alle analisi dei dati, monitorano, quantificano e aggregano i dati raccolti sugli individui e creano così creati profili precisi e dettagliati (Zuboff, 2015). Questo genera un'asimmetria di conoscenza un piccolo numero di organizzazioni con un numero relativamente piccolo di dipendenti che utilizzano i servizi di analisi acquisiscono il controllo sul resto della popolazione. Il rischio è quello che tale potere acquisito possa essere utilizzato per influenzare gli individui e il loro comportamento per creare valore economico o, in questo caso, anche politico (Solove, 2017). Spesso la popolazione rimane ignara di ciò che accade con i propri dati, ritrovandosi senza una scelta o potere di negoziare

PRINICIPI E LINEE GUIDA

I principi e le linee guida esistenti che gli organismi di regolamentazione applicano attraverso regolamenti, leggi e politiche esistono per proteggere le persone interessante dalle conseguenze generate dall'analisi dei big data. Tuttavia, tali principi e linee guida sono sempre un passo indietro rispetto agli sviluppi tecnologici in questo campo (Metcalf & Crawford, 2016). Data questa situazione, le organizzazioni che utilizzano l'analisi possono essere in grado di farlo in modo totalmente legale o comunque non regolamentato ma potenzialmente non etico. Per evitare questo gli organismi addetti come i governi, le università, le organizzazioni senza scopo di lucro o aziende apposite potrebbero sorvegliare come l'analisi dei big data viene utilizzata e supportare le organizzazioni a sviluppare principi e linee guida o migliorare quelli esistenti in modo da condurre analisi corrette dal punto di vista etico (Markus & Topi, 2015). Oltre agli organismi, secondo Metcalf & Crawford, (2016), sarebbe

opportuno che intervenissero anche le autorità di regolamentazione per supervisionare, verificare e controllare le pratiche di analisi delle organizzazioni e imporre condizioni e limiti per garantire un livello standard di qualità e risultati positivi. Successivamente, una distribuzione migliore dei vantaggi dell'analisi dei big data può consentire alle persone nella società di esercitare al meglio i propri diritti sulla privacy, nonché di avere maggiore conoscenza verso tale fenomeno e maggiore fiducia verso gli enti che se ne occupano. Una migliore distribuzione dei vantaggi può essere fatta attraverso l'applicazione delle leggi, dei regolamenti e delle linee guida interessate (Markus & Topi, 2015).

SORVEGLIANZA

Per sorveglianza si intende la "misura in cui le organizzazioni osservano, monitorano, misurano e profilano le vite degli individui in una società". Questo argomento è spesso associato alla privacy e alla sicurezza. Come detto. i dati vengono raccolti dalla quotidianità delle persone (*little data* in primis) attraverso i dispositivi digitali personali, oggetti che sfruttano l'IoT, social media, Internet, sensori, cloud etc. Le organizzazioni monitorano, sorvegliano, i comportamenti degli individui e questo influisce sulla loro privacy e libertà di scelta (Crawford, et al., 2014). Il rischio è che le organizzazioni che monitorano gli individui e potenzialmente possono sapere tutto di loro, riescano a influenzarne e regolarne il comportamento (Zuboff, 2015). Queste organizzazioni analizzano il comportamento passato degli individui e prevedono o regolano quali potrebbero o dovrebbero essere le loro azioni future; quindi, manipolano il comportamento degli individui a proprio vantaggio (Lyon, 2014). Famoso è il caso Snowden e il Datagate, con la divulgazione di documenti sulla sorveglianza di massa del 2013 e volta a rivelare dettagli sulle operazioni messe in atto dalla Agenzia per la Sicurezza Nazionale statunitense (NSA) insieme ai servizi di intelligence di altri paesi nei confronti di cittadini e istituzioni (statunitensi e non)

COERCIZIONE

La coercizione si riferisce alla "misura in cui la partecipazione e il funzionamento degli individui nella società dipendono dal contributo dei propri dati ai servizi di raccolta per l'analisi dei dati". Nasce dal fatto che le organizzazioni incoraggiano le persone a utilizzare app, social network e dispositivi vari con all'interno dei sensori per partecipare ad attività

sociali e politiche (Newell & Marabelli, 2014). L'unica condizione che gli individui hanno per la partecipazione è il contributo con i propri dati. Questo però porta a una riduzione, talvolta assenza, nella libertà di scelta e alternative. Infatti, se scelgono di non fornire i propri dati rischiano di venire sanzionati o esclusi da molte altre attività personali, sociali, politiche (Zuboff, 2015). In aggiunta, spesso gli individui dipendono da tali servizi fornendo i propri dati e senza alcuna conoscenza dello scopo reale della raccolta (che raccoglie i dati per un motivo ma poi li vende a terzi senza informare gli utenti) (Galliers, et al., 2017). Un esempio di partecipazione sociale è quella relativa al sistema di tracciamento digitale dei contatti durante la pandemia del Covid-19. In molti paesi, soprattutto quelli dove il virus si è diffuso ampiamente e anticipatamente rispetto ad altri, sono stati attivati diversi sistemi di *contact tracing*, più o meno invasivi, che si differenziano per i livelli di immistione sulla privacy dei cittadini. DI fatto, questi sistemi tengono traccia degli spostamenti degli individui attraverso GPS o Bluetooth degli smartphone e possono essere più o meno pervasivi (Petracca, et al., 2020). In Cina, ad esempio, il sistema chiamato Health Code, viene integrato alle applicazioni di pagamento (Alipay) e di messaggistica istantanea (WeChat), ovvero le app maggiormente utilizzate nel paese, e tiene conto degli spostamenti, della stazionarietà nei luoghi e al possibile rischio di contatto con potenziali portatori di virus degli individui. In Corea del Sud l'approccio è più invasivo nei confronti della privacy dei cittadini. L'app, chiamata Corona 100m, traccia gli spostamenti in maniera tale da poter capire dove si sono mosse le persone contagiate, con chi sono entrate in contatto, che attività svolgevano. Un'altra, Corona100, incrocia i dati di geolocalizzazione dell'utente con quelli forniti dal governo e con quelli delle videocamere di sicurezza dando vita di fatto ad un sistema di sorveglianza anche se a fini sanitari. Meno invasivo è, per esempio, l'app Immuni in Italia che adotta il tracciamento del contatto tramite Bluetooth e app entrambi attivati (Santoro, 2020). Questi sistemi, di fatto, permettono la partecipazione attiva degli individui alla società, con il solo contributo di alcuni (non sempre) dati personali.

ATTRIBUTI DEGLI STAKEHOLDER NELL'ANALISI DEI BIG DATA

Gli stakeholder possono essere analizzati secondo tre attributi (Someh, et al., 2019):

- Potere di influenzare l'analisi dei *data*, fa riferimento alla misura in cui uno stakeholder può imporre la propria volontà in una relazione

- Legittimità della loro relazione, con riferimento alla misura in cui le azioni di una parte interessata sono auspicabili, adeguate e appropriate in un sistema sociale;
- Urgenza, nella misura in cui le rivendicazioni delle parti interessate richiedono un'azione immediata.

In questo contesto, le organizzazioni hanno un alto grado di potere e di urgenza poiché possiedono la tecnologia, i dati, e l'expertise necessario allo svolgimento delle pratiche di analisi e perché riescono a portarle a compimento in tempi relativamente brevi. Tuttavia, hanno un basso grado di legittimità in quanto le loro azioni sono spesso all'opposto dei valori della società o degli individui (Currie & Seddon, 2017). Un alto grado di potere e di urgenza possono essere percepiti come pericolosi quando le loro azioni hanno un basso grado di legittimità.

Gli individui, invece, hanno un basso grado di potere e di urgenza perché hanno un basso potere negoziale nei confronti delle organizzazioni di cui spesso neanche sanno chiaramente le modalità di raccolta dati e perché la loro partecipazione nel processo di raccolta avviene quasi sempre in maniera passiva, e questo richiede minor immediatezza nell'intraprendere azioni. Al contrario, hanno un alto grado di legittimità in quanto le loro azioni sono per lo più adeguate e appropriate all'interno della società. Infatti, azioni inadeguate possono portare a sanzioni e conseguenze legali.

La società ha diversi gradi di potere, un basso grado di urgenza e un alto grado di legittimità. I diversi gradi dipendono dal fatto che è la società ad imporsi sulle questioni riguardanti l'analisi dei *data* attraverso le leggi, i regolamenti, le linee guida e le eventuali sanzioni che impongono ma, al contempo, l'emanazione di tali materiali non avviene contestualmente alle innovazioni tecnologiche adottate per l'analisi. Da qui deriva il basso grado di urgenza. Lo sviluppo di leggi etc. richiede più tempo e non sempre la società riesce a stare dietro allo sviluppo tecnologico. L'alto grado di legittimità, infine, è alto in quanto le azioni intraprese sono appropriate e adeguate per i loro cittadini (Someh, et al., 2019)

2.4 – INTERAZIONI TRA GLI STAKEHOLDER

Someh, et al., (2019) sostengono che le organizzazioni hanno un'elevata rilevanza e gli individui e la società hanno una bassa rilevanza, Per rilevanza intendiamo il peso,

l'importanza, che tali soggetti hanno nelle dinamiche relazionali l'une con le altre. Tale differenza implica che, attualmente, le organizzazioni che utilizzano l'analisi dei big data dominano le interazioni con gli individui e la società. Spesso, infati, le organizzazioni prendono i dati degli individui come una risorsa gratuita o a basso costo e li usano a proprio vantaggio (Zuboff, 2015). Al momento, le società dispongono pochi regolamenti, leggi e linee guide per guidare il modo in cui le organizzazioni utilizzano l'analisi dei big data, sebbene questa continui evolversi in maniera rapida (Metcalf & Crawford, 2016). Una sfida per le organizzazioni è quella di affrontare questa problematica in modo efficiente ed efficace affinché venga garantita l'accettazione di tali pratiche dagli individui, pena uno scontento generale che porti all'imposizione di regolamenti più rigorosi e sanzioni più pesanti da parte della società.

2.4.1 – Relazione tra gli individui e le organizzazioni

Gli individui sono sia la fonte originaria dei dati sia il fine ultimo delle analisi e delle decisioni prese dalle organizzazioni. Per questo motivo sono la parte chiave del mondo dei big data anche se spesso sono ignari di quali dati vengono raccolti e con quali scopi (Richard & King, 2014)

In molti casi, i dati vengono raccolti solo tramite consenso implicito e le organizzazioni non fanno altro che combinarli da più fonti, analizzarli e utilizzarli anche vendendoli ad altri (Martin, 2015). Non è detto, infatti, che gli individui sappiano realmente chi alla fine detenga i loro dati e con quale scopo. Oltreutto, non hanno sempre la possibilità di controllare chi ne ha accesso (Someh, et al., 2019). Anche se gli individui apprendessero le pratiche di analisi dei big data raramente riuscirebbero a limitare le informazioni che le aziende creano su di loro (Clarke, 2016). Pertanto, anche volendo, non sono in grado di modificare, correggere o eliminare i dati in possesso delle aziende. Questa mancanza di controllo può portare a probelmi relativi alla fiducia verso le organizzazioni in quanto gli individui si sentono costantemente monitorati e influenzati e la paura che le informazioni possano finire nelle mani sbagliate (Someh, et al., 2019)

Il fine dell'analisi è quello di creare nuove conoscenze sugli individui. Il problema è che, aggregando queste informazioni, si creino delle informazioni sull'individuo di cui lui stesso

non è a conoscenza, minando il loro diritto alla privacy. Ad esempio, l'analisi del comportamento sui social network può fornire dei risultati totalmente ignoti all'utente, con il rischio che questo si senta manipolato (Halavais, 2015) (Someh, et al., 2019). Inoltre, gli individui possono avere la sensazione di essere vincolati in seguito a una profilazione effettuata dall'algoritmo e di sentirsi discriminati socialmente o sfruttati economicamente sulla base di scelte prese involontariamente e inconsapevolmente (o quasi) dall'organizzazione, ad esempio, avere costi differenti per un'assicurazione auto a seconda dell'etnia, del sesso, del reddito etc. (Ananny, 2016)

Per aumentare la loro rilevanza nelle interazioni con le organizzazioni, gli individui devono aumentare il loro grado di potere e di urgenza. Possono farlo acquisendo maggiori conoscenze sull'analisi dei big data e comprendere le pratiche e le conseguenze dell'analisi per interagire con le organizzazioni. Oltretutto, possono garantire che le organizzazioni stabiliscano pratiche di governance etica e che devono assicurarsi di avere un maggiore accesso e controllo sui propri dati personali. Garantire la qualità dei dati personali può portare a delle pratiche di scambio dati trasparenti (Someh, et al., 2019). Inoltre, le organizzazioni dovrebbero sviluppare pratiche decisionali che rispettino la libertà di scelta degli individui per migliorare ulteriormente la fiducia e reputazione. Così facendo, viene a crearsi una governance etica solida per il futuro

2.4.2 – Relazione tra le organizzazioni e la società

L'analisi dei big data ha dei risvolti importanti per la società viste le dinamiche relazionali che si instaurano e che ricadono sulle relazioni di potere. Causa diretta delle relazioni di potere, in questo caso uno squilibrio di potere a favore delle organizzazioni, è la diseguaglianza che intercorre tra i due soggetti che crea asimmetrie di conoscenza e porta a una mancanza di fiducia degli individui nella società stessa (Zuboff, 2015)

È stato ampiamente discusso di come le società siano indietro con l'attuazione di leggi per regolare l'analisi dei big data rispetto alle innovazioni tecnologiche della stessa. Non a caso le organizzazioni, grazie a questo ritardo, cercano di allargare sempre più i propri domini, cercando di ottenere un vantaggio competitivo il prima possibile (Metcalf & Crawford, 2016). Oltre a promulgare leggi e linee guida, la società deve anche cercare di applicare le relative

sanzioni per punire e scoraggiare comportamenti scorretti dalle aziende che non dispongono delle governance etiche e accusano gli affronti della competizione (Someh, et al., 2019)

Pertanto, al fine di aumentare la loro rilevanza nelle interazioni con le organizzazioni, le società devono aumentare il loro potere e urgenza (Someh, et al., 2019). Per farlo una società dovrebbe attuare due soluzioni. La prima. già ampiamente discussa, è quella di emanare leggi e regolamenti e applicare le sanzioni a chi li trasgredisce. La seconda, invece, è quella di accompagnare e supportare le organizzazioni nella creazione di governance etiche, seguendole fornendo loro il materiale necessario. Le istituzioni devono interagire con le organizzazioni per garantire che gli squilibri di potere non si radichino e che le pressioni concorrenziali sulle organizzazioni non incentivano pratiche non etiche (Martin, 2015). Aumentare l'importanza delle società nelle loro interazioni con le organizzazioni può portare a vantaggi reciproci e, consentendo il discorso etico, far emergere pratiche di analisi dei big data che bilanciano gli interessi dei diversi stakeholder in modo più etico (Markus & Topi, 2015).

2.4.3 – Relazione tra gli individui e la società

Someh, et al., (2019) ritengono che l'analisi dei big data viene effettuata "prevalentemente per esigenze commerciali" e che i vantaggi che derivano vengono sfruttati per un chiaro "bilanciamento degli interessi" laddove può sorgere un significiativo squilibrio di potere. Per evitare tale squilibrio le persone dovrebbero comprendere meglio le pratiche di analisi e le conseguenze, nonché anche confrontarsi attivamente con la società nello sviluppo di principi e linee guida appropriati. Tali principi devono stabilire la possibilità di evitare conseguenze non etiche nell'analisi dei big data, come ad esempio la discriminazione involontaria (Clarke, 2016)

Le società, secondo Someh, et al., (2019), dovrebbero creare "consapevolezza di ciò che potrebbe accadere quando i big data vengono analizzati" e "proteggere i cittadini dall'abuso dell'analisi dei big data". Gli individui sono diventati più dipendenti dall'utilizzo dei dispositivi digitali con conseguenze importanti sulle loro abitudini e comportamenti. Inoltre, partecipare attivamente in una società vuol dire dipendere sempre più dall'utilizzo di app, social network,

dispositivi IoT, con la conseguenza che fornire i propri dati non rappresenterà quasi più una scelta (Newell & Marabelli, 2015).

In sostanza, sia gli individui che le società dovrebbero aumentare la loro rilevanza nelle interazioni con le organizzazioni. Da un lato, deve esservi una partecipazione attiva da parte degli individui nello sviluppo di linee guida e principi, specialmente nel momento in cui le società sono chiamate a stabilire delle sanzioni efficaci e ad imporle. Tali sanzioni aiuteranno a proteggere i diritti degli individui sulla privacy dei dati e la libertà di scelta (Crawford & Schultz, 2014). Dall'altro lato, le società devono trovare modi per condividere i vantaggi dell'analisi dei big data senza costringere gli individui a fornire dati per partecipare alla società, istruendoli poi per aiutarli a comprendere meglio i vantaggi e i costi dell'analisi dei big data (Zuboff, 2015).

Aumentare la rilevanza degli individui e delle società congiuntamente nelle loro interazioni con le organizzazioni può portare a vantaggi reciproci e, quindi, consentire un discorso etico e un forte impulso per le organizzazioni a sviluppare e adottare pratiche etiche di analisi dei big data.

2.5 – TRADEOFF

L'utilizzo delle tecnologie digitali può portare ad alcuni compromessi da parte degli individui per quanto riguarda alcuni problemi legati all'uso da parte delle aziende nell'uso dei dati raccolti attraverso il mondo online come app, smartphone, dispositivi IoT, e offline, come sensori etc.

PRIVACY VS SICUREZZA

I dispositivi digitali possono aumentare la sicurezza delle persone nella vita quotidiana. Uno smartphone può essere rintracciato grazie ai sensori GPS al suo interno che possono stabilirne la posizione; le auto di nuova generazione integrano sistemi di monitoraggio dell'ambiente circostante che si attivano, ad esempio, qualora un malintenzionato provasse a introdursi nell'abitacolo, oppure in caso di imminente incidente per registrare quanto accaduto. Questi esempi di soggetti che utilizzano le tecnologie digitali per migliorare la

sicurezza hanno, tuttavia, un certo costo in termini di privacy individuale. In alcuni casi, l'uso di app, social, applicazioni software possono anche interessare la privacy di terzi e non solo quella personale (Gerlach, et al., 2015). È chiaro, quindi, il risvolto sociale si crea nel momento in cui l'utilizzo e l'attivazione di tecnologie digitali di uso quotidiano per aumentare la sicurezza. Tuttavia, questo miglioramento nella sicurezza ha un costo in termini di riduzione della privacy.

Ad esempio, l'utilizzo dei Google Glass utilizzati dai ciclisti o *rider* per registrare i propri percorsi può essere un problema per quanto riguarda la privacy delle persone che vengono registrate. L'utilizzo di questo dispositivo viene percepito come negativo non tanto da chi lo indossa ma da chi potrebbe trovarsi a contatto (o semplicemente nei paraggi) di un utilizzatore. Questa possibilità va a minare la sensazione di sicurezza delle persone che si sentono, in conclusione, monitorate senza aver dato alcun consenso (Kudina & Verbeek, 2019). D'altra parte, il recente caso nelle modifiche dei termini e condizioni di "WhatsApp" (app di messaggistica) che prevedono la condivisione di dati con Facebook (che possiede WhatsApp), ha suscitato diverso scalpore. Questa condivisione, al di fuori dell'UE dove vige il GDPR ovvero il regolamento europeo per la protezione dei dati personali (una delle leggi sulla privacy più avanzate del mondo), ha causato uno spostamento di diversi utenti su app concorrenti (Konrad, 2021). WhatsApp condivide alcuni dati con Facebook già da diverso tempo anche in Europa ma non per scopi commerciali (differenza con i nuovi termini e condizioni nel resto del mondo) ma soltanto per scopi tecnici e di sicurezza. Questi dati comprendono informazioni dell'account come il numero di telefono, informazioni sul telefono cellulare e sull'indirizzo IP dell'utente, tra le altre cose. Per esempio, se si fa una videochiamata su WhatsApp alcuni dati vengono trasferiti a Facebook, perché l'infrastruttura tecnologica per fare le videochiamate è di Facebook. Questo è un comportamento consentito dal GDPR (Voigt & von dem Bussche, 2017). Per una maggiore sicurezza in termini di diffusione dei dati per

LIBERTÀ VS CONTROLLO

"La datificazione di ogni cosa rende possibile sia l'utilizzo dei dispositivi digitali per tener traccia di ogni decisione presa e di ogni posto visitato sia l'uso di questi dati per monitorare e controllare le abitudini e il comportamento degli utenti" (Newell & Marabelli, 2015). Esistono due tipi di controllo. Il primo si riferisce ad un "controllo informato", dove gli individui sono

consapevoli di essere costantemente monitorati e un "controllo non informato", dove gli individui vengono monitorati senza sapere di esserlo,

Libertà vs controllo informato

La questione di base è "se le persone hanno un determinato comportamento solo perché sono al corrente di essere controllato cambierebbero il loro agire se il controllo cessasse?". Il controllo informato è visibile in diversi campi, da quello lavorativo (dipendenti che usano un badge con sensori RFID e che vengono monitorati costantemente), a quello familiare (genitori che localizzano lo smartphone del figlio per sapere dove si trova). Questa tensione risiede tra un miglior controllo (da parte delle organizzazioni ma anche della società o degli individui) a scapito di individui che sentono di avere una certa libertà o autonomia (Newell & Marabelli, 2015). Ciò suggerisce che coloro che prendono decisioni su come utilizzare queste tecnologie (che siano aziende, enti pubblici o privati) potrebbero voler pensare di ridurre il grado sorveglianza sugli individui poiché questo sarebbe il prezzo che potrebbe voler pagare per permettere alle persone di sentirsi in controllo delle decisioni che prendono . Questo è, appunto, un compromesso tra controllo e libertà nel contesto della digitalizzazione della nostra vita quotidiana.

Libertà vs controllo non informato

Un problema maggiore risiede quando le persone non sanno di essere controllate. Nei social network, ad esempio, le persone vedono quello che l'algoritmo vuole farci vedere sulla base dei nostri interessi, dei nostri movimenti online e delle nostre ricerche (tramite cookies, per esempio). Queste strategie che vengono adottate dalle aziende per personalizzare i contenuti, i risultati nelle ricerche o, ad esempio, gli annunci pubblicitari, portano gli individui a essere sempre meno esposti alla diversità online. Un possibile effetto è quello per cui le persone possano diventare meno tolleranti alla diversità, essendo esposte sempre e solo a cose di loro interesse (Newell & Marabelli, 2015). L'uso strategico dei dati da parte delle organizzazioni per personalizzare il "nostro" Internet rischia di essere un altro modo per permettere la discriminazione

INDIPENDENZA VS DIPENDENZA

Questo compromesso riguarda la dipendenza dalle tecnologie digitali che migliorano, agevolano e semplificano le attività nella vita quotidiana. Nello specifico, il desiderio, l'esigenza di dipendere dagli strumenti IT e la capacità di vivere senza di loro. È il caso dei dispositivi GPS, dei sistemi di sicurezza sulle auto, ad esempio, Le persone saranno ancora in grado di orientarsi o di parcheggiare nonostante le auto integrano sempre di più ogni sensore necessario? I vantaggi, in questo caso, sono nettamente superiori. Nel caso delle automobili, la guida con pilota automatico è diventata una realtà consolidata ormai da diversi anni (Endsley, 2017). L'algoritmo decide per noi e decide anche meglio, rende sicura la guida perché è in grado ad esempio, di rallentare sulla base di informazioni sul traffico che ha reperito online al momento o sulla base delle previsioni meteo, senza che il conducente ne sappia qualcosa. Tuttavia, la conseguenza negativa di un eccessiva dipendenza dai dispositivi digitali è associata al rischio a cui le persone sono esposte nel momento in cui si dimenticano certe cose. Il progresso implica necessariamente l'automazione (e la perdita di alcune capacità manuali), e molte innovazioni sviluppate dalle aziende contribuiscono positivamente alla qualità di vita (e alla sicurezza). Tuttavia, sono i dispositivi digitali e il processo decisionale algoritmico associato a porre problemi, specialmente quando si supervisiona o si intraprendono attività umane che potrebbero comportare esiti pericolosi per la vita se la tecnologia smettesse di funzionare. Inoltre, a causa della connettività tra i sensori, esiste anche il possibile caos – scenario estremo ma potenziale – che si verificherebbe se tutto smettesse di funzionare per tutti contemporaneamente. Newell & Marabelli, (2015) sostengono che sia "la diffusione di tali automazioni IT tra i cittadini comuni che crea minacce se dovessimo diventare completamente dipendenti dalla tecnologia e incapaci di operare senza di essa". Tuttavia, l'adozione di alcune di queste automazioni è (o diventerà) praticamente obbligatoria per molti, creando discriminazioni nei confronti di coloro che non si conformano. Un semplice esempio riguarda i residenti negli Stati Uniti che, se desiderano utilizzare auto dotate di cambio manuale standard (invece di cambio automatico), dovranno pagare di più, solo perché "standard" non è uno standard negli Stati Uniti. D'altra parte, coloro che possono guidare solo auto automatiche dovranno pagare di più se vogliono noleggiare un'auto quando viaggiano all'estero, perché la maggior parte delle auto avrà un cambio manuale standard e l'auto automatica avrà un costo maggiore.

Capitolo 3 – RICERCA QUANTITATIVA

3.1 – INTRODUZIONE

Secondo la letteratura non si sa ancora molto, in termini di tradeoff tra privacy e sicurezza, fino a che punto gli utenti siano consapevoli di essere monitorati ogni qual volta navigano online o utilizzano le app o gli smartphone, attivano il GPS o utilizzano qualunque oggetto connesso a Internet. Infatti, sarebbe interessante sapere in che misura l'esigenza di utilizzare i servizi online prevale sulla sensazione potenzialmente scomoda di venire profilati (tramite i *little data*) (Newell & Marabelli, 2015).

L'avvento del digitale ha trasformato letteralmente le abitudini degli individui, specialmente riguardo la navigazione in rete. L'evoluzione delle tecnologie digitali, il miglioramento delle infrastrutture e i costi relativamente bassi hanno reso più facile e veloce l'accesso all'online. Più del 60% della popolazione mondiale è online con più del 90% la percentuale degli utenti che accede direttamente da telefono (Zanon, 2020). Online spendiamo circa il 40% del nostro tempo, per lavoro o svago. Aumenta esponenzialmente il numero degli utenti internet, degli utenti dei social networks, aumentano i siti e i sistemi tecnologici venduti e, parallelamente, cresce ad esempio anche il numero di siti i siti web hackerati, poco più di due al secondo (Stats, 2020). Qualunque movimento online viene tracciato, sempre più dati vengono raccolti più o meno consapevolmente e attraverso metodi più o meno legali.

Per quanto riguarda il concetto della privacy, già precedentemente discusso, alcuni ricercatori inquadrano la nozione di privacy come paradossale (Barth & de Jong, 2017) altri usano il concetto di "calcolo della privacy" (Chen, 2018). La ricerca più comune ruota attorno alla sicurezza e alla protezione della privacy (Acquisti, et al., 2015) (Kirwan, 2015). Altri si concentrano sulla tutela della privacy (Tissera, et al., 2017) e molti si concentrano su questioni legali riguardanti la privacy (Pope, 2012). Vi è anche una notevole quantità di ricerche che studiano le questioni relative alla protezione dei dati (Terry, 2017) e all'impatto che i social media e tutte le nuove tecnologie hanno sulla privacy (Cho, et al., 2018). Con tutta l'attenzione prestata alla privacy, è necessario, pertanto, esaminare le motivazioni che spingono le persone a gestire attivamente (concedere/negare l'accesso a terzi) le informazioni che considerano private nella vita di tutti i giorni.

Per comprendere la gestione attiva delle informazioni private, questa discussione si concentra sulla teoria della vulnerabilità dei dati e sulla gestione della privacy concettuale e operativa che è centrale per la "*Communication Privacy Management Theory*" (CPM) pubblicata sotto il titolo di "Boundaries of Privacy: Dialectics of Disclosure" come un libro nel 2002 da Petronio. L'ampiezza della ricerca che utilizza la teoria del CPM (Communication Privacy Management) dimostra la sua utilità per comprendere la privacy nella vita di tutti i giorni. La missione iniziale della teoria del CPM si è concentrata sulla determinazione di un modo praticabile per comprendere come concettualizzare e determinare modi utili per operare la natura della privacy e, in particolare, quella della gestione delle informazioni private.

La teoria del CPM riconosce che gli individui credono di possedere le proprie informazioni private e hanno il diritto di controllare tali informazioni (Schoeman & Ferdinand, 1984). La proprietà è rappresentata da metaforici "confini della privacy" che definiscono dove le persone ospitano e proteggono le loro informazioni (Brannon & Rauscher, 2018) (Petronio & Gaff, 2010). CPM utilizza l'identificatore di "proprietario delle informazioni" per rappresentare il legittimo controllo delle proprie informazioni private. Inoltre, comproprietari selezionati sono designati come "comproprietari autorizzati" a indicare la legittimità dell'accesso. Le persone credono di avere il controllo sui confini della loro privacy e credono di avere il diritto di concedere a chi può accedervi e quando le loro informazioni private sono off limits per gli altri (Hammonds & Joshua, 2015). Tuttavia, rivelare o divulgare informazioni private presenta rischi potenziali che possono portare a sentimenti di vulnerabilità per il proprietario (Bute, 2015). Tuttavia, anche avere un "senso" di controllo è importante perché può temperare i sentimenti di suscettibilità.

Invece, il costrutto della vulnerabilità dei dati pone l'attenzione sui comportamenti degli individui a causa di possibili danni dovuti alla dispersione delle loro informazioni personali. In generale, la vulnerabilità implica la sensibilità a lesioni o danni. Nel momento in cui un'azienda raccoglie le informazioni personali dei clienti aumenta il rischio potenziale di danni e, perciò, il loro sentimento di vulnerabilità (Scharf, 2007). La vulnerabilità dei dati è influenzata anche dalla teoria del Gossip che considera le trasmissioni non autorizzate di informazioni personali a terze parti (Richman & Leary, 2009). Questa teoria identifica anche due fattori chiave che influenzano gli effetti dannosi della vulnerabilità dei dati: trasparenza e controllo

3.2 – SVILUPPO DELLE IPOTESI

In questa sezione di sviluppo delle ipotesi verranno brevemente presentati i valori associati alla diffusione delle proprie informazioni personali online per meglio esprimere il modo in cui vengono stabilite le ipotesi.

3.2.1 – PARADOSSO DELLA PRIVACY

Prove empiriche a sostegno della letteratura indicano che gli individui sono disposti a scambiare le loro informazioni personali per ricompense relativamente piccole. Ad esempio, Carrascal, et al., (2013) hanno scoperto che gli utenti di Internet valutano la sicurezza della loro cronologia di navigazione online per poco, quasi il costo di un pasto al ristorante. D'altra parte, però, ulteriori studi riguardo l'atteggiamento degli utenti di Internet mostrano che gli utenti sono molto preoccupati per la loro privacy e per la raccolta e l'utilizzo delle proprie informazioni personali online (TRUSTe, 2014) (Madden, s.d.). Questa dicotomia tra attitudine/comportamento effettivo riguardo la privacy e le informazioni personali online è stata coniata come "paradosso della privacy" (Norberg, et al., 2007) o, per essere più precisi, "paradosso della privacy delle informazioni". Il paradosso della privacy ha implicazioni significative per l'e-commerce, l'e-government, il social networking online, nonché per la regolamentazione della privacy del governo. I siti di e-commerce e social network online raccolgono grandi quantità di informazioni personali.

La maggior parte delle persone non ha la capacità cognitiva di calcolare i rischi per la privacy e i vantaggi della divulgazione e non ha accesso a tutte le informazioni necessarie per formulare giudizi informati possibili trade-off riguardo la privacy. Gli individui prendono decisioni sulla privacy in un tempo limitato avendo informazioni incomplete su rischi e benefici. Inoltre, spesso non sono in grado di calcolare tutti i parametri rilevanti (Camerer, 1998). Pertanto, le loro decisioni in materia di privacy sono vincolate da informazioni incomplete e razionalità limitata (Acquisti & Grossklags, 2005), due condizioni che influenzano il processo decisionale in diversi contesti (ad esempio economia, amministrazione aziendale, ecc.). La razionalità limitata fa riferimento ai limiti cognitivi che

devono affrontare le persone, ovvero la conoscenza limitata dell'argomento e una possibile scarsità di capacità computazionale.

Le asimmetrie informative prevalgono nel rapporto tra consumatori e fornitori nel mercato Internet e mobile. Ad esempio, gli utenti di app per smartphone hanno una conoscenza molto scarsa di come vengono utilizzati i propri dati personali, non fanno affidamento sulle informazioni fornite dai gestori di tali applicazioni sulla raccolta e sull'utilizzo dei dati personali quando decidono quale applicazione scaricare. Considerano le informazioni (recensioni) dei loro simili e dell'app store più importanti e affidabili (Buck, et al., 2014)(Buck et al., 2014). Baek, et al., (2014) hanno mostrato che la dicotomia tra preoccupazioni per la privacy e l'intenzione comportamentale scompare quando agli individui vengono presentati argomenti a favore o contro l'uso delle informazioni personali da parte delle imprese online. I partecipanti allo studio di Baek sono stati divisi in tre gruppi. Al primo gruppo è stato presentato un breve messaggio che promuoveva la regolamentazione sulla raccolta e l'uso dei dati personali, al secondo gruppo è stato presentato un messaggio con argomenti a sostegno della raccolta e dell'uso dei dati personali e al terzo gruppo non è stato dato alcun messaggio. Quindi, a tutti i partecipanti è stato chiesto di completare un questionario di indagine che misurava i problemi di privacy e l'intenzione di divulgare informazioni personali. Le preoccupazioni e le intenzioni erano positivamente correlate nei primi due gruppi, mentre le preoccupazioni e le intenzioni non erano correlate nel terzo gruppo.

3.3 – MODELLO TEORICO

Il modello teorici di riferimento utilizzati per la ricerca sono quello del "*communication privacy management*" (CPM) e quello della vulnerabilità dei dati con lo scopo di indagare quali possano essere i fattori identificativi che influenzano le persone nel condividere le proprie informazioni online.

La ricerca è volta a indagare quale possa essere la relazione tra la vulnerabilità percepita derivante dalla condivisione delle informazioni personali online e l'atteggiamento nel rilasciarle.

Infine, in ultima analisi, capire come queste due variabili agiscano sulle intenzioni nel rilasciare tali informazioni online

CPM

Attraverso sei principi la CPM cerca di spiegare come gli individui gestiscono la loro privacy (Child, et al., 2009) (Tabella 2). La CPM può essere suddivisa in tre elementi: possesso della privacy (privacy ownership), controllo della privacy (privacy control) e agitazione della privacy (privacy turbulence)

Tabella 2- Assiomi CPM

Assioma n. 1	Le persone ritengono di avere il possesso delle loro informazioni;
Assioma n. 2	Poiché le persone ritengono di avere il possesso delle loro informazioni, credono anche di avere il diritto di controllare il flusso di tali informazioni, di come si muovano;
Assioma n. 3	Per controllare le proprie informazioni private, le persone sviluppano delle regole che successivamente utilizzano sulla base di criteri per loro importanti (motivazione, cultura, situazioni, differenze individuali, genere e rapporto rischi/benefici)
Assioma n. 4	Nel momento in cui gli individui forniscono l'accesso alle loro informazioni private tramite divulgazione o altri mezzi, allora tali informazioni sono di dominio pubblico
Assioma n. 5	Una volta che le informazioni diventano di dominio pubblico e vengono detenute collettivamente (comproprietà), le parti stabiliscono le norme sulla privacy per la diffusione a terzi, tra cui: a. Regole che determinano la quantità e la tipologia di informazioni private che possono essere condivise con altri (regola di permeabilità dei confini) b. Regole che guidano chi detiene queste informazioni nel determinare quanto controllo possono esercitare sulle informazioni private rese pubbliche (regole di proprietà dei confini) c. Regole che considerano chi altro, oltre a chi detiene già le informazioni personali private, può accedervi o conoscerle (regole di rapporti dei confini)

Assioma n. 6	Poiché le persone non negoziano in modo coerente, efficace o attivo le regole sulla privacy per le informazioni private di dominio pubblico, esiste la possibilità di violazioni, errori o interruzioni dei confini nel modo in cui i comproprietari controllano e regolano il flusso di informazioni verso terzi

PRIVACY OWNERSHIP

Le persone credono di essere gli unici proprietari delle loro informazioni private e confidano di avere il diritto di proteggere le loro informazioni o di concedere l'accesso (Brownlie, 2011) (Petronio & Gaff, 2010). Di conseguenza, la proprietà può essere limitata o condivisa con altri. Inoltre, quando i "proprietari originali" concedono ad altri l'accesso a informazioni private, questi diventano "comproprietari autorizzati" e sono percepiti dal "proprietario originale" come aventi responsabilità fiduciarie per le informazioni (Thompson, et al., 2012) (Tokic & Pecnik, 2011). La proprietà della privacy definisce i confini che circondano le informazioni, contrassegnandole come private. I confini della privacy aiutano a delineare il contesto così come le linee di demarcazione per le informazioni considerate private.

Poiché la comproprietà gioca un ruolo importante nel mantenere le informazioni private del "proprietario originale", viene prestata una crescente attenzione all'importanza della privacy del proprietario originale rispetto a quella del destinatario che presta servizio in un ruolo di comproprietà (Petronio & Reierson, 2009).

PRIVACY CONTROL

Il secondo elemento principale del CPM è il controllo della privacy, che simboleggia il motore che regola le condizioni di concessione e negazione dell'accesso alle informazioni private, ovvero in che misura le altre parti possono gestire le informazioni personali altrui. Poiché gli individui credono di possedere i diritti sulle loro informazioni private, ritengono anche, giustamente, che dovrebbero essere loro a controllare la loro privacy, anche dopo aver concesso l'accesso ad "altri soggetti autorizzati". Inoltre, il modo in cui le persone controllano il flusso delle proprie informazioni private avviene attraverso lo sviluppo e l'uso di regole sulla privacy che derivano da criteri decisionali come motivazioni, valori culturali e bisogni situazionali. Un nuovo schema sviluppato di recente sostiene che questi criteri possono essere classificati in due tipi: criteri fondamentali e criteri catalizzatori che guidano le scelte delle

regole sulla privacy Ci sono dei criteri di scelta delle regole sulla privacy che sono fondamentali e sono coerenti al modo in cui le persone tendono a gestire le proprie informazioni private. Tuttavia, ci sono catalizzatori che possono influenzare le modifiche a tali regole. Ad esempio, il cambio di stato (da celibe/nubile a sposata/o) delle coppie appena sposate spesso significa che le loro regole sulla privacy devono fondersi e cambiare per soddisfare le esigenze del partner e il loro nuovo stato di relazione. Di conseguenza, il matrimonio può essere un catalizzatore relazionale che richiede la modifica e la negoziazione delle norme sulla privacy.

Il fulcro centrale dell'analisi dei criteri catalizzatori fa riferimento al rapporto rischio-beneficio che si crea perché si innescano delle modifiche alle regole della privacy sulla base delle motivazioni (Child, et al., 2012) (Thompson, et al., 2012). Un evento catalizzatore, infatti, va ad impattare sui criteri fondamentali delle regole della privacy innescando dei possibili cambiamenti,

Tuttavia, "la comproprietà porta a confini di privacy collettivi detenuti e gestiti congiuntamente in cui i contributi di informazioni private possono essere forniti da tutti i membri", con il problema, a livello di affidabilità, di quando questi "proprietari originali" devono cedere le informazioni personali perché non più in grado di gestirle. È il caso, ad esempio, di quando i genitori non sono più in grado di gestire personalmente le proprie finanze. In questo caso, i figli adulti diventano "comproprietari autorizzati" e contribuiscono alla divulgazione di informazioni finanziarie private (trattando con gli istituti preposti), ma, a volte, ciò ha un costo per la loro relazione figlio adulto-genitore.

Infatti, il CPM, prevede che i confini della privacy vengono regolati attraverso decisioni su chi altro potrebbe essere a conoscenza, su quanto possono sapere gli altri all'interno e all'esterno del confine collettivo e sui diritti di divulgare le informazioni.

PRIVACY TURBULENCE

Il terzo elemento nel sistema di gestione della privacy del CPM è la turbolenza della privacy. La regolamentazione della privacy è imprevedibile, spesso a causa di situazioni che apportano delle modifiche ai criteri fondamentali. La ricerca ha illustrato la fattibilità di questo situazione in numerosi modi, ad esempio riguardo lo stigma dell'infertilità nelle coppie, se e come comunicarlo (Steuber & Solomon, 2012), riguardo la comunicazione di informazioni

mediche di parenti (Petronio & Lewis, 2010). Ad esempio, possono sorgere difficoltà di divulgazione, rendendo difficile sapere come affrontare in modo produttivo la gestione della privacy per raggiungere gli obiettivi necessari (Petronio & Gaff, 2010). C'è una serie di problemi che scoppiano creando scompiglio per il "proprietario originale" e per i "comproprietari autorizzati", ad esempio nel momento in cui viene comunicata una relazione sentimentale ai membri della propria famiglia con la richiesta che tale informazione non venga divulgata (Petronio & Reierson, 2009) .Nel complesso, lo stato di agitazione nella privacy è il segnale che debba avvenire necessariamente un cambiamento nel sistema di gestione della privacy per rendere adeguata la regolamentazione della privacy.

La CPM sostiene che ci possono essere delle violazioni ai propri dati che influiscono sulla gestione della privacy in diversi modi. Di conseguenza, queste situazioni creano ciò che CPM identifica come "turbolenza della privacy" (DeGroot & Vik, 2017). La violazione della privacy è problematica perché questa condizione può interrompere le regole sulla privacy, la proprietà, il controllo e i confini della privacy, nonché le relazioni esistenti sulla privacy (Wenzel Egan & Hesse, 2018) (Kennedy-Lightsey & Frisby, 2016). Sebbene la violazione della privacy abbia esiti negativi per il proprietario delle informazioni, alcune ricerche preliminari suggeriscono che a volte viene appresa una lezione e il proprietario ricalibra le regole sulla privacy per impedire di nuovo l'esperienza (Thorson, 2015)

VULNERABILITÀ DEI DATI

La teoria della vulnerabilità dei dati pone l'attenzione sui comportamenti degli individui a causa di possibili danni dovuti alla dispersione delle loro informazioni personali. Questa ricerca offre tre principali contributi teorici (Martin, et al., 2017).

In primo luogo, i clienti percepiscono un danno e rispondono negativamente alla raccolta e all'utilizzo dei dati da parte delle aziende. I test su tutti i tipi di vulnerabilità dei dati dei clienti mostrano effetti negativi significativi, alcuni dei quali si manifestano anche senza alcun danno finanziario diretto per il cliente. Questa visione incentrata sul cliente mostra che le persone identificano potenziali danni dovuti agli sforzi di gestione dei dati delle aziende. Di conseguenza, la vulnerabilità offre un costrutto più preciso per comprendere le risposte dei clienti all'uso delle loro informazioni da parte delle aziende rispetto a questioni generali di privacy o danni finanziari.

In secondo luogo, per descrivere come la sensazione di vulnerabilità dei clienti crea forti risposte negative da parte loro, viene utilizzata la teoria del Gossip. La teoria del Gossip ha un valore sia teorico che intuitivo per valutare come le persone rispondono all'accesso e all'utilizzo indesiderato delle informazioni dei clienti, quando ne vengono a conoscenza. A conferma di una premessa fondamentale della teoria del Gossip, troviamo che le persone sono suscettibili di come le proprie informazioni vengono percepite e valutate dagli altri (Richman & Leary, 2009), anche se gli altri sono aziende.

Terzo, ci sono due elementi periferici della teoria del Gossip che caratterizzano il modo in cui le persone gestiscono la diffusione delle proprie informazioni. Negli individui, la trasparenza e il controllo lavorano in sinergia per mitigare i sentimenti di violazione e migliorare la fiducia, il che è in linea con le promesse di trasparenza e controllo nelle pratiche di gestione dei dati delle aziende. Come le aziende gestiscono i propri dati e le loro pratiche è importante per ridurre la vulnerabilità percepita. Gli effetti forti, significativi e sinergici della trasparenza e del controllo permettono di diminuire la sensazioni di vulnerabilità degli individui. Allo stesso modo, questi effetti combinatori suggeriscono legami con la teoria della scelta informata, derivanti dall'enfasi della trasparenza sulla conoscenza e dall'enfasi del controllo sulla scelta (Cranage, 2004).

OTTIMISMO E TRATTI DELLA PERSONALITÀ

Si definisce ottimismo il "grado in cui una persona ha aspettative positive sul suo futuro”

L'ottimismo è una variabile di differenza individuale che va dal pessimista nella fascia bassa all’ottimista nella fascia alta, anche se molti studiosi sostengono che pessimismo e ottimismo sia relativamente indipendenti (Herzberg, et al., 2006) (Marshall, et al., 1992) (Zuckerman, 2003). Le definizioni scientifiche di ottimismo e pessimismo si concentrano sulle aspettative delle persone per ciò che riguarda il loro avvenire (Carver, et al., 2010). Gli ottimisti sono persone che si aspettano che accadano loro cose buone, positive; al contrario, i pessimisti sono persone che si aspettano che accadano loro cose brutte, negative. I modi in cui ottimisti e pessimisti differiscono nel loro approccio al mondo hanno un impatto sostanziale sulle loro vite. Differiscono, infatti, nel modo in cui affrontano i problemi e le avversità; differiscono anche nelle loro risorse, sia sociali che socioeconomiche.

Ci sono diversi studi che associano, come si vedrà più avanti, l'ottimismo ai cinque grandi tratti della personalità (Milligan, 2003) (Ebert, et al., 2002) (Lounsbury, et al., 2004). Il modello dei tratti della personalità è stato sviluppato a partire dagli anni '80 nell'ambito della psicologia comportamentale. In particolare, Lewis Goldberg ha fortemente sostenuto cinque fattori primari della personalità (Ackerman, 2021). Il suo lavoro è stato ampliato da McCrae & Costa, che hanno confermato la validità del modello e hanno fornito il modello utilizzato oggi: coscienziosità (conscientiousness), piacevolezza (agreeableness), nevrosi (neuroticism), apertura all'esperienza (openness to experience) ed estroversione (extraversion). Il modello è diventato noto come "Big Five" e ha ricevuto molta attenzione. È stata studiata in molte popolazioni e culture e continua ad essere la teoria della personalità più ampiamente accettata oggi. Ciascuno dei tratti della personalità dei Big Five rappresenta categorie estremamente ampie che coprono molti termini relativi alla personalità. Di seguito:

1. *Coscienziosità*

La coscienziosità è un tratto che può essere descritto come la tendenza a controllare gli impulsi e ad agire in modi socialmente accettabili, comportamenti che facilitano il comportamento diretto a uno scopo (John & Srivastava, 1999). Le persone coscienziose eccellono nella loro capacità di ritardare la gratificazione, lavorare secondo le regole e pianificare e organizzare in modo efficace.

I tratti all'interno del fattore di coscienza includono: persistenza, ambizione, completezza, autodisciplina, consistenza, prevedibilità, controllo, affidabilità, intraprendenza, lavoro duro, energia, perseveranza, pianificazione.

È probabile che le persone con un alto livello di coscienza abbiano successo a scuola e nella loro carriera, eccellere in posizioni di leadership e perseguire ostinatamente i propri obiettivi con determinazione e previdenza (Lebowitz, 2016). Le persone con poca coscienza hanno molte più probabilità di procrastinare e di essere volubili, impetuosi e impulsivi.

2. *Piacevolezza*

Questo fattore riguarda il modo in cui le persone vanno d'accordo con gli altri. Mentre l'estroversione riguarda le fonti di energia e la ricerca di interazioni con gli altri, la piacevolezza riguarda l'orientamento verso gli altri. È un costrutto che si basa su come un individuo interagisce generalmente con gli altri.

I seguenti tratti ricadono sotto l'ombrello della piacevolezza: altruismo, fiducia, modestia, umiltà, pazienza, moderazione, tatto, cortesia, gentilezza, lealtà, altruismo, disponibilità, sensibilità, amabilità, allegria, considerazione.

Le persone molto gradevoli tendono ad essere benvolute, rispettate e sensibili ai bisogni degli altri. Probabilmente hanno pochi nemici e sono affettuosi con i loro amici e i loro cari, oltre che simpatizzanti per le difficoltà degli estranei (Lebowitz, 2016). Le persone nella fascia più bassa dello spettro della gradevolezza hanno meno probabilità di essere fidate e apprezzate dagli altri. Tendono ad essere insensibili, schietti, maleducati, di cattivo umore, antagonisti e sarcastici. Sebbene non tutte le persone che hanno un basso livello di gradevolezza siano crudeli o irritanti, è improbabile che lascino gli altri con una calda sensazione confusa.

3. *Nevroticismo*

Il nevroticismo non è un fattore di meschinità o incompetenza, ma uno di fiducia e di sentirsi a proprio agio nella propria pelle. Comprende la stabilità emotiva e il carattere generale.

Questi tratti sono comunemente associati al nevroticismo: imbarazzo, pessimismo, malumore, gelosia, paura, nervosismo, ansia, timidezza, diffidenza, autocritica, mancanza di confidenza, insicurezza, instabilità, ipersensibilità.

Quelli ad alto contenuto di nevroticismo sono generalmente inclini ad ansia, tristezza, preoccupazione e bassa autostima. Possono essere capricciosi o facilmente arrabbiati e tendono ad essere autocoscienti e insicuri di sé stessi (Lebowitz, 2016).

Gli individui che ottengono un punteggio nella fascia bassa del nevroticismo hanno maggiori probabilità di sentirsi sicuri di sé, sicuri di sé e avventurosi. Possono anche essere coraggiosi e liberi da preoccupazioni o dubbi su sé stessi.

4. *Apertura all'esperienza*

L'apertura all'esperienza è stata descritta come la profondità e la complessità della vita mentale e delle esperienze di un individuo (John & Srivastava, 1999). A volte è anche chiamato intelletto o immaginazione. L'apertura all'esperienza riguarda la disponibilità delle persone a provare cose nuove, la loro capacità di essere vulnerabili e la loro capacità di pensare fuori dagli schemi.

I tratti comuni relativi all'apertura all'esperienza includono: immaginazione. perspicacia. interessi vari. originalità. audacia. preferenza per la varietà. intelligenza. creatività. curiosità. percettività. intelletto. complessità / profondità.

Un individuo che è molto aperto all'esperienza è probabilmente qualcuno che ha un amore per l'apprendimento, ama le arti, si impegna in una carriera creativa o in un hobby e ama incontrare nuove persone (Lebowitz, 2016). Un individuo che è poco aperto all'esperienza probabilmente preferisce la routine alla varietà, si attiene a ciò che sa e preferisce arti e intrattenimento meno astratti.

5. *Estroversione*

Questo fattore ha due estremità familiari del suo spettro: estroversione e introversione. Riguarda da dove un individuo trae la sua energia e come interagisce con gli altri. In generale, gli estroversi traggono energia o si ricaricano interagendo con gli altri, mentre gli introversi si stancano di interagire con gli altri e riempiono la loro energia con la solitudine.

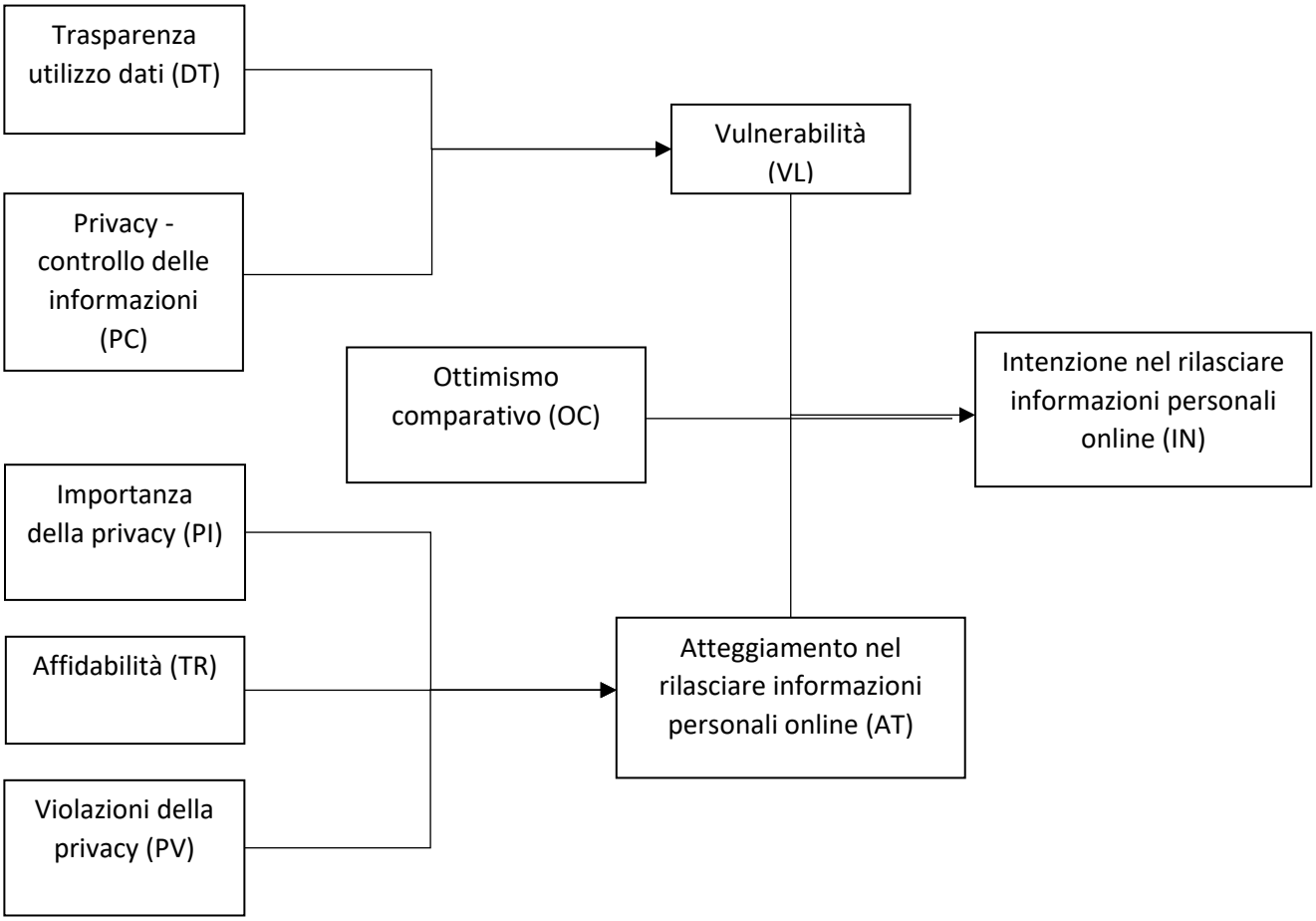
I tratti associati all'estroversione sono: socievolezza, assertività, allegria, natura in uscita, energia, loquacità, capacità di essere articolato, natura amante del divertimento, tendenza all'affetto, cordialità, fiducia sociale.

Le persone ad alto tasso di estroversione tendono a cercare opportunità di interazione sociale, dove sono spesso la "vita del partito". Stanno bene con gli altri, sono socievoli e inclini all'azione piuttosto che alla contemplazione (Lebowitz, 2016). Le persone a basso livello di estroversione hanno più probabilità di essere persone “di poche parole che sono silenziose, introspettive, riservate e premurose.

MODELLO PROPOSTO

Nel modello proposto vengono costituite e analizzate ipotesi per definire quali variabili hanno un impatto sulle intenzioni degli individui nel rilasciare le proprie informazioni personali online. In questo studio, la propensione a rilasciare informazioni personali online - analizzato tramite l’atteggiamento e le variabili che lo influenzano quali l’importanza della privacy (privacy ownership), l’affidabilità (privacy control), le violazioni della privacy (privacy turbulence) – e la vulnerabilità dei dati – analizzata attraverso il controllo della privacy e la trasparenza dei dati – sono esaminati empiricamente e stabiliti nel quadro teorico

Figura 1 - Modello proposto



3.3.1 – Trasparenza utilizzo dei dati

La trasparenza dei dati è fondamentale nel contesto di problemi più generali come la riservatezza e l'affidabilità dei dati. Ad esempio, consente agli interessati di avere una visione completa di come i loro dati personali vengono elaborati e utilizzati. Consente agli utenti dei dati di ottenere informazioni dettagliate sull'origine dei dati, nonché su eventuali modifiche apportate ai dati come un modo per valutare l'affidabilità e migliorare la qualità. Inoltre, la trasparenza dei dati consente alle organizzazioni di spiegare meglio le decisioni basate sui dati ai propri clienti e consente alle forze dell'ordine e alle aziende specializzate di indagare più facilmente sulle violazioni dei dati. La trasparenza dei dati sarà sempre più critica nel contesto dei domini applicativi in cui le decisioni vengono prese sulla base di tecnologie di big data e algoritmi di apprendimento automatico che possono essere imprecisi o discriminatori

o avere altri effetti negativi. Senza processi completi di trasparenza dei dati, è difficile, se non impossibile, indagare e prevenire l'uso scorretto dei dati.

Ad alto livello, la trasparenza dei dati può essere definita come “la capacità dei soggetti di accedere in modo efficace a tutte le informazioni relative ai dati utilizzati nei processi e nelle decisioni che li riguardano” (Bertino, et al., 2019). Questa definizione si basa sull'idea generale che i processi vengano eseguiti e le decisioni prese sulla base dei dati e che questi processi e decisioni abbiano un impatto sul soggetto. Pertanto, questa spiegazione copre due casi importanti:

1) quando i dati sul soggetto sono raccolti e utilizzati in un processo o decisione che ha interessato il soggetto
2) quando dati diversi dai dati relativi al soggetto sono utilizzati in un processo o decisione che interessa il soggetto.

Un esempio di quest'ultimo caso è quando le raccomandazioni sono generate da un classificatore costruito utilizzando i dati di un campione di popolazione che non includeva l'argomento. In tal caso, rientra nell'ambito della trasparenza dei dati fornire informazioni al soggetto sulle caratteristiche dei dati utilizzati per generare il classificatore anche se i suoi dati non sono stati utilizzati. Questa definizione sottolinea due requisiti principali. Il primo è che la trasparenza dei dati richiede non solo la divulgazione dei dati specifici utilizzati e per quali scopi, ma anche la divulgazione di metadati, ad esempio dove e con quali mezzi i dati sono stati raccolti. Il secondo requisito è che i soggetti dovrebbero essere in grado di accedere prontamente a tali informazioni e comprenderle. In altre parole, le informazioni dovrebbero essere facili da usare e non presentate in forme molto oscure. La nostra definizione include anche una classificazione più ampia del soggetto, che suddividiamo in quattro categorie

La teoria del Gossip afferma che la trasparenza sull’uso dei dati (di seguito "trasparenza") fornisce ai clienti informazioni su come l'azienda raccoglie, condivide e protegge i loro dati (Martin, et al., 2017). La trasparenza garantisce ai clienti la conoscenza di quali informazioni forniscono all'azienda, come vengono utilizzate e quali aziende partner possono accedere a tali dati (Kumar, et al., 2014) (Tucker, 2014). Quando la vulnerabilità dell'accesso ai dati è già bassa, è probabile che queste percezioni siano comunque deboli, quindi fornire ai clienti trasparenza dovrebbe avere scarso effetto sulla violazione o sulla fiducia. Tuttavia, potrebbe sopprimere gli effetti dannosi sulla violazione e sulla fiducia quando la vulnerabilità dell'accesso ai dati è elevata.

In particolare, Baumeister, et al., (2004) asseriscono che la trasparenza (assieme al controllo, separatamente e in modo interattivo) mitighi gli effetti dannosi di tutti i tipi di vulnerabilità dei dati dei clienti. Inoltre, la trasparenza (contiguamente al controllo) può sopprimere gli effetti dannosi sia sulla violazione che sulla fiducia quando la vulnerabilità dell'accesso ai dati è elevata. Se le aziende fornissero ai clienti sia trasparenza che controllo, la combinazione dovrebbe generare forti sentimenti di empowerment, anche se la loro vulnerabilità è significativa (Baker, et al., 2005). L'empowerment può quindi ridurre le aspettative di danno percepito a causa della vulnerabilità dell'accesso ai dati, perché i clienti credono di avere la conoscenza e il controllo sull'uso dei propri dati, il che mitiga le loro risposte emotive e attribuzioni negative

Ipotesi 1: la trasparenza nell'utilizzo dei dati (DT) influenza negativamente il sentimento di vulnerabilità (VL)

3.3.2 – Privacy – controllo delle informazioni

Nella nostra vita privata desideriamo controllare le informazioni sulle nostre vite. Vogliamo controllare le informazioni che potrebbero essere imbarazzanti o danneggiarci. Inoltre, desideriamo controllare le informazioni che potrebbero aumentare le nostre opportunità e consentirci di portare avanti i nostri progetti. La nozione di privacy e la nozione di controllo combaciano. Ma come si adattano insieme? Esiste una tradizione, soprattutto per quanto riguarda la riservatezza delle informazioni, per definire la privacy in termini di controllo. Alan Westin sostiene: "La privacy è la pretesa di individui, gruppi o istituzioni di determinare da soli quando, come e in che misura le informazioni su di loro vengono comunicate ad altri" (Westin, 1967). Successivamente, Arthur Miller dice: "... l'attributo fondamentale di un effettivo diritto alla privacy è la capacità dell'individuo di controllare la circolazione delle informazioni che lo riguardano ..." (Miller, 1971). In tempi più recenti Charles Fried afferma: "La privacy non è semplicemente la mancanza d'aria di informazioni su di noi nella mente degli altri, piuttosto è il controllo che abbiamo sulle informazioni su noi stessi". (Fried, 1984). Dag Elgesem suggerisce: "A mio avviso, avere privacy personale significa avere la capacità di acconsentire alla diffusione di informazioni personali" (Elgesem, 1996). Il controllo delle

informazioni personali è estremamente importante come, ovviamente, lo è la privacy. Il concetto stesso di privacy è meglio definito in termini di accesso limitato e non di controllo. La privacy, inoltre, riguarda fondamentalmente la protezione dalle intrusioni e dalla raccolta di informazioni da parte di altri. Ciò nonostante, il controllo individuale delle informazioni personali risulta estremamente importante nella gestione della privacy. Queste distinzioni hanno un'importanza pratica. È possibile avere il controllo ma nessuna privacy oppure la privacy ma nessun controllo. L'obiettivo finale è quello di mirare ad avere sia il controllo che la privacy: quando si attenuano tali distinzioni si è più vulnerabili a perderne una. Ad esempio, fornire tecnologie per il miglioramento della privacy (PET) che sembrano promuovere il controllo individuale può agire offuscando la necessità di una maggiore protezione della privacy, non fornirla. Un problema fondamentale nella definizione del concetto di privacy in termini di controllo individuale delle informazioni è che riduce molto ciò che può essere privato. Si riesce a controllare ben poco. In pratica, non è possibile controllare grandi quantità di informazioni personali che circolano attraverso miriadi di reti di computer e database. Se la privacy dipendesse per definizione dal nostro controllo individuale, semplicemente non ci sarebbe una privacy significativa

Il controllo del cliente (di seguito "controllo") sull'uso delle informazioni e sulle decisioni di gestione dei dati dovrebbe aiutare i clienti a sentirsi responsabilizzati in contesti ad alta vulnerabilità, che possono sopprimere i loro sentimenti di violazione (Kumar, et al., 2014) (Tucker, 2014). Con il controllo, un cliente può determinare se partecipare a determinate forme di condivisione dei dati, il che riduce l'incertezza e le percezioni di intrusione. Come per la trasparenza, quando la vulnerabilità dell'accesso ai dati è già bassa, è probabile che queste percezioni siano comunque deboli, quindi fornire ai clienti il controllo dovrebbe avere scarso effetto sulla violazione o sulla fiducia.

Ipotesi 2: il controllo delle informazioni relativamente alla privacy (PC) influenza negativamente il sentimento di vulnerabilità (VL)

3.3.3 – Importanza della privacy

La privacy è importante perché ci consente di divulgare selettivamente le informazioni personali e di impegnarci in comportamenti appropriati e necessari per creare e mantenere relazioni personali diversificate. Senza questo controllo, è implicito, la diversità delle relazioni diminuirebbe; le relazioni si "appiattirebbero" (Rachels, 1976)

Il controllo sull'accesso a noi stessi e alle informazioni su noi stessi è giustificato in virtù del ruolo abilitante che questo controllo gioca nella nostra capacità di creare e mantenere la diversità delle relazioni sociali che consideriamo parte di una buona vita. Tali relazioni sociali includono quella di essere un padre, una madre, una figlia, un figlio, una moglie, un marito, un amico, un socio in affari, un compagno di squadra, ecc. Queste relazioni sono definite da comportamenti, atteggiamenti e certi tipi di scambi di informazioni caratteristici. Diversi tipi di relazioni richiedono (e sono in parte definiti da) il dare e il trattenere determinati tipi e quantità di informazioni personali. L'amicizia richiede rivelazioni su noi stessi che, ad esempio, una relazione d'affari non lo fa. Rivelare le nostre speranze, sogni o delusioni a un amico è appropriato e previsto nel caso dell'amicizia, ma non nel caso di una relazione d'affari (a meno che non si sia evoluto in un'amicizia). Un presunto amico a cui tali informazioni non erano state rivelate, laddove fossero state rivelate ad altri, poteva legittimamente chiedersi se lui o lei fosse davvero considerato un amico dall'altro. Affinché le persone abbiano e sostengano tali rapporti, le intrusioni o le invasioni della privacy che minano la nostra capacità di impegnarsi in comportamenti costitutivi o critici per queste relazioni devono essere vietate o limitate. Inoltre, la divulgazione e lo scambio di informazioni devono essere limitati alle parti che partecipano alla relazione. Nel caso dei comportamenti, gli individui devono essere in grado di controllare o limitare l'accesso a sé stessi e agli spazi in cui conducono le loro relazioni. Se non avessero tale controllo, potrebbero non essere in grado di impegnarsi nei comportamenti costitutivi del tipo specifico di relazione. Ci sono due ragioni per cui tali comportamenti potrebbero essere limitati dalla mancanza di privacy di accesso. In primo luogo, possono, per motivi emotivi, essere inibiti rispetto al comportamento in un certo modo se non viene fornita la privacy di accesso. In secondo luogo, il comportamento può, di per sé o in modo derivato, fornire la conoscenza della persona, conoscenza che normalmente sarebbe riservata alle parti della relazione. Per tutti questi motivi, gli individui hanno bisogno di controllare l'accesso a sé stessi e ai propri spazi.

Gli individui devono anche essere in grado di controllare il flusso di informazioni su sé stessi. Il motivo è che i rapporti si basano sullo scambio esclusivo e selettivo di informazioni tra le parti del rapporto. Se le persone perdono il controllo sulle proprie informazioni personali, ciò metterà a repentaglio la loro capacità di effettuare le divulgazioni o comunicazioni selettive appropriate. Naturalmente, ciò non impedirà loro di impegnarsi effettivamente nell'atto comunicativo pertinente. Tuttavia, la perdita del controllo sulle informazioni personali minerà la loro capacità di comunicare selettivamente ed esclusivamente informazioni su sé stessi. Una volta divulgate a terzi o pubblicate al grande pubblico, l'individuo perde la capacità di raccontare ad un amico (ad esempio) qualcosa su sé stesso che l'amico non sa ma, nel ruolo di amico, dovrebbe sapere, e cosa gli altri al di fuori del ruolo di amico non dovrebbe sapere, ma, appunto, lo so. L'informazione perde così valore per l'individuo rispetto agli scambi di informazioni che costituiscono il rapporto in questione. Viene fornito, quindi, un resoconto di diversi aspetti della privacy che possono essere suddivisi in almeno due grandi categorie: (a) controllo sull'accesso a sé stessi e ai propri spazi e (b) controllo sull'accesso alle proprie informazioni.

Ipotesi 3: l'importanza della privacy (PI) influenza positivamente l'atteggiamento nel rilasciare le informazioni personali online (AT)

3.3.4 – Affidabilità

Le aziende online inseriscono le loro politiche sulla privacy sui loro siti Web per costruire la fiducia dei consumatori. Le politiche sulla privacy online mirano a ridurre il timore che le loro informazioni personali vengano divulgate (Wu, et al., 2012). I clienti online spesso misurano il rischio dell'attività online sull'uso improprio o sulla rivelazione della privacy delle informazioni (Mlne & Culnan, 2004). Devono nutrire sentimenti di fiducia nei confronti dei siti web prima di rivelare informazioni (Shoenbachler & Gordon, 2002). La ricerca suggerisce che la disponibilità a fornire informazioni personali in linea è una questione importante nel mondo online, nonché una preoccupazione per la fiducia e la privacy e può influenzare il successo delle imprese elettroniche. La privacy è stata un argomento delicato molto prima dell'invenzione dei computer. È stato definito come il desiderio delle persone di scegliere

liberamente in quali circostanze e in che misura esporre sé stesse, il proprio atteggiamento e il proprio comportamento agli altri (Westin, 1967). L'anonimato, che significa mantenere le restanti informazioni non identificate nella sfera pubblica, è un altro concetto cruciale relativo alla privacy. Significa essere in grado di farlo. Al giorno d'oggi, la diffusione di Internet elimina la capacità delle persone che utilizzano il Web di rimanere non identificate. Gli utenti online lasciano molte impronte elettroniche che descrivono in dettaglio il loro comportamento e le loro preferenze che possono essere facilmente ottenute, utilizzate o condivise con estranei (Zviran, 2008). A causa del rapido sviluppo di nuove tecnologie Web, la privacy degli utenti di Internet può essere invasa in molti modi diversi. Inoltre, i consumatori non hanno alcun controllo sull'uso secondario delle informazioni personali fornite durante la loro attività su Internet. Enormi quantità di informazioni personali sugli individui vengono raccolte e utilizzate dalle aziende attraverso il modulo di registrazione e moduli d'ordine e / o attraverso l'uso di software di tracciamento o cookie. Queste informazioni ottenute consentono alle aziende di seguire le attività online dei clienti e raccogliere informazioni sugli interessi e le preferenze personali. Questi dati diventano preziosi per le aziende, poiché aiutano a identificare le richieste dei clienti, creare programmi pubblicitari efficaci e vendere meglio lo spazio pubblicitario sui loro siti web (Liu, et al., 2004). La preoccupazione per la privacy online porta a una mancanza di disponibilità a fornire informazioni personali online e, talvolta, anche alla riluttanza a utilizzare Internet. Le preoccupazioni dei consumatori sulla privacy non limitano solo lo sviluppo del commercio elettronico, ma possono anche influire sulla validità e sulla completezza dei database dei consumatori. Per evitare le inesattezze, le società Internet dovrebbero garantire agli utenti che la loro privacy sia ben protetta. Il problema si riduce al livello di fiducia tra il consumatore e l'azienda. Costruire la fiducia diventa un elemento chiave per ridurre le preoccupazioni sulla privacy dei consumatori e per migliorare le relazioni tra consumatori e imprese (Milne & Boza, 2000). La disponibilità a fornire informazioni personali online è strettamente correlata alle preoccupazioni sulla privacy. Uno dei modi per migliorare la fiducia dei consumatori e ridurre la preoccupazione per la privacy è creare una politica sulla privacy. Tali politiche forniscono una spiegazione ai clienti su come i siti web utilizzeranno i dati personali e di conseguenza li informano sugli strumenti di sicurezza e sui sistemi di protezione dei siti web. Le aspettative a riguardo sono negative, si presuppone che l'affidabilità influenzi negativamente in quanto la fiducia degli individui quando si parla di privacy è scarsa.

Ipotesi 4: l'affidabilità (TR) influenza negativamente l'atteggiamento nel rilasciare le informazioni personali online (AT)

3.3.5 – Violazioni della privacy

La frequenza e l'entità della violazione della privacy nel web è aumentata in termini di portata e intensità e l'esposizione dei dati privati dei clienti su larga scala è diventata un evento comune. Sebbene esistano leggi rigide per la protezione della privacy, la facilità di raccolta e trasferimento dei dati privati dei clienti e un desiderio sempre più ampio di combinare e integrare i dati dei clienti per l'analisi di mercato ha reso l'uso non autorizzato dei dati privati dei clienti allettante per le aziende nel loro perseguimento di maggiore quota di mercato e maggiori profitti (McFarland, 2012). Sebbene l'hacking sia un evento esterno e imprevisto, l'uso non autorizzato dei dati privati dei clienti è una decisione interna delle aziende. Tuttavia, sia la violazione da parte degli hacker che l'uso intenzionale non autorizzato dei dati privati dei clienti potrebbero avere conseguenze dannose per le aziende, come è stato dimostrato dalla reazione degli utenti di Facebook alla sua modifica della politica sulla privacy e dal suo metodo di ricerca più invadente che espone le informazioni dei clienti su Facebook (Sengupta, 2013). La violazione delle informazioni private dei clienti potrebbe violare la loro fiducia nell'azienda. È ampiamente riconosciuto che la fiducia è necessaria affinché qualsiasi azienda possa prosperare, ed è ancora più necessaria negli ambienti online in cui il fiduciario può sentirsi più vulnerabile quando ha a che fare con un fiduciario senza volto e remoto. La perdita di fiducia porta alla perdita di vendite e ad altri danni irreparabili e "devastanti" (Tomlinson & Mayer, 2009). La conseguenza della violazione è che erode la successiva fiducia dell'utente, il che può ridurre la misura in cui il fiduciario (utente) collaborerà con il fiduciario fornendoli le proprie informazioni personali (Liao, et al., 2009). Bies & Tipp, (1996) definiscono la violazione della fiducia come "aspettative non soddisfatte riguardo al comportamento di un altro o quando [il fiduciario] non agisce in modo coerente con i propri valori". Pertanto, eventi negativi e trasgressioni riguardo la trasmissione dei dati riducono la propensione dell'individuo a rilasciare i propri dati (Tyler & Kramer, 1996).

Ipotesi 5: le violazioni della privacy (PV) influenzano negativamente l'atteggiamento nel rilasciare le informazioni personali online (AT)

3.3.6 – Ottimismo comparativo

La maggior parte degli studi sulla privacy online si è concentrata sul cosiddetto paradosso della privacy (Norberg, et al., 2007) in base al quale gli utenti mostrano una preoccupazione sostanziale per l'uso improprio delle informazioni personali ma tendono a non impegnarsi in comportamenti di protezione della privacy (ad es. impostazioni sulla privacy o cancellazione dei cookie) o addirittura a intraprendere comportamenti rischiosi (ad esempio, visitare siti sospetti o rivelare informazioni personali critiche) (Gross & Acquisti, 2005). Gli atteggiamenti e gli effettivi comportamenti degli utenti online sono generalmente incoerenti e in alcuni contesti addirittura contraddittori. Per risolvere il paradosso della privacy, studi recenti si sono concentrati sulla mancanza di competenze, conoscenze o abilità online tra gli utenti che questi studi definiscono teoria del deficit cognitivo. Fondamentalmente, la teoria del deficit cognitivo sostiene che gli utenti sono sinceramente preoccupati per la violazione della privacy online ma mancano di conoscenze specifiche su come proteggere la loro privacy (Debatin, et al., 2009) (Park, 2013). Sebbene la teoria del deficit cognitivo sia una spiegazione efficace e promettente del motivo per cui gli utenti si impegnano in comportamenti online rischiosi a livello individuale, è limitata nella sua capacità di spiegare perché la privacy online è emersa come un problema `` sociale '' che molti cittadini vogliono affrontare attraverso la legge protezione (Solove, 2011). In effetti, le persone temono che le aziende private pratichino la sorveglianza nel prossimo futuro (Andrejevic, 2007) e temono che i gruppi socialmente vulnerabili, in particolare i giovani utenti online, avranno maggiori probabilità di cadere vittime di violazioni della privacy (Hodder & Livingstone, 2009). Casi come quello di Kimberly Swan (Case, 2009), una giovane lavoratrice licenziata perché ha pubblicato reclami relativi al lavoro su Facebook, sono allarmanti, anche se rari. Per i motivi di cui sopra, le preoccupazioni sulla privacy online dovrebbero essere indagate a livello sociale, non solo a livello personale, e la letteratura sul paradosso della privacy dovrebbe distinguere il rischio per la privacy personale dal rischio per gli altri. Per quanto a nostra conoscenza, solo uno studio (Cho, et al., 2010) ha confrontato queste due fonti (ad esempio, personali rispetto ad altre) di stime del rischio per la privacy. Coerentemente con la letteratura comparativa sull'ottimismo relativa

ad altri rischi (ad es. Cancro o incidenti stradali), Cho, et al., (2010) hanno riferito che gli utenti, in generale, credono che la propria privacy sia ben protetta ma che la privacy online degli altri utenti sia vulnerabile a intrusioni esterne. Nonostante i loro risultati teorici, Cho, et al., (2010) hanno definito gli altri come "altri generalizzati" e quindi non hanno tentato di differenziare gli obiettivi di confronto. La letteratura suggerisce che il livello di ottimismo comparativo è correlato alla tipicità degli obiettivi di confronto (Helweg-Larsen & Shepperd, 2001) (Perloff, 2009). Ad esempio, se gli obiettivi di confronto sono noti per essere molto vulnerabili a un rischio particolare (ad esempio, le donne come vittime di reati), l'ottimismo comparativo è accresciuto tra i meno vulnerabili socialmente. Nel contesto del rischio per la privacy online, i giovani utenti sono solitamente discussi come forti candidati a cadere vittime di violazioni della privacy, mentre gli utenti più anziani sono meno preoccupati in parte perché non sono così attivi online e in parte perché i loro giorni rimanenti sono brevi

Ipotesi 6: l'ottimismo comparativo (CO) influenza negativamente le intenzioni nel rilasciare informazioni personali online (IN)

Essendo le ultime due variabili del modello, la vulnerabilità (VL) e l'atteggiamento nel rilasciare informazioni personali online (AT) possono rivelare diverse incognite circa le intenzioni degli individui nel rilasciare le informazioni personali online (IN)

Ipotesi 7: la vulnerabilità (VL) influenza positivamente le intenzioni nel rilasciare informazioni personali online (IN)

Ipotesi 8: l'atteggiamento nel rilasciare informazioni personali online (AT) influenza negativamente le intenzioni nel rilasciare informazioni personali online (IN)

L'ottimismo comparativo viene inserito come moderatore nelle relazioni AT -> IN e VL -> IN. In generale, le relazioni di moderazione sono ipotizzate a priori dal ricercatore e specificamente testate. Il test della relazione moderatrice dipende dal fatto che il ricercatore ipotizzi se una specifica relazione del modello o se tutte le relazioni del modello dipendono dai punteggi del moderatore. La moderazione descrive una situazione in cui la relazione tra due costrutti non è costante ma dipende dai valori di una terza variabile, denominata variabile moderatore oppure, come in questo caso, quando un moderatore non fa altro che rafforzare una relazione già esistente. Non a caso la variabile moderatore (o costrutto) cambia la forza o anche la direzione di una relazione tra due costrutti nel modello. I moderatori possono essere

presenti nei modelli strutturali in diverse forme. Possono rappresentare tratti osservabili come sesso, età o reddito ma possono anche rappresentare tratti non osservabili come l'attitudine al rischio, l'atteggiamento verso un marchio o il gradimento degli annunci. Pertanto:

Ipotesi 9: l'ottimismo comparativo (CO) funge da moderatore nella relazione AT -> IN. CO modera la relazione tra AT e IN in modo tale che a un livello più alto di CO si rafforzerebbe la relazione negativa tra AT e IN.

Ipotesi 9a: l'ottimismo comparativo (CO) funge da moderatore nella relazione VL -> IN. CO modera la relazione tra VL e IN in modo tale che a un livello più alto di CO si rafforzerebbe la relazione positiva tra AT e IN.

Tabella 3 - Variabili e scale

VARIABILE	ITEMS	FONTE
PRIVACY (CONTROLLO DELLE INFORMAZIONI)	Ritengo di avere il controllo su cosa succede alle mie informazioni personali	Il grado di controllo è misurato con una scala Likert a sette punti (Martin, et al., 2017)
	Spetta a me stabilire quanto un entità può utilizzare le mie informazioni personali	
	Ho voce in capitolo su come le mie informazioni vengono usate	
	Ho voce in capitolo sulla condivisione delle mie informazioni personali con altri.	
IMPORTANZA DELLA PRIVACY	Sono sensibile al modo in cui le aziende gestiscono le mie informazioni personali.	Il grado di sensibilità è misurato con una scala Likert a sette punti (Martin, et al., 2017)
	È importante mantenere intatta la mia privacy dalle società online.	
	La privacy personale è molto importante, rispetto ad altri soggetti.	
	Sono preoccupato per le minacce alla mia privacy personale	
TRASPARENZA UTILIZZO DATI	Le attività di gestione delle mie informazioni personali online da parte dei soggetti (social	Il grado di chiarezza viene

	networks, siti internet, provider di servizi telefonici etc.) a cui le rilascio sono: • Chiare / Non chiare • Confuse / Dirette • Difficili / Facili da comprendere • Vaghe / Trasparenti	misurato con una scala di differenziale semantico a sette punti (Martin, et al., 2017)
AFFIDABILITÀ	I soggetti (social networks, siti internet, provider di servizi telefonici etc.) a cui rilascio le mie informazioni online: • Disonesti / Onesti • Falsi / Sinceri • manipolativi / Non manipolativi • Non affidabili / Affidabili	Il grado di affidabilità viene misurato con una scala di differenziale semantico a sette punti (Kirmani, et al., 2017)
VIOLAZIONI DELLA PRIVACY	Riguardo le attività con le mie informazioni personali da parte dei social networks che utilizzo mi sento più o meno violato	Il grado di in cui una persona si sente mancata di rispetto e tradita è misurato con una scala Likert a sette punti (Martin, et al., 2017)
	Riguardo le attività con le mie informazioni personali da parte dei motori di ricerca che utilizzo mi sento più o meno violato	
	Riguardo le attività con le mie informazioni personali da parte dei browser Internet che utilizzo mi sento più o meno violato	
	Riguardo le attività con le mie informazioni personali da parte dei provider di servizi telefonici che utilizzo mi sento più o meno violato	
VULNERABILITÀ	Le informazioni personali che i social networks che utilizzo hanno di me mi fanno sentire più o meno vulnerabile	Il grado di suscettibilità a subire danni è misurato con una scala Likert a sette
	Le informazioni personali che i motori di ricerca che utilizzo hanno di me mi fanno sentire più o meno vulnerabile	

	Le informazioni personali che i browser Internet che utilizzo hanno di me mi fanno sentire più o meno vulnerabile	punti (Martin, et al., 2017)
	Le informazioni personali che i provider di servizi telefonici che utilizzo hanno di me mi fanno sentire più o meno vulnerabile	
ATTEGGIAMENTO NEL RILASCIARE INFORMAZIONI PERSONALI ONLINE	Quando penso a come le mie informazioni personali online vengono gestite sono più predisposto a fornire informazioni veritiere	Per misurare quanto una persona ritiene corretto fornire informazioni personali si utilizza una scala Likert con sette punti (Martin, et al., 2017)
	Quando penso a come le mie informazioni personali online vengono gestite fornisco di proposito informazioni personali non veritiere	
	Quando penso a come le mie informazioni personali online vengono gestite penso che vada bene dare informazioni personali fuorvianti	
INTENZIONE NEL RILASCIARE INFORMAZIONI PERSONALI ONLINE	Non mi crea alcun problema rilasciare le mie informazioni personali online	Per misurare il grado di accordo si utilizza una scala di intenzione comportamentale con sette punti (Davis & Warshaw, 1992)
	È probabile che in futuro continuerò a rilasciare le mie informazioni personali online	
	Ho intenzione di continuare a rilasciare le mie informazioni personali online	
OTTIMISMO COMPARATIVO	Ho maggiori probabilità di avere un'esperienza negativa sulla privacy rispetto agli altri utenti a seguito dell'utilizzo dei social networks	Il grado di comparazione viene misurato con una scala Likert a sette punti (Baek, et al., 2014)
	Ho maggiori probabilità di avere un'esperienza negativa sulla privacy rispetto agli altri utenti a seguito dell'utilizzo dei motori di ricerca	
	Ho maggiori probabilità di avere un'esperienza negativa sulla privacy rispetto agli altri utenti a seguito dell'utilizzo dei browser di ricerca	

	Ho maggiori probabilità di avere un'esperienza negativa sulla privacy rispetto agli altri utenti a seguito dell'utilizzo dei provider di servizi telefonici	

3.4 – COLLEZIONE DEI DATI

L'analisi dello studio è stata effettuata utilizzando SmartPls. Le statistiche descrittive sono stare utilizzate per determinare il profilo del campione. Le statistiche descrittive sui dati demografici, le domande di riscaldamento, e le domande sull'utilizzo di Internet e sulla conoscenza del tema della raccolta dati sono state analizzate utilizzando Microsoft Excel. SmartPLS è stato poi utilizzato per effettuare i test sulle ipotesi.

La collezione dei dati è avvenuta attraverso un questionario di 21 domande volte a indagare le dimensioni indicate precedentemente. Il questionario è stato creato tramite Qualtrics, una piattaforma di experience Management (XM) studiata per ottimizzare la ricerca circa le esperienze su clienti, dipendenti, prodotti e brand dei clienti, dei membri di un'azienda e dei colleghi, nonché adatta alla somministrazione di analisi e sondaggi. Il questionario è stato diffuso per un periodo di 13 giorni (dal 24 febbraio all' marzo 2021, data di chiusura del questionario). La somministrazione è avvenuta online in versione digitale in una sola lingua, l'italiano, a persone che si sono sottoposte in maniera del tutto volontaria all'indagine. I mezzi di somministrazione sono stati prevalentemente i social network (WhatsApp, Facebook, LinkedIn, Instagram), via e-mail e attraverso una diffusione a catena tramite passaparola a familiari, parenti e amici di amici.

La ricerca si è concentrata prevalentemente su persone che navigano sul web per più di un'ora al giorno e persone con un grado di istruzione minimo (diploma di scuola secondaria di secondo grado). A questo proposito, il questionario è stato rivolto a persone che rispecchiassero queste caratteristiche come una certa abitudine e frequenza a navigare online e quindi lavoratori e studenti con un certo grado di istruzione e assiduamente connessi sul web. Il grado di istruzione è stato inserito per avere un campione più mirato e meno dispersivo. La frequenza all'utilizzo del web, invece, perché la navigazione online era un requisito necessario e fondamentale per valutare la bontà del questionario del rispondente.

Il questionario si apre con alcune domande di carattere demografico, alcune domande di riscaldamento e le due domande filtro. Le prime domande di carattere demografico indagano il genere, l'età, e la professione. Le domande di riscaldamento, invece, indagano la provenienza del rispondente, ovvero come è arrivato a compilare il questionario (se dai social, via e-mail o di persona), anche da dove deriva la sua conoscenza riguardo il tema della raccolta dati online e quanto crede di essere informato riguardo questo tema.

Successivamente, sono state proposte una serie di domande che riguardano il grado di accordo/disaccordo su alcuni items – propri delle variabili che si intendono analizzare – sulla base di una scala Likert da 1 a 7 (1= Totalmente in disaccordo, 7= Assolutamente d'accordo). In mezzo, in maniera del tutto casuale, sono state inserite due attention check questions uguali, ovvero "Rispondere 2 a questa domanda", per identificare i questionari che non sono stati svolti con coscienziosità e quindi non pertinenti.

Le domande finali riprendono le domande iniziali (genere, età, titolo di studio conseguito) con la funzione di attention check question per cercare una corrispondenza tra le stesse domande poste all'inizio e queste ultime in fase di conclusione. In aggiunta, sono state inserite altre domande a carattere demografico per indagare la provincia di residenza e il livello di reddito.

È stato rilevato un campione di 470 persone di cui si è svolto uno screening iniziale analizzando i questionari aperti tramite il link ma non iniziati. I questionari iniziati ammontano a 444 da cui, in seconda analisi tramite le prima domande filtro "Qual è il titolo di studio più alto che hai conseguito?" e successivamente con la seconda "Con quale frequenza navighi su internet (motori di ricerca, social networks, mail etc.) al giorno?". sono stati tenuti validi 344 questionari. Di conseguenza, tramite la attention check question "Rispondere 2 a questa domanda" proposta due volte, sono stati scelti 248 risposte per arrivare a 239 in ultima fase di controllo con la concordanza tra le domande di età e genere poste sia all'inizio che alla fine. L'ammontare finale delle risposte valide da analizzare è risultato essere 239. Tuttavia, visti i limiti di accesso al software nella versione gratuita utilizzata e stabiliti per un massimo di 100 record, sono stati scelti le prime 100 risposte su 239 in ordine di compilazione del questionario (data e ora).

Di seguito sono riportate le risposte alle domande di profilazione poste all'inizio e alla fine del questionario

Tabella 4 – Profilazione demografica (100 intervistati)

	N	%
Genere		
Donna	51	51%
Preferisco non specificarlo	1	1%
Uomo	48	48%
Età in anni compiuti		
>65	1	1%
18-25	41	41%
26-35	22	22%
36-45	13	13%
46-55	17	17%
55-65	6	6%
Come sei venuto a conoscenza di questo sondaggio?		
Di persona	7	7%
E-mail	12	12%
WhatsApp	81	81%
Qual è il titolo di studio più alto che hai conseguito?		
Diploma di scuola secondaria di secondo grado	**52**	**52%**
Laurea specialistica	19	19%
Laurea triennale	20	20%
Master o superiore	9	9%
Qual è la tua professione?		
Disoccupato	6	6%
Impiegato	53	53%
Libero professionista	16	16%
Studente	15	15%
Studente / lavoratore	10	10%
Con quale frequenza navighi su internet (motori di ricerca, social networks, mail etc.) al giorno?		
> 12 ore	1	1%
Tra le 2 e le 5 ore	68	68%
tra le 5 e le 8 ore	21	21%
tra le 8 e le 12 ore	10	10%
Quanto ritieni di essere informato riguardo il tema della raccolta dei dati personali online? (1= Per nulla informato, 7= Totalmente informato)		
1 = PER NULLA INFORMATO	10	10%
2	16	16%
3	23	23%
4 = MEDIAMENTE INFORMATO	24	24%
5	14	14%
6	11	11%
7 = TOTALMENTE INFORMATO	2	2%
Da dove deriva la tua conoscenza riguardo il tema della raccolta dati online? – Risposta multipla		

Notiziari, giornali, telegiornali	21	
Internet, web	64	
Esperienza personale	34	
Scuola, università	13	
Famiglie, amici	14	
Termini e condizioni di utilizzo	37	
Provincia di residenza		
Lecce	1	1%
Londra	1	1%
Padova	89	89%
Pavia	1	1%
Pordenone	1	1%
Salerno	5	5%
Verona	1	1%
Vicenza	1	1%
Reddito familiare		
< 15.000,00 €	12	12%
> 100.000,00 €	3	3%
15.000 - 49.999,00 €	66	66%
50.00,00 € - 79.999,00 €	13	13%
80.000,00 € - 99.999,00 €	6	6%

I risultati hanno indicato una quasi parità di genere tra i rispondenti, con 51% di donne e 48% di uomini, prevalentemente in età giovane. Infatti, il 41% delle persone ha età compresa tra i 18 e i 25 anni e il 22% tra i 26 e 35. Il campione analizzato è concentrato prevalentemente nella provincia di Padova (89%) e nel nord Italia. Questo perché il mezzo tramite cui i rispondenti sono approdati sul questionario è stato prevalentemente l'app di messaggistica istantanea WhatsApp (81%) e via e-mail (12%), ovvero i primi a cui il questionario è stato somministrato. Il campione originario di 470 rispondenti ha avuto una diffusione più diramata sia in Italia (Italia del sud, nord-ovest) ma anche all'estero (Germania e Svezia) grazie soprattutto ad altri mezzi come i social networks (Facebook, LinkedIn, Instagram). Nel valutare lo stato di reddito, si è riscontrato come il 66% delle persone ha un livello di reddito compreso tra 15.000,00 – 49.000,00 euro e un 12% al di sotto dei 15.000,00 euro.

Questi dati sono coerenti e in linea con un ulteriore informazione rilevante, ovvero le ore di navigazione su Internet. Escluse le ore di navigazione per motivi di lavoro, il 68% afferma che passa online tra le 2 e le 5 ore al giorno e il 21% delle persone tra le 5 e le 8 ore giornaliere. Infatti, sono proprio i ragazzi più giovani, studenti e giovani lavoratori appartenenti alla

Generazione Z (18-25 anni) e i Millennials (26–35 anni), a fruire maggiormente dei servizi online.

Approfondendo l'analisi sul tema della raccolta dati, si evince come il 73% abbia un livello di conoscenza a riguardo medio-basso (10% per nulla informato, 24% mediamente informato, 39% nel mezzo) e che tale conoscenza derivi in maggior misura direttamente dal mondo online (Internet/web, termini e condizioni di utilizzo, esperienza personale). Questi dati rispecchiano quanto enunciato nel capitolo precedente, dove si spiega come prevale la conoscenza del tema in maniera diretta tramite web e come la conoscenza degli individui sul tema della raccolta dei dati online sia mediamente scarsa se non del tutto assente.

Il campione analizzato risulta essere coerente con le premesse del capitolo precedente, ovvero:

- Scarsa informazione circa il tema della raccolta dati online
- Tempo di utilizzo e navigazione in Internet mediamente alta (escluse le ore di navigazioni per motivi professionali)
- Età media giovane

3.5 – ANALISI DEI DATI – SMARTPLS

Esistono due approcci principali per stimare le relazioni in un modello di equazioni strutturali (Hair, et al., 2011). Uno è l'approccio CB-SEM più ampiamente applicato, l'altro è PLS-SEM. Ciascuno è appropriato per un diverso contesto di ricerca e i ricercatori devono comprendere le differenze per applicare il metodo corretto.

Per capire quando utilizzare PLS-SEM rispetto a CB-SEM bisogna concentrarsi sulle caratteristiche e sugli obiettivi che distinguono i due metodi (Hair, et al., 2012). In situazioni in cui la teoria è meno sviluppata, i ricercatori dovrebbero considerare l'uso di PLS-SEM come approccio alternativo al CB SEM. Ciò è particolarmente vero se l'obiettivo principale dell'applicazione della modellazione strutturale è la previsione e la spiegazione dei costrutti target (Rigdon, 2012). Una differenza concettuale cruciale tra PLS-SEM e CB-SEM riguarda il modo in cui ciascun metodo tratta le variabili latenti incluse nel modello. CB-SEM considera i costrutti come fattori comuni che spiegano la covarianza tra i suoi indicatori associati. I punteggi di questi fattori comuni non sono né conosciuti né necessari nella stima dei

parametri del modello. PLS-SEM, d'altra parte, utilizza proxy per rappresentare i costrutti di interesse, che sono composti di indicatori variabili ponderati per un particolare costrutto. Per questo motivo, PLSSEM costituisce un approccio basato su compositi al SEM, che allenta i forti presupposti del CB-SEM secondo cui tutta la covarianza tra insiemi di indicatori è spiegata da un fattore comune (Henseler, et al., 2014) (Rigdon, 2012) (Rigdon, et al., 2014).

L'algoritmo PLS-SEM basato sulla varianza è stato originariamente sviluppato da (Wold, 1985) e successivamente esteso (Lohmöller, 1989) (Bentler & Huang, 2014), (Dijkstra, 2014), (Dijkastra & Henseler, 2015). L'algoritmo stima i coefficienti del percorso e altri parametri del modello in un modo che massimizza la varianza spiegata dei costrutti dipendenti (cioè, minimizza la varianza inspiegabile).

I modelli di percorso nel metodo SEM sono diagrammi utilizzati per visualizzare visivamente le ipotesi e le relazioni variabili che vengono esaminate quando viene applicato il SEM (Hair, et al., 2011) (Hair, et al., 2016). I costrutti (cioè le variabili che non sono misurate direttamente) sono rappresentati nei modelli di percorso come cerchi o ovali. Gli indicatori, chiamati anche elementi (items) o variabili manifeste, sono le variabili proxy misurate direttamente che contengono i dati grezzi. Sono rappresentati nei modelli di percorso come rettangoli. Le relazioni tra i costrutti così come tra i costrutti e gli indicatori loro assegnati sono mostrate come frecce. In PLS-SEM, le frecce sono sempre unidirezionali, rappresentando così le relazioni direzionali. Le frecce a una testa sono considerate relazioni predittive e, con un forte supporto teorico, possono essere interpretate come relazioni causali. La teoria strutturale mostra come le variabili latenti sono correlate tra loro (cioè mostra i costrutti e le relazioni di percorso tra di loro nel modello strutturale). Le variabili possono anche servire sia come variabili indipendenti che dipendenti. Quando le variabili latenti servono solo come variabili indipendenti, vengono chiamate variabili latenti esogene. Quando le variabili latenti servono solo come variabili dipendenti o come variabili indipendenti e dipendenti, vengono chiamate variabili latenti endogene. Qualsiasi variabile latente che ha solo frecce a una testa che escono da essa è una variabile latente esogena. In contrasto, le variabili latenti endogene possono avere frecce a una punta che entrano ed escono da esse o solo che entrano in esse.

La stima del modello fornisce misure empiriche delle relazioni tra gli indicatori e i costrutti (modelli di misurazione), nonché tra i costrutti (modello strutturale). Le misure empiriche ci consentono di confrontare i modelli di misurazione e i modelli strutturali teoricamente stabiliti con la realtà, rappresentata dai dati del campione. In altre parole, possiamo

determinare quanto bene la teoria si adatta ai dati. I risultati di PLS-SEM vengono esaminati e valutati utilizzando un processo sistematico. L'obiettivo di PLS-SEM è massimizzare la varianza (cioè il valore R^2) delle variabili latenti endogene nel modello del percorso PLS. Per questo motivo, la valutazione della qualità della misurazione PLS-SEM e dei modelli strutturali si concentra sulle metriche che indicano le capacità predittive del modello.

L'esame delle stime PLS-SEM consente al ricercatore di valutare l'affidabilità e la validità delle misure del costrutto. In particolare, la misurazione multivariata implica l'utilizzo di diverse variabili (cioè multi-item) per misurare un costrutto. Quando si valutano i modelli di misurazione, dobbiamo distinguere tra costrutti misurati in modo riflettente e formattato.
I due approcci si basano su concetti diversi e richiedono pertanto la considerazione di diverse misure di valutazione. I modelli di misurazione riflessivi vengono valutati in base alla loro coerenza interna, affidabilità e validità. Le misure specifiche includono l'affidabilità composita (come mezzo per valutare l'affidabilità della coerenza interna), la validità convergente e la validità discriminante. Dopo la stima del modello, vengono utilizzate metriche diverse per valutare le misure formative per la validità convergente, la significatività e la pertinenza dei pesi degli indicatori e la presenza di correlazione tra gli indicatori. Quindi, dopo aver stabilito l'affidabilità e la validità, i criteri di valutazione primari per i risultati PLS-SEM sono i coefficienti di determinazione (valori R^2) così come la dimensione e la significatività dei coefficienti di percorso.

3.5.1 – Validità del costrutto

La validità di un costrutto include l'affidabilità composita per valutare la coerenza interna, l'affidabilità dell'indicatore individuale e la varianza media estratta (AVE) per valutare la validità convergente, ovvero il grado di correlazione tra due misure dello stesso costrutto (Anderson & Gerbing, 2013). La valutazione dei modelli di misurazione riflessivi include anche la validità discriminante, che si riferisce alla misura in cui un costrutto è veramente distinto da altri costrutti per standard empirici . Il criterio di Fornell-Larcker, i carichi incrociati e in particolare il rapporto di correlazioni eterotatto-monotratto (HTMT) possono essere utilizzati per esaminare la validità discriminante (Hair, et al., 2017). Nelle sezioni seguenti, affrontiamo ogni criterio per la valutazione dei modelli di misurazione riflessivi.

3.5.2 – Affidabilità della coerenza interna

Il primo criterio ad essere valutato è tipicamente quello dell'affidabilità della coerenza interna. Il criterio tradizionale per la coerenza interna è l'Alfa di Cronbach che fornisce una stima dell'affidabilità basata sulle correlazioni delle variabili indicatore osservate. L'Alfa di Cronbach presume che tutti gli indicatori siano ugualmente affidabili (cioè, che tutti gli indicatori hanno carichi esterni uguali sul costrutto). Inoltre, l'Alfa di Cronbach è sensibile al numero di elementi nella scala e tende generalmente a sottovalutare l'affidabilità della coerenza interna. In quanto tale, può essere utilizzato come misura più conservativa dell'affidabilità della coerenza interna. A causa dei limiti dell'Alfa di Cronbach, è tecnicamente più appropriato applicare una misura diversa dell'affidabilità della coerenza interna, che viene definita affidabilità composita. Questa misura di affidabilità tiene conto dei diversi carichi esterni delle variabili indicatore.

L'Alfa di Cronbach è una misura conservativa dell'affidabilità (cioè, si traduce in valori di affidabilità relativamente bassi). Al contrario, l'affidabilità composita tende a sovrastimare l'affidabilità della coerenza interna, determinando così stime di affidabilità relativamente più elevate. Pertanto, è ragionevole considerare e riportare entrambi i criteri. Quando si analizza e si valuta l'affidabilità della coerenza interna delle misure, la vera affidabilità di solito si trova tra l'Alfa di Cronbach (che rappresenta il limite inferiore) e l'affidabilità composita (che rappresenta il limite superiore). Nello specifico, i valori di affidabilità composita e quelli dell'Alfa di Cronbach sono i medesimi. I valori tra 0,70 e 0,90 possono essere considerati soddisfacenti, valori superiori a 0,90 (e decisamente superiori a 0,95) non sono desiderabili perché indicano che tutte le variabili indicatore stanno misurando lo stesso fenomeno e quindi non è probabile che siano una misura valida del costrutto. Infine, i valori di affidabilità composita inferiori a 0,60 indicano una mancanza di affidabilità della coerenza interna. A tal proposito, Churchill, (1979) suggerisce che un valore della Alfa di Cronbach compreso tra 0.60 e 0.70 è accettabile.

Tali risultati dimostrano l'affidabilità del costrutto. Ciò significa che gli elementi di misurazione di ciascuna variabile latente svolgono bene il loro lavoro e non misurano un'altra variabile latente nel modello di ricerca.

Poiché Hair, et al., (2017) sostengono che i caricamenti degli elementi con un Alfa di Cronbach compresa tra 0,40 e 0,70 dovrebbero essere considerati per la cancellazione se solo la

cancellazione può aumentare l'affidabilità composita, sono stati rimossi due valori, AT1 e PC2, in quanto elementi semanticamente ridondanti.

Come mostrato nella tabella, le variabili hanno un valore per l'Alfa di Cronbach superiore a 0.70, La variabile PC ha un valore inferiore e pari a 0.664 e quindi non accettabile. Prendendo in considerazione Churchill, (1979), tale valore risulta comunque accettabile.

Tabella 5 - Affidabilità e validità del costrutto

	Alfa di Cronbach	**rho_A**	**Affidabilità composita**	**Varianza Media Estratta (AVE)**
AT	0.848	0.898	0.928	0.866
CO	0.891	0.927	0.923	0.751
DT	0.941	0.979	0.944	0.591
EM1	0.933	1.000	0.942	0.669
EM2	0.960	1.000	0.945	0.527
IN	0.831	0.848	0.899	0.749
PC	0.664	0.701	0.823	0.615
PI	0.771	0.849	0.840	0.575
PV	0.933	1.033	0.951	0.831
TR	0.948	1.020	0.951	0.620
VL	0.911	0.933	0.938	0.791

Il modello proposto risulta così essere affidabile.

3.5.3 – Validità convergente

La validità convergente misura il grado di correlazione tra due misure dello stesso costrutto. Per valutare la validità convergente dei costrutti riflettenti, i ricercatori considerano i carichi esterni degli indicatori e la varianza media estratta (AVE). Elevati carichi esterni su un costrutto indicano che gli indicatori associati hanno molto in comune, che viene catturato dal costrutto. La dimensione del carico esterno è anche comunemente chiamata affidabilità dell'indicatore.

Una misura comune per stabilire la validità convergente a livello di costrutto è la varianza media estratta (AVE). Questo criterio è definito come il valore medio grande dei carichi al quadrato degli indicatori associati al costrutto (cioè, la somma dei carichi al quadrato divisa

per il numero di indicatori). Pertanto, l'AVE è equivalente alla comunanza di un costrutto. Utilizzando la stessa logica utilizzata con i singoli indicatori, un valore AVE di 0,50 o superiore indica che, in media, il costrutto spiega più della metà della varianza dei suoi indicatori. Al contrario, un AVE inferiore a 0,50 indica che, in media, rimane più varianza nell'errore degli elementi che nella varianza spiegata dal costrutto. L'AVE di ciascun costrutto misurato in modo riflettente dovrebbe essere valutata.

Nel modello proposto, tutte le variabile presentano valori di AVE superiore a 0.5. Esiste, quindi, una buona validità convergente.

3.5.4 – Validità discriminante

La validità discriminante è la misura in cui un costrutto è veramente distinto da altri costrutti sulla base di standard empirici.

Il criterio di Fornell-Larcker è il primo approccio per valutare la validità discriminante. Confronta la radice quadrata dei valori AVE con le correlazioni delle variabili latenti. In particolare, la radice quadrata dell'AVE di ogni costrutto dovrebbe essere maggiore della sua correlazione più alta con qualsiasi altro costrutto. La logica del metodo Fornell-Larcker si basa sull'idea che un costrutto condivide più varianza con i suoi indicatori associati (items della stessa varabile latente) che con qualsiasi altro costrutto (Fornell & Larcker, 1981).

Alternativamente, quando si presentano problemi di validità discriminante, si procede con l'analisi dei cross loadings (carichi incrociati). In particolare, il carico esterno di un indicatore sul costrutto associato dovrebbe essere maggiore di qualsiasi suo carico incrociato (cioè la sua correlazione) su altri costrutti.

In questo caso, il criterio di Fornell-Larcker è più che sufficiente. Nella tabella seguente, i valori sulla diagonale rappresentano la radice quadrata dell'AVE. Per un adeguata validità discriminate, tali valori devono essere maggiori degli elementi fuori dalla diagonale e posizionati nelle righe e nelle colonne corrispondenti (Hulland, 1999). Il test di validità discriminante non rivela alcun problema e, pertanto, non è necessario procedere con l'analisi dei cross loadings.

Tabella 6 - Validità discriminante

	AT	CO	DT	EM1	EM2	IN	PC	PI	PV	TR	VL
AT	**0.931**										
CO	0.145	**0.878**									
DT	-0.127	-0.218	**0.768**								
EM1	0.084	0.209	0.020	**0.818**							
EM2	-0.130	0.018	-0.030	-0.242	**0.726**						
IN	-0.429	-0.292	0.372	0.180	-0.189	**0.866**					
PC	-0.019	-0.041	0.195	-0.073	-0.208	0.159	**0.784**				
PI	0.310	0.202	-0.208	-0.050	0.111	-0.407	-0.218	**0.758**			
PV	0.249	0.276	-0.393	0.008	-0.031	-0.258	-0.263	0.574	**0.912**		
TR	-0.155	-0.241	0.434	-0.071	-0.097	0.339	0.216	-0.252	-0.417	**0.787**	
VL	-0.041	-0.210	0.272	-0.180	-0.200	0.381	0.477	-0.226	-0.306	0.303	**0.889**

Successivamente viene valutato l'indice HTMT (eterotratto-monotratto), ovvero la media di tutte le correlazioni degli indicatori tra costrutti che misurano diversi fenomeni (Henseler, et al., 2015)

I ricercatori devono fare affidamento su una procedura chiamata bootstrap per derivare una distribuzione della statistica HTMT Nel bootstrap, i sottocampioni vengono estratti casualmente (con sostituzione) dal set di dati originale. Ogni sottocampione viene quindi utilizzato per stimare il modello. Questo processo viene ripetuto fino a quando non è stato creato un gran numero di sottocampioni casuali, tipicamente circa 5.000. I parametri stimati dai sottocampioni (in questo caso, la statistica HTMT) vengono utilizzati per derivare errori standard per le stime. Con queste informazioni, è possibile derivare un intervallo di confidenza bootstrap. L'intervallo di confidenza è l'intervallo in cui cadrà il valore reale della popolazione HTMT, assumendo un certo livello di confidenza

In tal senso, viene eseguita la procedura di bootstrapping per calcolare i valori di HTMT e quelli medi (rispettivamente "campione originario" e "media del campione") su 5.000 sottocampioni e un livello di significatività pari a 0.05 (intervallo di confidenza parti a 95%). Le colonne etichettate con 2,5% e 97,5% mostrano i limiti inferiore e superiore dell'intervallo di confidenza al 95% (bootstrap accelerato con correzione delle distorsioni). Le correlazioni etero-tratto (tra indicatori di diverse variabili latenti) dovrebbero essere più piccole delle correlazioni mono-tratto (tra indicatori della stessa variabile), il che significa che il rapporto HTMT dovrebbe essere inferiore a 1.0 (per confermare la validità discriminante). Come si può notare, nessun intervallo di confidenza include il valore 1. La tabella di seguito sintetizza i

risultati dell'indice etero-tratto mono-tratto e, come si può osservare, i criteri di valutazione sono stati soddisfatti, supportando l'affidabilità e la validità delle misure.

Tabella 7 – Indice etero-tratto mono-tratto HTMT

	Campione originario	Media del campione (M)	2,50%	97,50%
CO -> AT	0,171	0,199	0,06	0,413
DT -> AT	0,127	0,186	0,096	0,351
DT -> CO	0,251	0,271	0,127	0,463
EM1 -> AT	0,109	0,171	0,062	0,363
EM1 -> CO	0,268	0,297	0,141	0,491
EM -> DT	0,151	0,214	0,122	0,35
EM2 -> AT	0,234	0,251	0,102	0,465
EM2 -> CO	0,136	0,217	0,098	0,437
EM2 -> DT	0,123	0,204	0,121	0,337
EM2 -> EM1	0,215	0,326	0,123	0,667
IN -> AT	0,506	0,502	0,278	0,692
IN -> CO	0,323	0,333	0,136	0,543
IN -> DT	0,356	0,371	0,197	0,567
IN -> EM1	0,182	0,223	0,09	0,43
IN -> EM2	0,12	0,202	0,097	0,382
PC -> AT	0,102	0,196	0,08	0,363
PC -> CO	0,166	0,254	0,127	0,42
PC -> DT	0,223	0,294	0,154	0,509
PC -> EM1	0,21	0,308	0,189	0,465
PC -> EM2	0,285	0,344	0,21	0,52
PC -> IN	0,217	0,272	0,105	0,517
PI -> AT	0,316	0,343	0,171	0,544
PI -> CO	0,257	0,303	0,146	0,498
PI -> DT	0,223	0,284	0,179	0,42
PI -> EM1	0,147	0,221	0,113	0,368
PI -> EM2	0,221	0,284	0,169	0,435
PI -> IN	0,399	0,455	0,294	0,649
PI -> PC	0,3	0,351	0,185	0,577
PV -> AT	0,239	0,268	0,117	0,467
PV -> CO	0,326	0,332	0,151	0,517
PV -> DT	0,395	0,396	0,22	0,577
PV -> EM1	0,101	0,164	0,083	0,284
PV -> EM2	0,1	0,174	0,093	0,308
PV -> IN	0,295	0,3	0,087	0,549
PV -> PC	0,326	0,348	0,118	0,605
PV -> PI	0,669	0,666	0,478	0,817
TR -> AT	0,121	0,184	0,086	0,354
TR -> CO	0,263	0,289	0,142	0,457

TR -> DT	0,485	0,487	0,297	0,67
TR -> EM1	0,142	0,205	0,112	0,336
TR -> EM2	0,149	0,21	0,117	0,334
TR -> IN	0,376	0,384	0,207	0,571
TR -> PC	0,27	0,322	0,176	0,518
TR -> PI	0,249	0,3	0,169	0,466
TR -> PV	0,424	0,423	0,247	0,588
VL -> AT	0,085	0,164	0,065	0,361
VL -> CO	0,234	0,24	0,092	0,42
VL -> DT	0,248	0,287	0,135	0,515
VL -> EM1	0,207	0,225	0,085	0,442
VL -> EM2	0,179	0,236	0,12	0,420
VL -> IN	0,425	0,444	0,177	0,713
VL -> PC	0,61	0,611	0,345	0,846
VL -> PI	0,285	0,318	0,125	0,567
VL -> PV	0,335	0,347	0,105	0,602
VL -> TR	0,332	0,349	0,137	0,567

3.5.5 – Dimensioni e significatività del coefficiente di percorso del modello interno

La misura più comunemente utilizzata per valutare il modello strutturale è il coefficiente di determinazione (valore R^2). Questo coefficiente è una misura del potere predittivo del modello ed è calcolato come correlazione al quadrato tra i valori effettivi e previsti di uno specifico costrutto endogeno. Il coefficiente rappresenta gli effetti combinati delle variabili latenti esogene sulla variabile latente endogena. In altre parole, il coefficiente rappresenta la quantità di varianza nei costrutti endogeni spiegata da tutti i costrutti esogeni ad esso collegati. Poiché R^2 è la correlazione al quadrato dei valori effettivi e previsti e, come tale, include tutti i dati che sono stati utilizzati per la stima del modello per giudicare il potere predittivo del modello, rappresenta una misura del potere predittivo nel campione, ovvero una variabile descrive la variabile che influenza (Rigdon, 2012) (Sarstedt, et al., 2014).

Il valore R^2 varia da 0 a 1, con livelli più alti che indicano livelli più alti di accuratezza predittiva. Perché i valori R^2 siano accettabile dipende dalla complessità del modello e dalla disciplina di ricerca. Valori di R^2 intorno a 0,20 sono considerati alti in discipline, come in questo caso, in cui si analizza il comportamento dei consumatori. Negli studi sui fattori di successo (ad esempio, negli studi che mirano a spiegare la soddisfazione o la fedeltà del

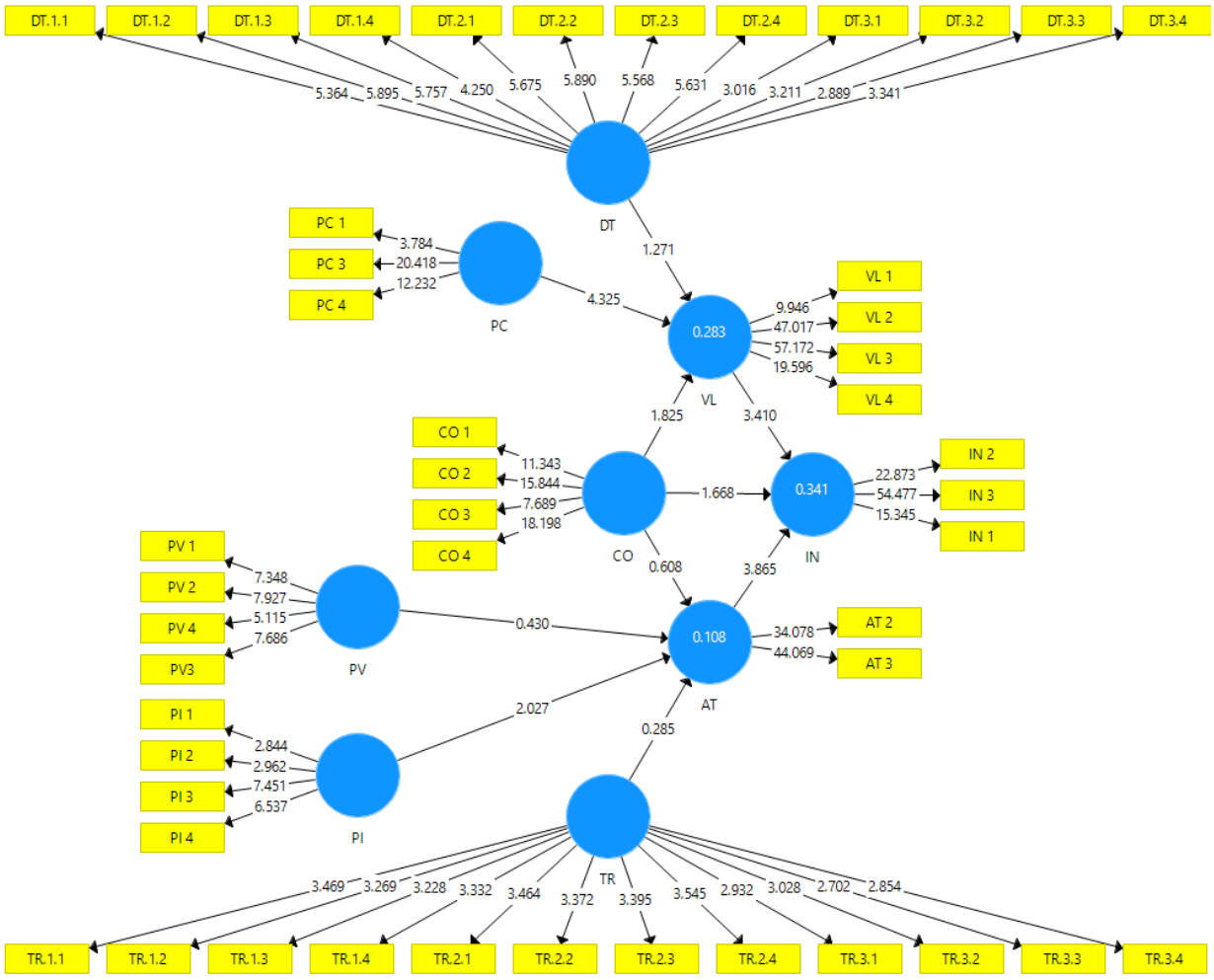
cliente), i ricercatori si aspettano valori molto più alti, come 0,75 e oltre. Nella ricerca accademica che si concentra su questioni di marketing, i valori R^2 di 0,75, 0,50 o 0,25 per le variabili latenti endogene possono, come regola pratica, essere rispettivamente descritti come sostanziali, moderati o deboli (Hair, et al., 2011) (Henseler, et al., 2009)

Dopo aver eseguito l'algoritmo PLS-SEM e aver effettuato il bootstrap su 5000 sottocampioni con un livello di significatività pari a 0.05 si ottengono stime per le relazioni del modello strutturale (cioè i coefficienti di percorso), che rappresentano le relazioni ipotizzate tra i costrutti. I coefficienti di percorso hanno valori standardizzati approssimativamente tra –1 e +1. Valori vicini a questi due estremi sono statisticamente significativi (cioè, diversi da zero nella popolazione). Al contrario, valori intorno allo 0 sono statisticamente non significativi. La significatività, quindi, è data dal suo errore standard. L'errore standard calcolato tramite la procedura di bootstrapping consente di calcolare i t-value e i p-value per tutti i coefficienti del percorso strutturale. Quando il t-value è maggiore del valore critico, concludiamo che il coefficiente è statisticamente significativo a una certa probabilità di errore (cioè, livello di significatività). I valori critici comunemente usati per i test a due code sono 1,65 (livello di significatività = 10%), 1,96 (livello di significatività = 5%) e 2,57 (livello di significatività = 1%).

Ritornando al campione analizzato, il coefficiente R^2 è 0.106 per la variabile endogena latente AT, 0.451 per IN e 0.261 per VL. Ciò vuol dire che le altre variabili spiegano AT per 10,6 % (PV, PI, TR), che DT e PC spiegano VL al 26,1% e che IN è spiegata al 45,1% da CO, VL e AT. Come detto, valori intorno allo 0.2 sono più che accettabili se si tratta di analizzare variabili comportamentali e, in questo caso, VL e IN sono più che ottimi.

Per quanto riguarda la significatività, invece, viene utilizzato il valore critico 1.96 pari al 5% di livello di significatività: t-value al di sotto di questa soglia sono da considerarsi statisticamente non significativi. Come da modello sottostante, gli effetti diretti rendono:

Figura 2 - Coefficienti di percorso



- L'ipotesi sulla relazione PC -> VL è statisticamente significativa (t-value = 4.122 > 1.96);
- L'ipotesi sulla relazione AT -> IN è statisticamente significativa (t-value = 4.507 > 1.96);
- L'ipotesi sulla relazione VL -> IN è statisticamente significativa (t-value = 3.987 > 1.96);
- L'ipotesi sulla relazione PI -> AT è statisticamente significativa (t-value = 2.133 > 1.96);
- L'ipotesi sulla relazione CO -> IN è statisticamente è significativa (t-value = 2.470 > 1.96);
- L'ipotesi sulla relazione DT -> VL è statisticamente non significativa (t-value = 1.532 > 1.96);
- L'ipotesi sulla relazione PV -> AT è statisticamente non significativa (t-value = 0.551 <1.96);

- L'ipotesi sulla relazione TR -> AT è statisticamente non significativa (t-value = 0.343 <1.96):

La relazione più significativa è quella di AT su IN. Valide anche CO e VL che influenzano la variabile dipendente IN. AT e VL sono forti predittori di IN, così come PC lo è per VL. PI risulta essere predittore della variabile AT.

3.5.6 – Test di ipotesi

Sulla base dei risultati appena descritti, il modello di misurazione ha una buona affidabilità dei singoli articoli, validità convergente e validità discriminante. Le variabili latenti rientrano nel livello di errore accettabile. Il modello di misurazione, pertanto, dimostra una robustezza sufficiente necessaria per testare la relazione tra le variabili latenti e la variabile dipendente. Il modello viene successivamente valutato per determinarne il potere esplicativo e per testare le ipotesi di ricerca.

In questo studio, il SEM viene utilizzato per misurare gli effetti delle variabili indipendenti sulle variabili dipendenti. Gli effetti diretti sono indicati come un percorso dalla variabile esogena a quella endogena controllando i mediatori. L'effetto indiretto è un percorso dalla variabile esogena a quella endogena attraverso una variabile mediatore. La somma di questi effetti diretti e indiretti compone l'effetto totale (Imai, et al., 2010).

Sem è stato utilizzato per valutare le ipotesi di questo studio. Nella tabella di seguito sono mostrati gli effetti diretti, indiretti e totali standardizzati e i t-values delle variabili del modello. L'approccio di bootstrap con 5000 campioni è stato utilizzato per testare gli effetti indiretti.

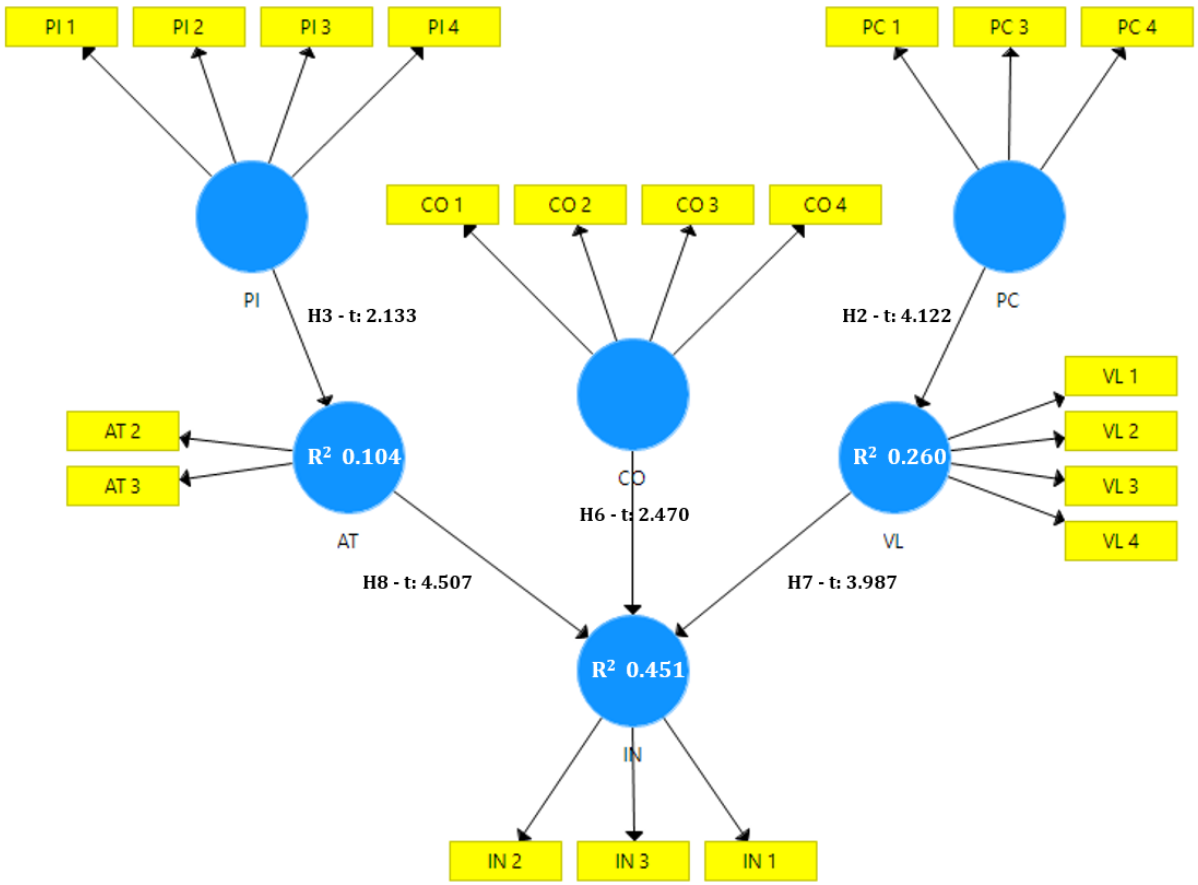
Tabella 8 – Effetti Totali

	Campione originario (O)	**Media del campione (M)**	**Deviazione standard (DEVST)**	**T statistics (|O/DEVST|)**	**P values**	
AT -> IN	**-0.421**	**-0.374**	**0.093**	***4.507***	***0,000***	**Effetti Diretti**
CO -> IN	**-0.218**	**-0.216**	**0.088**	***2.470***	***0.014***	**Effetti Diretti**
DT -> IN	0.066	0.085	0.055	1.208	0.227	Totale effetti indiretti
DT -> VL	0.186	0.213	0.121	1.532	0.126	Effetti Diretti
EM1 -> IN	**0.266**	**0.233**	**0.125**	**2.127**	**0.033**	**Effetti Diretti**
EM2 -> IN	-0.092	-0.094	0.188	0.488	0.625	Effetti Diretti

PC -> IN	**0.156**	**0.164**	**0.053**	***2.934***	***0.003***	**Totale Effetti Indiretti**
PC -> VL	**0.440**	**0.436**	**0.107**	***4.122***	***0.000***	**Effetti Diretti**
PI -> AT	**0.248**	**0.270**	**0.116**	***2.133***	***0.033***	**Effetti Diretti**
PI > IN	-0.104	-0.104	0.056	1.853	0.064	Totale effetti indiretti
PV -> AT	0.078	0.076	0.141	0.551	0.581	Effetti Diretti
PV -> IN	-0.033	-0.026	0.053	0.614	0.539	Totale effetti indiretti
TR -> AT	-0.058	-0.065	0.690	0.343	0.731	Effetti Diretti
TR -> IN	0.024	0.027	0.063	0.389	0.698	Totale effetti indiretti
VL -> IN	**0.354**	**0.379**	**0.089**	***3.987***	***0.000***	**Effetti Diretti**

Secondo la tabella ci sono cinque percorsi significativi quando si considerano gli effetti diretti e uno quando si considerano gli effetti specifici indiretti. I valori di t mostrano il significato di questi percorsi. Tali effetti significativi sono tra le variabili AT e IN, CO e IN, PC e VL, PI e AT, VL e IN e PC e IN passando per VL.

Figura 3- Modello ipotizzato e coefficienti di percorso



Ipotesi 1: "Trasparenza nell'utilizzo dei dati (DT) influenza negativamente il sentimento di vulnerabilità (VL)" non è stata confermata dall'analisi dei risultati. DT non risulta un predittore significativo per il sentimento di vulnerabilità (t-value = 1.532)

Ipotesi 2: "Controllo delle informazioni relativamente alla privacy (PC) influenza negativamente il sentimento di vulnerabilità (VL)" è stata confermata dall'analisi dei risultati. PC risulta un predittore significativo per il sentimento di vulnerabilità (t-value = 4.122)

Ipotesi 3: "Importanza della privacy (PI) influenza positivamente l'atteggiamento nel rilasciare le informazioni personali online (AT)" è stata confermata dall'analisi dei risultati. PI risulta un predittore significativo per l'atteggiamento nel rilasciare le informazioni personali online (t-value = 2.133)

Ipotesi 4: "Affidabilità (TR) influenza negativamente l'atteggiamento nel rilasciare le informazioni personali online (AT)" non è stata confermata dall'analisi dei risultati. TR non risulta un predittore significativo per l'atteggiamento nel rilasciare le informazioni personali online (t-value = 0.343)

Ipotesi 5: "Violazioni della privacy (PV) influenzano negativamente l'atteggiamento nel rilasciare le informazioni personali online (AT)" non è stata confermata dall'analisi dei risultati. PV non risulta un predittore significativo per l'atteggiamento nel rilasciare le informazioni personali online (t-value = 0.551)

Ipotesi 6: "Ottimismo comparativo (CO) influenza negativamente le intenzioni nel rilasciare informazioni personali online (IN)" è stata confermata dall'analisi dei risultati. CO risulta un predittore significativo per le intenzioni nel rilasciare informazioni personali online (t-value = 2.470)

Ipotesi 7: "Vulnerabilità (VL) influenza positivamente le intenzioni nel rilasciare informazioni personali online (IN)" è stata confermata dall'analisi dei risultati. VL risulta un predittore significativo per le intenzioni nel rilasciare informazioni personali online (t-value = 3.987)

Ipotesi 8: "Atteggiamento nel rilasciare informazioni personali online (AT) influenza negativamente le intenzioni nel rilasciare informazioni personali online (IN)" è stata confermata dall'analisi dei risultati (t-value = 4.507)

Ipotesi 9: "Ottimismo comparativo (CO) funge da moderatore nella relazione AT -> IN" è stata confermata dall'analisi dei risultati (t-value = 2.127).

Ipotesi 9a: "Ottimismo comparativo (CO) funge da moderatore nella relazione VL -> IN" non è stata confermata dall'analisi dei risultati (t-value = 0.488)

Tabella 9- Risultato delle ipotesi

IPOTESI	SUPPORTATA	NON SUPPORTATA
Ipotesi 1: la trasparenza nell'utilizzo dei dati (DT) influenza negativamente il sentimento di vulnerabilità (VL)		X
Ipotesi 2: il controllo delle informazioni relativamente alla privacy (PC) influenza negativamente il sentimento di vulnerabilità (VL)	X	
Ipotesi 3: l'importanza della privacy (PI) influenza positivamente l'atteggiamento nel rilasciare le informazioni personali online (AT)	X	
Ipotesi 4: l'affidabilità (TR) influenza negativamente l'atteggiamento nel rilasciare le informazioni personali online (AT)		X
Ipotesi 5: le violazioni della privacy (PV) influenzano negativamente l'atteggiamento nel rilasciare le informazioni personali online (AT)		X
Ipotesi 6: l'ottimismo comparativo (CO) influenza negativamente le intenzioni nel rilasciare informazioni personali online (IN)	X	
Ipotesi 7: la vulnerabilità (VL) influenza positivamente le intenzioni nel rilasciare informazioni personali online (IN)	X	
Ipotesi 8: l'atteggiamento nel rilasciare informazioni personali online (AT) influenza negativamente le intenzioni nel rilasciare informazioni personali online (IN)	X	
Ipotesi 9: "Ottimismo comparativo (CO) funge da moderatore nella relazione AT -> IN"	X	
Ipotesi 9a: "Ottimismo comparativo (CO) funge da moderatore nella relazione VL -> IN"		X

3.5.7 – Analisi dei fattori moderatori

Come introdotto nello sviluppo delle ipotesi, l'analisi dei moderatori viene effettuata sulla base di una domanda posta a priori dal ricercatore. L'obiettivo è quello di valutare il ruolo moderatore della variabile CO. Le ipotesi hanno cercato di accertare il ruolo moderatore della variabile CO nelle relazioni tra le variabili indipendenti AT e VL e la variabile dipendente IN, ovvero tra AT-> IN e VL -> IN.

L'analisi dei fattori moderatori viene svolta con l'approccio dell'indicatore di prodotto. È l'approccio standard per creare il termine di interazione nelle analisi basate sulla regressione. L'approccio dell'indicatore di prodotto prevede la moltiplicazione di ogni indicatore della variabile latente esogena con ogni indicatore della variabile moderatore (Chin, et al., 2003).

Ci sono altri due approcci, "ortogonalizzante" e de "i due stadi", spiegati brevemente di seguito. Il primo è un'estensione dell'approccio dell'indicatore di prodotto e viene utilizzato per affrontare i costrutti quando le variabili utilizzate nell'approccio dell'indicatore di prodotto devono essere standardizzate (Little, et al., 2006). Il secondo, quello dei due stadi, viene proposto da Chin, et al., (2003) come mezzo per eseguire un'analisi di moderazione quando il costrutto esogeno e / o il moderatore vengono misurati in modo formattato.

Proseguendo, i risultati (tabella 8 – effetti totali) rivelano un ruolo moderatore statisticamente non significativo di CO nella relazione tra VL e IN (B = 0.092, t = 0.478, p = 0.632). CO si è rivelato avere un ruolo moderatore statisticamente significativo nella relazione tra AT e IN (B = 0.266, t = 2.127, p = 0.037)

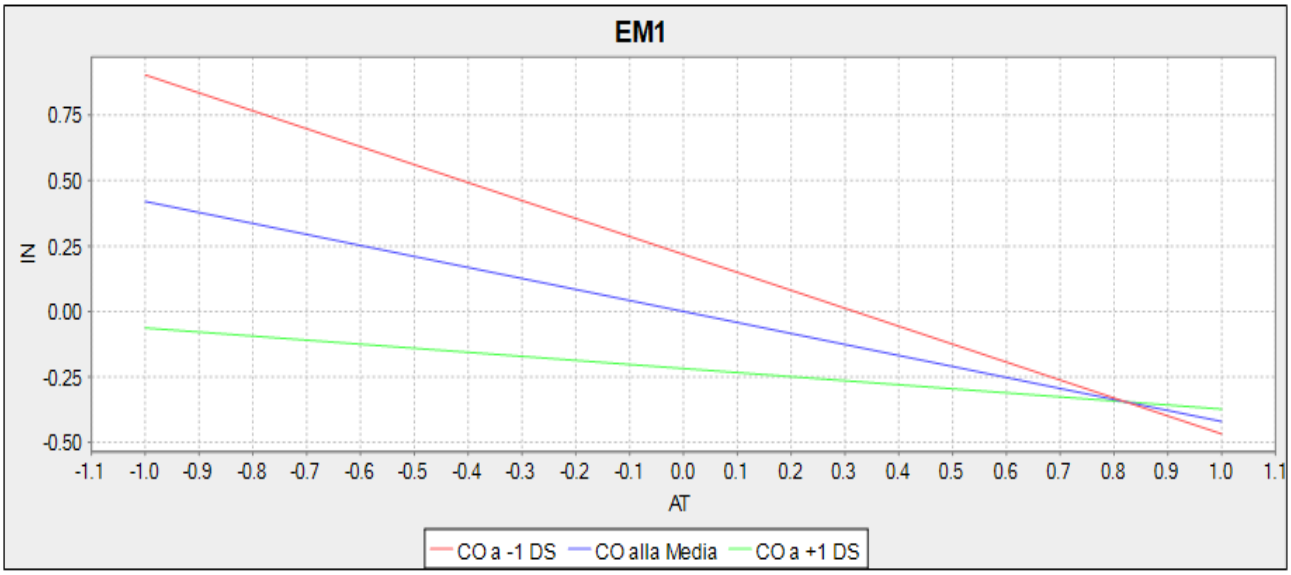
Si procede con l'analisi del moderatore CO per quanto riguarda la relazione AT -> IN. Di seguito, un riepilogo dei valori dei coefficienti di percorso:

	Campione originario (O)	Media del campione (M)	Deviazione standard (DEVST)	T statistics (|O/DEVST|)	P values
AT -> IN	**-0.421**	**-0.374**	**0.093**	***4.507***	***0,000***

Si evince come la relazione tra AT e IN sia negativa (-0.421) e, pertanto, a valori alti di AT corrispondono bassi valori di IN. Il moderatore non fa altro che rafforzare questa relazione. Di seguito viene effettuata un'analisi semplice della pendenza.

Un modo comune per illustrare i risultati di un'analisi di moderazione è mediante grafici di pendenza. L'asse x rappresenta il costrutto esogeno (AT) e l'asse y il costrutto endogeno (IN). Le linee rappresentano la relazione tra AT e IN per i livelli basso (rosso), alto (verde) e medi (blu) del costrutto moderatore CO.

Figura 4 – Grafico della pendenza del moderatore



È possibile analizzare la pendenza dell'effetto moderatore in maggiore dettaglio. La linea rossa che rappresenta un livello basso del costrutto moderatore CO ha una pendenza più ripida mentre la linea inferiore, che rappresenta un livello alto del costrutto moderatore CO, ha una pendenza meno ripida. Come regola pratica e approssimativa, la pendenza del livello alto del costrutto moderatore CO è l'effetto semplice (cioè 2.456) più l'effetto di interazione (+2.086), mentre la pendenza del livello basso del costrutto moderatore CO è l'effetto semplice (cioè 2.456) meno l'effetto di interazione (−2.086).

Quindi, il semplice grafico della pendenza supporta la precedente discussione sul termine di interazione negativa: livelli di Ottimismo Comparativo superiori comportano una relazione più debole tra Atteggiamento e Intenzioni, mentre livelli inferiori di Ottimismo Comparativo

portano a una relazione più forte tra Atteggiamento e Intenzioni. In altre parole, a bassi livelli di Ottimismo Comparativo c'è un impatto maggiore della variabile Atteggiamento dove per livelli alti di Atteggiamento corrispondono alti livelli di Intenzioni (linea rossa). Tuttavia, l'aumento di Ottimismo Comparativo smorza, anche se di poco, la relazione tra Atteggiamento e Intenzioni dove ad alti livelli di Atteggiamento corrispondono livelli inferiori di Intenzioni.

3.6 – RISULTATI

Lo studio è stato condotto per indagare le intenzioni degli individui a rilasciare le proprie informazioni personali online. La tipologia di informazioni online e i metodi di raccolta dati online sono stati spiegati precedentemente nell'analisi della letteratura. In questa sezione verranno discussi nel dettaglio i risultati dell'analisi del modello di ricerca che dimostrano i comportamenti online adottati dagli individui quando si tratta della loro privacy e delle loro informazioni personali online.

Secondo i risultati del modello di misurazione, si è riscontrato come il sentimento di vulnerabilità (VL) sia influenzato negativamente dall'attenzione, dal controllo, che gli individui hanno sulla loro privacy, sui dati e le informazioni che rilasciano e condividono online (PC). D'altra parte, la trasparenza dei dati (DT) è risultata insignificante quando sono stati analizzati i suoi effetti diretti sul sentimento di vulnerabilità (VL). In letteratura si è visto come queste variabili influenzino negativamente la vulnerabilità quando si tratta della condivisione della proprie informazioni online (Martin, et al., 2017). In questo studio condotto su un campione limitato di individui che passa buona parte della loro quotidianità online non per motivi professionali, sorprendentemente, una variabile (DT) è risultata insignificante sul sentimento di vulnerabilità. Tuttavia, una questione da considerare è che questa variabile non dipende direttamente dagli individui ma dalle organizzazioni, siti, enti che si occupano di rendere trasparenti la gestione delle informazioni. Le politiche di trasparenza sulla raccolta e l'uso dei dati online non sono riconducibili agli individui che non possono deciderle direttamente e che risultano, pertanto, attori passivi.

I risultati hanno indicato che, al contrario, il controllo che gli individui possono esercitare sulle proprie informazioni influenza negativamente il sentimento di vulnerabilità. Ciò significa che a un maggiore controllo sulla diffusione delle proprie informazioni personali online è corrisposto un minor sentimento di vulnerabilità, un rischio minore che i propri dati vengano

usati e raccolti in maniere illecite e diverse da quelle dichiarate (Baek, et al., 2014). Laddove, infatti, gli individui riescono a controllare cosa succede alle loro informazioni personali, quanto un'entità può utilizzarle e come queste vengono condivise, la percezione che questi dati possano essere usati in modo non appropriato viene meno. Al contrario, se il controllo diminuisce gli individui sono meno propensi a rilasciare i propri dati.

La vulnerabilità, quindi, risulta un fattore importante per quanto riguarda le intenzioni effettive di un individuo nel rilasciare le proprie informazioni personali online. In generale, ci si aspetta che per un persona, maggiore sia la paura che un'azione possa avere conseguenze negative, minori siano le intenzioni nel proseguire con tale azione. Ed è quello che risulta dall'analisi del modello. A valori alti di vulnerabilità sono corrisposti bassi valori circa le intenzioni delle persone. Questo è in linea con la letteratura: maggiore è la paura che le informazioni personali che un utente lascia (volontariamente) o rilascia (involontariamente, *little data*) possano essere usate nella maniera sbagliata, minore allora sarà la volontà a rilasciarle (Martin, et al., 2017). Tuttavia, le abitudini riguardo l'utilizzo di Internet non lasciano poi tanta scelta: per poter navigare online è indispensabile che qualche traccia del proprio passaggio venga lasciata, consciamente o inconsciamente. Ed è qui, pertanto, che gli individui possono limitare la quantità di informazioni condivise per sentirsi più protetti. Come è risultato dall'analisi, le persone in media si sentono al sicuro riguardo le proprie informazioni personali proprio in virtù del fatto che tali informazioni non sono complete e si limitano all'essenziale. Ed è per questo che è possibile utilizzare la teoria del gossip per valutare come le persone rispondono all'accesso e all'uso indesiderato delle informazioni da parte di terzi, quando ne vengono a conoscenza. Quando il gossip diventa saliente, produce una serie di risposte emotive e cognitive negative dal target verso la fonte, quindi dall'individuo all'azienda, per esempio (Baumeister, et al., 2004). Per evitare che ciò accada, l'individuo tara e sceglie con cura quali informazioni divulgare e quali invece tenere private.

La privacy, di per sé, è vista come uno dei fattori più importanti per determinare la propensione di un individuo a rilasciare le proprie informazioni personali online. Il valore che gli individui danno alla privacy online è molto importante. I risultati dell'analisi del modello spiegano come si ponga questo fattore rispetto al sentimento di fiducia nelle organizzazioni e a quello di non sentirsi al sicuro, il quale impatta significativamente sulla propensione degli individui a rilasciare le proprie informazioni personali online. La letteratura spiega come, in verità, sia la componente fiduciaria a influenzare maggiormente l'atteggiamento (Wu, et al., 2012). Tuttavia, la variabile in questione, nello studio effettuato, non è risultata essere

significativa da un punto di vista statistico. D'altro canto, è anche corretto specificare come nella vita quotidiana le persone tendono ad avere una scarsa fiducia verso chi possiede e gestisce i loro dati (Leary & Leder, 2009).

Parallelamente, come si evince dall'analisi, a influenzare l'atteggiamento sono la sensibilità dei propri dati e l'importanza di evitare il più possibile eventuali minacce o eventi che minano la sicurezza della privacy. La privacy, di per sé stessa, deve rimanere intatta. La letteratura sostiene che le persone hanno un senso già sviluppato di quanto poco ci si possa fidare dei soggetti che raccolgono i dati (Leary & Leder, 2009) e stabilisce come una maggiore attenzione e sensibilità alla privacy si traduca in comportamenti preventivi volti a proteggere e a tutelare i propri dati. Maggiori sono le attenzioni che gli individui rivolgono alle questioni relative alla privacy, più prudenti saranno i comportamenti online e si avrà, in generale, un atteggiamento tutto sommato benevolo e non ostile nel rilasciare le proprie informazioni personali online. Pertanto, come risultato dall'analisi del modello, gli individui che ritengono la privacy molto importante e sono sensibili ai loro dati e alle loro informazioni presenti online sono altresì i più disposti a condividere tali informazioni in quanto adottano dei comportamenti di tutela contro spiacevoli avvenimenti. Tali comportamenti sono relativamente facili da adottare e non richiedono una grande conoscenza dei sistemi informatici. Infatti, un esperimento condotto da Chen, et al., (2017) ha rivelato come tra i comportamenti più frequenti spiccano l'installazione di programmi di antivirus o maggiori cambi di password rispetto ad altri utenti, compiti relativamente semplici da effettuare. Tali individui si sentono più protetti e sono quindi più tranquilli a navigare online.

Le violazioni della privacy non sembrano influenzare in alcun modo l'atteggiamento. L'ipotesi iniziale faceva riferimento ai comportamenti degli individui in seguito ad eventi spiacevoli come la fuga dei dati o l' uso improprio delle informazioni personali presenti online e come questi potessero impattare negativamente sui comportamenti futuri. Tuttavia, tale risultato potrebbe andare di pari passo con l'esigenza costante di utilizzare internet e navigare online, nonostante spiacevoli eventi che gli individui, talvolta, si vedono costretti ad affrontare.

Ecco perché anche l'atteggiamento, oltre al sentimento di vulnerabilità, influenza le intenzioni nel rilasciare le proprie informazioni personali online. I comportamenti tutelativi adottati portano anche ad atteggiamenti e abitudini di carattere preventivo. L'analisi ha mostrato come gli atteggiamenti influenzino negativamente le intenzioni a condividere i propri dati, Dai risultati si evince che le informazioni fornite sovente differiscono dalla realtà: le persone sono

più predisposte, se ne hanno l'occasione, a fornire informazioni non del tutto corrette che possono risultare fuorvianti. In questo caso, le persone che tendono a non fornire informazioni corrette sono le stesse che continueranno a rilasciare le proprie informazioni personali online.

Anche l'ottimismo comparativo (CO) è risultato influenzare negativamente le intenzioni di condivisione dei propri dati online. Un individuo ottimista ritiene che, rispetto ad altri, difficilmente possa incorrere in spiacevoli episodi e che tali episodi siano sempre distanti da lui. Infatti, le persone che credono di avere maggiori probabilità di avere un'esperienza negativa in termini di privacy rispetto ad altri sono le stesse che faticano o limitano drasticamente la qualità e la quantità di informazioni personali che inseriscono volontariamente online. Poiché alla domanda " Ho maggiori probabilità di avere un'esperienza negativa sulla privacy rispetto agli altri utenti a seguito dell'utilizzo di…" le risposte ricevute sono state per valori al di sotto della media, è possibile affermare che le persone tendenzialmente sono più ottimiste che pessimiste.

L'ottimismo comparativo è stato inserito, però, per verificare l'effetto che tale variabile potesse avere come moderatore sia sul sentimento di vulnerabilità sia anche sull'atteggiamento degli individui nel rilasciare le informazioni personali online. Statisticamente, è risultata significativa solo la relazione di moderazione tra Atteggiamento e Intenzioni e, sorprendentemente, non quella tra Vulnerabilità e Intenzioni. Essendo la relazione tra Ottimismo Comparativo e Intenzioni negativa, dall'analisi dei fattori moderatori è emerso come a bassi valori di CO la variabile Atteggiamento impatti maggiormente sulla variabile Intenzioni. Ciò vuol dire che le persone relativamente ottimiste sono più predisposte a rilasciare informazioni personali online e che, al contempo, sono anche quelle che continueranno a farlo in futuro.
Sarebbe stato interessante vedere come l'ottimismo avrebbe potuto influenzato la Vulnerabilità. Infatti, presumibilmente, avrebbe rafforzato la relazione positiva tra Vulnerabilità e Intenzioni e per la quale, una persona ottimista, dovrebbe sentirsi meno esposta, meno a rischio, e pertanto, maggiormente intenzionata a rilasciare le proprie informazioni online. Purtroppo, non è possibile affermare o smentire questa ipotesi poiché la relazioni di moderazione è risultata statisticamente non significativa, forse a causa di un campionamento ridotto.

La vulnerabilità non sembra essere influenzata da fattori di ottimismo, forse perché sono entrambe due variabili che mirano ad analizzare la stessa cosa: un sentimento che, seppur diverso,

Nonostante la poca fiducia in generale verso chi raccoglie e gestisce i dati personali online e nonostante la scarsa trasparenza e la paura su come tali informazioni possano venire utilizzate è inevitabile che l'individuo continuerà a navigare online durante la sua quotidianità, non solamente per motivi professionali. Le persone passano molte ore sul web condividendo i propri dati e cercando informazioni di ogni genere. Per sopperire ai molti lati negativi, gli utenti adottano dei comportamenti di tutela e di salvaguardia della privacy per sentirsi più protetti e per continuare a navigare online.

3.6.1 – Conseguenze dell'effetto moderatore

Il ruolo di comportamenti ottimistici nella privacy online è stato suggerito per la prima volta da (Acquisti & Grossklags, 2005). Xu, (2012) ha anche ipotizzato che gli utenti di SNS (Social Network Sites) potrebbero credere di essere meno suscettibili ai rischi per la privacy rispetto ai loro coetanei. Ad oggi esistono pochi studi che hanno indagato empiricamente i comportamenti ottimistici degli utenti in relazione ai loro rischi per la privacy online (Baek, et al., 2014) (Campbell, et al., 2007) (Cho, et al., 2010) (Debatin, et al., 2009) (Li, 2008) (Kim & Hancock, 2015).

I risultati riguardo l'ottimismo comparativo, come già accennato, sono stati sorprendenti.
La letteratura suggerisce che il livello di ottimismo comparativo è correlato negativamente ai soggetti che credono di poter incorrere in spiacevoli episodi. Si può affermare che la vulnerabilità è strettamente legata alle azioni che gli individui non possono intraprendere e che, di conseguenza, subiscono. Tuttavia, se analizzato nella sua utilità di moderatore, CO non è risultato significativo nella relazione tra la vulnerabilità e le intenzioni nel rilasciare le proprie informazioni personali online. È possibile condurre ulteriori ricerche per indagare il motivo alla base di questa contraddizione. Inoltre, è possibile che durante la sua applicazione ci siano alcuni fattori che non sono stati considerati nel modello e potrebbero dover essere adeguati a produrre un modello più accurato ed efficace.

Come anticipato nell'analisi del modello proposto, l'ottimismo è stato associato in diversi studi ai Big Five dei tratti della personalità. In particolare, gli studi si sono concentrati nella relazione con il nevroticismo e l'estroversione (Boland & Cappeliez, 1997) (Marshall, et al., 1992). Tuttavia, uno studio condotto da (Sharpe, et al., 2011) ha rivelato come l'ottimismo sia fortemente correlato anche ad altri due fattori: coscienziosità e piacevolezza. Gli autori hanno sviluppato tre principali percorsi concettuali per aiutare a descrivere le relazioni tra l'ottimismo e i Big Five:

1. Percorso affettivo: coinvolge sia l'affettività negativa inerente al fattore Nevroticismo, sia gli aspetti affettivi positivi del fattore Estroversione. Questo è un percorso evidente nelle concettualizzazioni teoriche dell'ottimismo (Peterson, 2000) (Scheier & Carver, 1992) e già fortemente supportato nella letteratura di ricerca (Boland & Cappeliez, 1997) (Marshall, et al., 1992)
2. Percorso sociale: coinvolge gli aspetti dell'urgenza dell'estroversione e il fattore della piacevolezza. Ricerche passate supportano l'idea che gli ottimisti siano più socialmente abili, amichevoli e dimostrino livelli più elevati di soddisfazione con le relazioni intime, ma questo in genere è stato studiato come risultato di ottimismo piuttosto che da una prospettiva dei tratti (Peterson & Vaidya, 2003) (Srivastava, et al., 2006)
3. Percorso della persistenza: coinvolge il fattore di personalità Coscienziosità. Questo percorso è forse meno intuitivo degli altri due percorsi, ma ha un supporto specifico nella letteratura che mostra che gli ottimisti non solo credono che sperimenteranno risultati positivi nella vita, ma mantengono anche un vigoroso perseguimento degli obiettivi per garantire risultati positivi (Carver & Scheier, 1993) (Segerstrom, et al., 2003)

Il modello a tre percorsi così proposto aiuta a descrivere i profili dei tratti della personalità di base degli individui ottimisti e pessimisti

Sulla base dei risultati ottenuti e della letteratura analizzata, l'ottimista tende ad avere un profilo di personalità di base caratterizzato da un'elevata stabilità emotiva, estroversione, gradevolezza e coscienziosità (Sharpe, et al., 2011) (Srivastava, et al., 2006) . Questo profilo di personalità porta allo sviluppo di convinzioni ottimistiche e, quindi, a una visione del mondo complessivamente positiva con conseguente tendenza verso una migliore salute mentale/fisica e un comportamento capace di adattarsi ad ogni situazione (Carver, et al., 2010). Lungo il percorso affettivo, una maggiore affettività positiva e una minore affettività

negativa tendono a portare a una visione ottimistica del mondo. Una maggiore urgenza e una natura gradevole tendono a portare all'ottimismo lungo il percorso sociale. Nel percorso della persistenza, livelli più elevati di coscienziosità/persistenza si traducono in una visione del mondo più positiva per l'ottimista. Il pessimista, d'altra parte, ha un profilo di tratto caratterizzato da bassa stabilità emotiva (cioè nevroticismo), estroversione, gradevolezza e coscienziosità con relazioni lungo i tre percorsi che lavorano in direzioni opposte a quella dell'ottimista. Questo profilo di personalità porta allo sviluppo di convinzioni pessimistiche e una visione del mondo negativa con conseguente tendenza verso problemi di salute mentale / fisica e comportamenti disadattivi (Peterson & Vaidya, 2003).

Inoltre, l'ottimismo comparativo trova spazio, secondo la letteratura, anche nel campo della percezione del rischio circa la privacy online da parte degli individui. Secondo (Metzger & Suh, 2017), l'ottimismo comparativo è il concetto migliore per esaminare la percezione del rischio degli individui in quanto "non è possibile avere una misura obiettiva ed oggettiva dei rischi riguardo la privacy online" (Baek, et al., 2014). Negli studi di Metzger & Suh, (2017) si evince come le persone siano fermamente convinte del fatto che, se comparate ad altre persone, il loro rischio di incorrere in eventi spiacevoli circa la loro privacy online è inferiore. Inoltre, sempre gli stessi studi rivelano come chi fa un utilizzo assiduo di Internet è, paradossalemente, meno preoccupato e più ottimista riguardo alle minacce sulla privacy online (Campbell, et al., 2007). Questo è in linea con i risultati della ricerca. Le persone, più tempo passano online, più sono convinte di non incorrere in situazioni rischiose e continuano, pertanto, a navigare e condividere i propri dati. In letteratura, la percezione del rischio viene associata alla vulnerabilità (Acquisti, et al., 2015). Per quanto la variabile Ottimismo Comparativo come moderatore tra Vulnerabilità e Intenzioni, come già detto, non sia risultata statisticamente significativa, in letteratura trova comunque un vasto campo di argomenti a favore. A un maggior controllo sulle proprie informazioni online corrisponde un minor sentimento di vulnerabilità e, quindi, un minor rischio percepito. Infatti, controllo e rischio percepito sono correlati negativamente (Metzger & Suh, 2017). Pertanto, sarebbe possibile affermare come anche l'ottimismo possa rafforzare la relazione tra Vulnerabilità e Intenzioni e, quindi, le persone ottimiste che hanno una minore percezione del rischio e si sentono di conseguenza meno vulnerabili sono anche quelle che possono continuare a condividere le proprie informazioni personali online.

Sulla base della letteratura analizzata, la presente ricerca porta alla conclusione che le persone che continuano a rilasciare le proprie informazioni personali online sono anche

quelle che percepiscono un rischio minore riguardo la loro privacy online, sono persone più ottimiste. Analizzando i risultati della ricerca, inoltre, è possibile affermare come le persone più propense a rilasciare le proprie informazioni online siano anche quelle maggiormente intenzionate a rilasciarle nuovamente. Inoltre, l'ottimismo gioca un ruolo per nulla trascurabile. La moderazione dell'Ottimismo tra Atteggiamento e Intenzioni ha identificato come tale relazione negativa sia maggiore a meno che il livello di ottimismo nelle persone non sia alto. Infatti, la relazione tra Atteggiamento e Intenzioni viene smorzata ad alti livelli di Ottimismo, ovvero quando sono coinvolti individui che hanno caratteri di estroversione e coscienziosità, hanno aspettative più rosee di ciò che può succedere in futuro e una stabilità emotiva solida. Sono persone generalmente più aperte e socievoli e con una migliore capacità di adattamento alle situazioni che affrontano.

Tali risultati danno credito alla teoria della privacy online, estendo la teoria sull'ottimismo comparativo relativamente ai comportamenti, al sentimento di vulnerabilità e rischio percepito e alle intenzioni nel condivideere le proprie informazioni personali online anche nel contesto della privacy negli SNS (Social Networks Sites) (Acquisti, et al., 2015).

3.6.2 – Implicazioni manageriali

La sensazione che le proprie informazioni personali possano venire utilizzate in modi non consoni è fonte di gran paura per gli individui. Le aziende, più che su un discorso di trasparenza, possono lavorare su quanto e come gli individui hanno la possibilità di controllare le proprie informazioni online. Oltre alle informazioni rilasciate volontariamente, possono dar loro il controllo anche sulle tracce che lasciano quando navigano online. È possibile anche creare un'infrastruttura basate su tecnologie semplici che permettono di tenere sotto controllo costantemente dove finiscono le informazioni e chi vi potrebbe accedere. Questa soluzione sarebbe ottima soprattutto nel momento in cui gli utenti accedono a siti, e-commerce in primis, di cui non è chiara l'esatta provenienza, la gestione né tantomeno i fattori che rendono tali siti sicuri e affidabili.

Ovviamente anche le aziende stesse devono rinforzare tutti gli strumenti, le azioni e le tecnologie per garantire una totale sicurezza circa le informazioni raccolte. L'obiettivo è quello di far sentire l'utente il meno possibile vulnerabile ed esposto a minacce (Tucker,

2014). Questo garantirebbe anche una migliore qualità delle informazioni raccolte. Una qualità dei dati migliore può portare a una personalizzazione sempre più precisa, cucita sulle esigenze degli individui e sui loro interessi e a strategie di marketing sempre più accurate e misurabili.

Un'ulteriore strada che le aziende possono percorrere è quella di fornire alle persone tutti gli strumenti necessari per la gestione delle informazioni. Ciò vuol dire dar loro la possibilità di decidere quali informazioni possono essere utilizzate e quali no, decidere a quali terze parti possono essere vendute/scambiate. Per far ciò, tuttavia, è necessario uno snellimento e una semplificazione delle procedure di gestione della privacy attualmente presenti.

Informare le persone è uno step fondamentale che le organizzazioni (e società) dovrebbero fare. Informarle in maniera chiara e diretta sulle modalità di raccolta dati e sull'utilizzo che, se autorizzati, ne faranno. Per far questo, oltre al consueto "termini e condizioni", è necessario istruire le persone sui luoghi di lavoro e, specialmente, sui luoghi di istruzione, visto che la maggior parte degli utenti che passano molte ore online sono soprattutto giovani sotto i 30 anni.
Le persone possono anche essere informate sulla cosiddetta "filiera dei dati". In Europa, il GDPR garantisce la sicurezza sull'uso e la condivisione dei dati poiché le aziende, dal momento in cui raccolgono i dati dai clienti, fornitori e collaboratori devono comunque dimostrare di tenere traccia di quello che avviene ai dati, non solo del loro trattamento ma anche di eventuali cessioni o perdite (Gruschka, et al., 2018). La privacy è a tutti gli effetti una questione presa seriamente da tutti i garanti europei e perciò, come spiegato nell'analisi della letteratura, le aziende devono rendersi conformi alle norme per non incorrere in sanzioni.

3.6.3 – Limitazioni e ricerca futura

L'analisi di questa ricerca è stata fatta su un campione ridotto a 100 rispondenti a fronte di un campione analizzabile di 239. Il motivo è da ricondursi all'utilizzo del software di analisi SmartPls nella sua versione gratuita. Il campione analizzato è stato limitato all'Italia anche se c'è stato qualche rispondente dall'estero (Germania, Inghilterra, Svezia). È possibile ottenere nuovi risultati analizzando le intenzioni nel rilasciare le proprie informazioni personali online allargando il bacino di utenza e raggiungendo sia più persone della penisola italiana facendo

una distinzione interna, sia anche utenti esteri e analizzando gli utenti di diversi paesi, occidentali e orientali. Inoltre, tali intenzioni possono essere analizzate anche confrontando le diverse tipologie generazionali.

Lo studio ha rilevato e confermato come le persone non si sentano al sicuro nel fornire i propri dati online e adottano dei comportamenti tutelativi per salvaguardare le proprie informazioni presenti sul web (Acquisti, et al., 2012). I fattori che secondo la letteratura influenzano sia il sentimento di vulnerabilità che l'atteggiamento nel rilasciare le proprie informazioni online (trasparenza dei dati, fiducia/affidabilità, rischio di violazione della privacy) sono apparsi sorprendentemente insignificanti in questo studio. I risultati attesi erano diversi, ovvero che la trasparenza e l'affidabilità fossero variabili significative rispettivamente sulla vulnerabilità e sull'atteggiamento, soprattutto vista la scarsa conoscenza sul tema della raccolta dei dati e la tendenza a usufruire di Internet con un maggiore frequenza.

Per uno studio più efficace e completo, i ricercatori dovrebbero innanzitutto aver chiaro il profilo in senso ampio degli utenti che navigano online quotidianamente. La ricerca si è limitata ad analizzare il campione sulla base della frequenza di utilizzo quotidiano ma ci sono altri aspetti che possono integrare la ricerca. Ad esempio, sarebbe interessante conoscere le differenze, le abitudini, gli atteggiamenti e le intenzioni tra chi utilizza internet prevalentemente per cercare informazioni, chi lo utilizza per usufruire dei social network (attivamente e passivamente) o chi anche, ad esempio, solo per la fruizione di servizi di streaming.

Inoltre, è necessaria una ricerca costante per capire come le aziende possono adottare dei sistemi che garantiscono agli utenti una più completa gestione dei servizi relativi alla privacy e una maggiore trasparenza nelle pratiche di gestione dati accrescendo il senso di fiducia nei loro confronti. Tuttavia, ci sono ancora molte opportunità per ricerche future in modo da delineare un quadro al passo con l'evolversi delle tecnologie per seguire e adattarsi ai comportamenti degli individui online.

Infine, dati i risultati dell'effetto di moderazione, la ricerca potrebbe rivolgersi a migliorare e perfezionare le attività di marketing che riguardano la sfera della personalizzazione delle esperienze (di navigazione e di acquisto in primis) per creare maggiore engagement con gli individui definiti come ottimisti.

FIGURE

TABELLE

BIBLIOGRAFIA

Abbasi, Sarker & Chiang, 2016. Big Data Research in Information Systems: Toward an Inclusive Research Agenda. *Information Systems,* Vol. 17(Iss. 2 Article 3).

Abu Kausar, Dhaka & Singh, 2013. Web Crawler: A Review. *International Journal of Computer Applications,* Volume 63(No.2).

Acemoglu & Katz, 2011. Skills, tasks and technologies: Implications for employment and earnings. *Handbook of Labor Economics,* Volume 4, pp. 1043-1171.

Ackerman, 2021. *PositivePsichology.* [Online]
Available at: https://positivepsychology.com/big-five-personality-theory
[Accessed 23 03 2021].

Acquisti, Brandimarte & Loewenstein, 2015. Privacy and human behavior in the age of information. *Science,* 347(6221), pp. 509-514.

Acquisti & Grossklags, 2005. Privacy and rationality in individual decision making. *Economics of Information Security,* 1540(7993), pp. 27-33.

Acquisti, John & Loewenstein, 2012. The Impact of Relative Standards on the Propensity to Disclose. *Journal of Marketing Research,* Volume XLIX, pp. 160-174.

Akerman, Gaarder & Mogstad, 2015. The Skill Complementarity of Broadband Internet. *The Quarterly Journal of Economics,* 130(4), pp. 1781-1824.

Akyildiz, Sankarasubramaniam & Cayirci, 2002. A Survey on Sensor Networks. *IEEE Communications Magazine,* 163(6804), pp. 102-114.

Alloy, et al., 2006. Prospective incidence of first onsets and recurrences of depression in individuals at high and low cognitive risk for depression. *Journal of Abnormal Psychology,,* 115(1), pp. 145-156.

Ananny, 2016. Toward an Ethics of Algorithms: Convening, Observation, Probability, and Timeliness. *Science, Technology, & Human Values,* 41(1), pp. 93-117.

Anderson & Gerbing, 2013. Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin,* 103(3), pp. 411-423.

Andrejevic, 2007. ISpy: Surveillance and power in the interactive era.. *Mid-American Studies Association,* 48(3), pp. 177-178.

Anon., n.d. [Online]
Available at: https://azure.microsoft.com/it-it/overview/what-is-cloud-computing/

Atkinson, Castro & Ezell, 2009. The digital road to recovery: a stimulus plan to create jobs and boost productivity and revitalize America. *The Information Technology & Innovation Foundation.*

Baek, Kim & Bae, 2014. My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. *Computers in Human Behavior,* Volume 31, pp. 48-56.

Baker, Gentry & Rittenburg, 2005. Building Understanding of the Domain of Consumer Vulnerability. *Journal of Macromarketing,* 25(2), pp. 128-139.

Barocas & Nissembaum, 2014. Big data's end run around procedural privacy protections. *Communications of the ACM,* 57(11), pp. 31-33.

Barret, Davidson & Prabhu, 2015. Service innovation in the digital age: key contributions and future directions. *MIS Q,* Volume 39, pp. 135-154.

Barth & de Jong, 2017. The privacy paradox – investigating discrepancies between expressed privacy concerns and actual online behavior – a systematic literature review.. *Telematics Inform,* 34(7), pp. 1038-1058.

Baumeister, Zhang & Vohs, 2004. Gossip as Cultural Learning. *Review of General Psychology,* 8(2), pp. 111-121.

Bélanger & Crossler, 2011. Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly,* 35(4), pp. 1017-1041.

Benlian & Haffke, 2016. Does mutuality matter? Examining the bilateral nature and effects of CEO-CIO mutual understanding.. *The Journal of Strategic Information Systems,* 25(2), pp. 104-126.

Bentler & Huang, 2014. On components, latent variables, PLS and simple methods: Reactions to Rigdon's rethinking of PLS. *Long Range Planning,* 47(3), pp. 138-145.

Berger & Frey, 2016. Industrial Renewal in the 21st Century: Evidence from US Cities. *Regional Studies,* 51(3), pp. 404-413.

Bertino, Merril, Nesen & Utz, 2019. Redefining Data Transparency: A Multidimensional Approach. *IEEE COMPUTER SOCIETY,* pp. 16-26.

Beyer & Laney, 2012. The Importance of "Big Data": A Definition.

Bies & Tipp, 1996. Beyond distrust: getting even and the need for revenge. *Sage Publications, Newbury Park.*

Binns, Zhao, Van Kleek & Shadbolt, 2018. Measuring third party tracker power across web and mobile.

Boland & Cappeliez, 1997. Optimism and neuroticism as predictors of coping and adaptation in older women. *Personality and Individual Differences,* 22(6), pp. 909-919.

Brannon & Rauscher, 2018. Managing face while managing privacy: factors that predict young adults' communication about sexually transmitted infections with romantic partners.. *Health Communication,* 34(14), pp. 1833-1844.

Briley, Rudd & Aaker, 2017. Cultivating Optimism: How to Frame Your Future during a Health Challenge. *Journal of Consumer Research,* 44(4), pp. 895-915.

Brownlie, 2011. Not 'going there': Limits to the professionalization of our emotional lives. *Sociology of Health & Illness,* 33(1), pp. 130-144.

Brynjolfsson, & McAfee, 2014. *The second machine age: Work, progress, and prosperity in a time of brilliant technologies.* New York: W. W. Norton & Company.

Buck, Horbel, Germelmann & Eymann, 2014. *The unconscious app consumer: discovering and comparing the informationseeking patterns among mobile application consumers.,* Tel Aviv: Twenty Second European Conference on Information Systems.

Bute, 2015. Co-ownership of private information in the miscarriage context. *Journal of Applied Communication Research,* 43(1), pp. 23-43.

Camerer, 1998. Bounded rationality in individual decision making. *Experimental Economics,* Volume 1, pp. 163-183.

Campbell, Greenauer, Macaluso & End, 2007. Unrealistic optimism in internet events. *Computers in Human Behavior,* 23(3), pp. 1273-1284.

Carlo, Lyytinen & Boland Jr, 2012. Dialectics of collective minding: contradictory appropriations of information technology in a high-risk project.. *MIS Quarterly,* 36(4), pp. 1081-1108.

Carrascal, et al., 2013. *Your browsing behavior for a Big Mac: economics of personal information online..* Rio de Janeiro, IW3C2.

Carver & Scheier, 1993. Optimism. In S. J. Lopez & C. R. Snyder (Eds.),. In: Snyder & Lopez, eds. New York: Oxford University Press, pp. 74-86.

Carver, Scheier & Segerstrom, 2010. Optimism. *Clinical Psychology Review,* 30(7), pp. 879-889.

Case, 2009. *Social not-working. The Sun, Retrieved from.* [Online]
Available at: <http://www.thesun.co.uk/sol/homepage/news/article2277727.ece>
[Accessed 24 02 2021].

Chellappa & Sin, 2005. Personalization Versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. *Information Technology and Management,* Volume 6, pp. 181-202.

Chen, 2018. Revisiting the privacy paradox on social media with concerns, privacy self-efficacy, and social capital on privacy management. *American Behavioral Scientist,* 62(10), pp. 1392-1412.

Chen, Beaudoin & Hong, 2017. Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior,* Volume 70, pp. 291-302.

Child, Haridakis & Petronio, 2012. Blogging privacy rule orientations, privacy management, and content deletion practices: The variability of online privacy management activity at different stages of social media use.. *Computers in Human behavior,* 28(5), pp. 1859-1872.

Child, Pearson & Petronio, 2009. Blogging, communication, and privacy management: Development of the blogging privacy management measure.. *Journal of the American Society for Information Science and Technology,* 60(10), pp. 2079-2094.

Chin, Marcolin & Newsted, 2003. A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Information Systems Research,* 14(2), pp. 127-219.

Cho, Knijnenburg, Kobsa & Li, 2018. Collective privacy management in social media: a cross-cultural validation. *ACM Trans. Comput.-Hum. Interact,* 25(3), pp. 1-33.

Cho, Lee & Chung, 2010. Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience.. *Computer in Human Behavior,* 26(5), pp. 987-995.

Churchill, 1979. A paradigm for developing better measures for marketing construct. *Journal of Marketing Research,* Volume 16, pp. 64-73.

Clarke, 2016. Big Data, Big Risk. *Information Systems Journal,* 26(1), pp. 77-90.

Clark & Newell, 2013. Institutional work and complicit decoupling across the U.S. capital markets: the case of rating agencies. *Business Ethics Quarterly,* 23(1), pp. 1-30.

Columbus, 2014. *The Year Big Data Adoption Goes Mainstream in the Enterprise.* [Online] Available at: https://www.forbes.com/sites/louiscolumbus/2014/01/12/2014-the-year-big-data-adoption-goes-mainstream-in-the-enterprise/?sh=61057dd72055 [Accessed 29 12 2020].

Cranage, 2004. Conservative Choice, Service Failure, and Customer Loyalty: Testing the Limits of Informed Choice. *Journal of Hospitality & Tourism Research,* 28(3), pp. 327-345.

Crandall, Lehr & Litan, 2007. *The Effects of Broadband Deployment on Output and Employment: A Cross-sectional Analysis of U.S. Data.,* s.l.: Citeseer.

Crawford, Miltner & Gray, 2014. Critiquing Big Data: Politics, Ethics, Epistemology. *International Journal of Communication,* Volume 8, pp. 1663-1672.

Crawford & Schultz, 2014. Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *B.C.L. Rev.,* 55(1), pp. 93-128.

Cui & Wu, 2016. Utilizing customer knowledge in innovation: Antecedents and impact of customer involvement on new product outcomes.. *Journal of the Academy of Marketing Science,* Volume 44, pp. 516-538.

Currie & Seddon, 2017. The regulatory, technology and market "dark arts trilogy" of high frequency trading: A research agenda. *Journal of Information Technology,* Volume 32, pp. 111-126.

Dash, Mohapatra & Pattniak, 2010. A survey on Application of Wireless sensor network using Cloud Computing. *International Journal of Computer Science & Emerging Technologies,* 1(4), pp. 50-55.

Davenport & Kudyba, 2016. Designing and developing analytics-based data products. *MIT Sloan Management Review,* 58(1), pp. 83-89.

Davenport & Patil, 2012. Data scientist. *Harvard Business Review,* pp. 70-76.

Davis & Warshaw, 1992. What Do Intention Scales Measure?. *The Journal of General Psychology,* 119(4), pp. 391-407.

Debatin, Lovejoy, Horn & Huges, 2009. Facebook and online privacy: Attitudes, behaviors, and unintended consequences.. *Journal of Computer-Mediated Communication,* Volume 15, pp. 83-108.

DeGroot & Vik, 2017. We were not prepared to tell people yet": confidentiality breaches and boundary turbulence on Facebook.. *Comput Human Behavior,* Volume 70, pp. 351-359.

Delforte, 2016. *Data Center Efficiency Assessment,* New York: New York Data Center.

DERA, 2016. *Rohstoffe fur Zukunftstechnologien,* Potsdam: Helmholtz-Zentrum Potsdam.

Diakopoulos, 2016. Accountability in algorithmic decision making. *Communications of the ACM,* 59(2), pp. 56-62.

Dijkastra & Henseler, 2015. Consistent partial least squares path modeling. *MIS Quarterly,* 39(2), pp. 297-316.

Dijkstra, 2014. PLS' Janus face—response to Professor Rigdon's "Rethinking partial least squares modeling: In praise of simple methods.". *Long Range Planning,* 47(3), pp. 146-153.

Diney & Hart, 2006. An extended privacy calculus model for e-commerce transaction. *Information Systems Research,* 17(1).

Ebert, Tucker & Roth, 2002. Psychological resistance factors as predictors of general health status and physical symptom reporting. *Psychology, Health, and Medicine,* 7(3), pp. 363-375.

Ekbia, et al., 2015. Big data, bigger dilemmas: A critical review. *JOURNAL OF THE ASSOCIATION FOR INFORMATION SCIENCE AND TECHNOLOGY,* 66(8), pp. 1523-1546.

Elgesem, 1996. Privacy Respect for Persons,and Risk. In: Elgesem, ed. *Philosophical Perspectives on Computer-Mediated Communication.* Albany: State University of New York Pres, pp. 45-66.

Ellicott, et al., 1990. Life events and the course of bipolar disorder. *The American Journal of Psychiatry,* 147(9), pp. 1194-1198.

Endsley, 2017. Autonomous Driving Systems: A Preliminary Naturalistic Study of the Tesla Model S. *Journal of Cognitive Engineering and Decision Making,* 11(3), pp. 225-238.

Fahey & Hino, 2020. COVID-19, digital privacy, and the social limits on data-focused public health responses. *International Journal of Information Management,* Volume 55.

Falahrastegar, Haddadi, Uhlig & Mortier, 2014. Anatomy of the third-party web tracking ecosystem.

Fang, Jiang & Song, 2016. Customer profitability forecasting using Big Data analytics: A case study of the insurance industry. *Computers & Industrial Engineering,* Volume 101, pp. 554-564.

Figueroa, 2018. New technology, labour and digital sovereignty. *Global Labour Column,* Volume 315.

Flammini & Sisinni, 2014. Wireless Sensor Networking in the Internet of Things and Cloud Compuing Era. *Procedia Engineering,* Volume 87, pp. 672-679.

Flick, 2016. Informed Consent and the Facebook Emotional Manipulation Study. *Research Ethics,* 12(1), pp. 14-28.

Fornell & Larcker, 1981. Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research,* 18(1), pp. 39-50.

Frey & Osborne, 2013. The future of employment: How susceptible are jobs to computerisation?. *Technological Forecasting and Social Change,* Volume 114, pp. 254-280.

Fried, 1984. Privacy. *Philosophical Dimemsions of Privacy,* pp. 203-222.

Galliers, Newell, Shanks & Topi, 2017. Datification and its human, organizational and societal effects. *The Journal of Strategic Information Systems,* 26(3), pp. 185-190.

Gao, e. a., 2016. Disruptive trends will transform the auto industry.

Garud & Rappa, 1994. A Socio-Cognitive Model of Technology Evolution. *Organization Science,* 5(3), pp. 344-362.

Gerlach, Widjaja & Buxmann, 2015. Handle with care: How online social network providers' privacy policies impact users' information sharing behavior. *The Journal of Strategic Information Systems,* 24(1), pp. 33-43.

Gillet, Lehr, Osorio & Sirbu, 2006. *Measuring Broadband's Economic Impact,* Arlington: Massachusetts Institute of Technology .

Goes, 2014. Editor's Comments: Big Data and IS Research. *MIS Quarterly,* 38(3), pp. 3-8.

Gölzer & Fritzsche, 2017. Data-driven operations management: Organisational implications of the digital transformation in industrial practice.. *Production Planning & Control,* 28(16), pp. 1332-1343.

Goos,, Konings & Vandeweyer,, 2015. Employment Growth in Europe: The Roles of Innovation, Local Job Multipliers and Institutions. *Local Job Multipliers and Institutions.*

Goos, Manning & Salomons, 2014. Explaining Job Polarization: Routine Biased Technological Change and Offshoring. *The American Economic Review,* 104(8), pp. 2509-2526.

Gossart, 2015. Rebound effects and ICT: a review of the literature. *Innovations for sustainability,* pp. 435-448.

Greenstein & Prince, 2006. The diffusion of the Internet and the Geography of the Digital Device in the United States. *NBER Working Paper,* Volume 12182.

Greenwald, 2017. How AI is transforming the workplace. *Wall Street Journal .*

Grégoire & Fisher, 2008. Customer Betrayal and Retaliation: When Your Best Customers Become Your Worst Enemies. *Journal of the Academy of Marketing Science,* 36(2), pp. 247-261.

Gross & Acquisti, 2005. Information revelation and privacy in online social networks. *Proceedings of the 2005 ACM workshop on Privacy in the electronic society,* pp. 71-80.

Gruschka, Mavroeidis, Mavroeidis & Jensen, 2018. Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR. *IEEE International Conference on Big Data (Big Data),* pp. 5027-5033.

Gunther, Mehrizi, Huysman & Feldberg, 2017. Debating big data: a literature review on realizing value from big data. *The Journal of Strategic Information Systems,* 26(3), pp. 191-209.

Gunther, Mehrizi, Huysman & Feldberg, 2017. Debating big data: a literature review on realizing value from big data. *The Journal of Strategic Information Systems,* 26(3), pp. 191-209.

Günther, Rezazade Mehrizi, Huysman & Feldberg, 2017. Debating big data: A literature review on realizing value from big data.

Gust, et al., 2017. How a traditional company seeded new analytics capabilities. *MIS Quarterly Executive,* 16(3), pp. 215-230.

Hair, et al., 2016. *Essentials of business research methods.* 3rd.ed ed. New York: Routledge.

Hair, Hult, Ringle & Sarstedt, 2017. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM).* Second Edition ed. U.S.: Sage publications.

Hair, Ringle & Sarstedt, 2011. PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice,* 19(2), pp. 139-152.

Hair, Sarstedt & Ringle, 2012. Partial least squares: The better approach to structural equation modeling?. *Long Range Planning,,* 45(5-6), pp. 312-319.

Halavais, 2015. Overcoming terms of service: a proposal for ethical distributed research. *Information, Communication & Society,* 22(11), pp. 1567-1581.

Hammonds & Joshua, 2015. A model of privacy control: examining the criteria that predict emerging adults' likelihood to reveal private information to their parents. *Western Journal of Communication,* 79(5), pp. 591-613.

Hansen & Sia, 2015. Hummel's digital transformation toward omnichannel retailing: key lessons learned.. *MIS Quarterly Executive,* 14(2).

Helweg-Larsen, Sadeghian & Webb, 2001. The stigma of being pessimistically biased. *Journal of Social and Clinical Psychology,* 21(1), pp. 92-107.

Helweg-Larsen & Shepperd, 2001. Do moderators of the optimistic bias affect personal or target risk estimates? A review of the literature. *Personality and Social Psychology Bulletin,* 5(1), pp. 79-95.

Henseler, et al., 2014. Common beliefs and reality about partial least squares: Comments on Rönkkö & Evermann (2013).. *Organizational Research Methods,* 17(2), pp. 182-209.

Henseler, Ringle & Sarstedt, 2015. A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science,* 43(1), pp. 115-135.

Henseler, Ringle & Sinkovics, 2009. The use of partial least squares path modeling in international marketing.. *Advances in International Marketing,,* Volume 20, pp. 277-319.

Herzberg, Glaesmer & Hoyer, 2006. Separating optimism and pessimism: A robust psychometric analysis of the Revised Life Orientation Test. *Psychological Assessment,* 18(4), p. 433.

Hess, Matt, Benlian & Wiesbock, 2016. Options for formulating a digital transformation strategy. *MIS Quarterly Executive,* 15(2).

Hess, Matt, Benlian & Wiesboeck, 2016. *Digitalization and leadership – how experienced leaders interpret daily realities in a digital world.* Oestrich-Winkel, EBS University.

Higgins, 2006. Value from hedonic experience and engagement. *Psychological Review,* 113(3), p. 439.

Hlatshwayo, & Hlatshwayo, 2012. The evolving structure of the American economy and the employment challenge. *Comparative Economic Studies,* 54(4), pp. 703-708.

Hodder & Livingstone, 2009. Children and the internet: Great expectations, challenging realities. *Polity .*

Hoffman & Novak, 2017. Consumer and object experience in the internet of things: An assemblage theory approach.. *Journal of Consumer Research,* 44(6), pp. 1178-1204.

Holotiuk & Beimborn, 2017. *Critical success factors of digital business strategy.* Frankfurt, Frankfurt School of Finance & Management.

Howard,, Agarwal, & Hussain,, 2011. The Dictators' Digital Dilemma: When Do States Disconnect Their Digital Networks?. Issue 13.

Hulland, 1999. Use of partial least squares (PLS) in strategic management research: a review of four recent studies. *Strategic Management Journal,* 20(2), pp. 195-204.

Imai, Keele & Tingley, 2010. A General Approach to Causal Mediation Analysis.. *Psychological Methods,* 15(4), p. 309.

Ismagilova, Gileva, Galimova & Glukhov, 2017. Digital Business Model and SMART Economy Sectoral Development Trajectories Substantiation. *Internet of Things, Smart Spaces, and Next Generation Networks and Systems,* pp. 13-28.

Jöhnk, Röglinger, Thimmel & Urbach, 2017. How to implement agile IT setups: a taxonomy of design options.. *Association for Information Systems,* pp. 1521-1535.

John & Srivastava, 1999. *The Big-Five trait taxonomy: History, measurement, and theoretical perspectives. In L. A. Pervin & O. P. John (Eds.),.* Vol 2 ed. Berkeley: University of California.

Jones, 2018. How to stop data centers from gobbling up the world's electricity. *Nature ,* 561(7722), pp. 163-167.

Kahre, Hoffman & Ahlemann, 2017. *Beyond business-IT alignment-digital business strategies as a paradigmatic shift: a review and research agenda,* Honolulu: Hamilton Library.

Kane, et al., 2016. Aligning the Organization for its Digital Future. *MIT Sloan Management Review ,* 50(1).

Kannan & Li, 2017. Digital marketing: A framework, review and research agenda. *International Journal of Research in Marketing,* 34(1), pp. 22-45.

Kasturi, Prasanna Devi, Vinu Kiran & Manivannan, 2016. Airline Route Profitability Analysis and Optimization Using BIG DATA Analyticson Aviation Data Sets under Heuristic Techniques. *Procedia Computer Science,* Volume 87, pp. 86-92.

Katz, & Callorda,, 2014. Economic impact of broadband deployment in Ecuador. *Regional Dialogue on the information society.*

Katz, 2012. *Impact of broadband on the economy: research to date and policy issue.* Geneva, International Telecommunication Union.

Katz, Avila & Meille, 2011. *Economic impact of wireless broadband in rural America.* [Online] Available at: http://rca-usa. org/wp-content/uploads/2011/02/Economic-Study-02.24, [Accessed 28 22 2020].

Katz & Dorn, 2013. The growth of low-skill service jobs and the polarization of the US labor market. *American Economic Review,* 103(5), pp. 1553-97.

Katz, Gubernik & Felix, 2014. Technology and adolescents: perspectives of the things to come. *Education and Information Technologies,* 19(4), pp. 863-886.

Katz, Levy & Murnane, 2003. The skill content of recent technological change: An empirical exploration. *The Quarterly journal of economics,* 118(4), pp. 1279-1333.

Kay & Mattern, 2004. The Design Space of Wireless Sensor Networks. *IEEE wireless communications,* 11(6), pp. 54-61.

Kelting, Duhachek & Whitler, 2017. Can Copycat Private Labels Improve the Consumer's Shopping Experience? A Fluency Explanation. *Journal of the Academy of Marketing Science,* 45(4), pp. 569-585.

Kennedy-Lightsey & Frisby, 2016. Parental privacy invasion family communication patterns, and perceived ownership of private information. *Communication Reports,* 29(2), pp. 75-86.

Kim & Hancock, 2015. Optimistic bias and Facebook use: Self–other discrepancies about potential risks and benefits of Facebook use. *Cyberpsychology, Behavior and Social Networking,* 18(4), pp. 214-220.

Kirmani, Hamilton, Thompson & Lantzy, 2017. Doing Well Versus Doing Good: The Differential Effect of Underdog Positioning on Moral and Competent Service Providers. *Journal of Marketing,* 81(1), pp. 103-117.

Kirwan, 2015. Psychology and security: utilizing psychological and communication theories to promote safer cloud security behaviors.

Klötzer & Pflaum, 2017. *Toward the development of a maturity model for digitalization within the manufacturing industry's supply chain,* Bamberg: Association for Information System.

Konrad, 2021. *Il Post.* [Online]
Available at: https://www.ilpost.it/2021/01/12/whatsapp-privacy-facebook/

Krishnamurthy, Naryshkin & Wills, 2011. Privacy leakage vs. protection measures: The growing disconnect. *Proceedings of the Web,* 2(2011), pp. 1-10.

Kudina & Verbeek, 2019. Ethics from Within: Google Glass, the Collingridge Dilemma, and the Mediated Value of Privacy. *Science, Technology, & Human Values,* 44(2), pp. 291-314.

Kumar, Zhang & Luo, 2014. Modeling Customer Opt-In and Opt-Out in a Permission-Based Marketing Context. *Journal of Marketing Research,* 51(4), pp. 403-419.

Lamberton & Stephen, 2016. A thematic exploration of digital, social media and mobile marketing: Research evolution from 2000 to 2015 and an agenda for future inquiry. *Journal of Marketing,* 80(6), pp. 146-172.

Leach, Ellemers & Barreto, 2007. Group Virtue: The Importance of Morality (vs. Competence and Sociability) in the Positive Evaluations of In-Groups. *Journal of Personality and Social Psychology,* 93(2), p. 234.

Leary & Leder, 2009. The Nature of Hurt Feelings: Emotional Experience and Cognitive Appraisals. *Feeling Hurt in Close Relationships in New York: Cambridge University Press,* pp. 15-33.

Lebowitz, 2016. *businessinsider.* [Online]
Available at: http://www.businessinsider.com/big-five-personality-traits-predict-leadership-2016-12
[Accessed 22 03 2021].

Leischnig, Wölfl, Ivens & Hein, 2017. From digital business strategy to market performance: Insights into key concepts and processes. *Association for Information System.*

Lemon & Verhoef, 2016. Understanding customer experience throughout the customer journey. *Journal of marketing,* 80(6), pp. 69-96.

Leonhardt, Haffke, Kranz & Benlian, 2017. *Reinventing the IT function: the role of IT agility and IT ambidexterity in supporting digital business transformation.,* Guimarães: Ecis.

Li, 2008. Third-person effect, optimistic bias, and sufficiency resource in internet use.. *Journal of Communication,* 58(3), pp. 568-587.

Liao, Luo & Gurung, 2009. Rebuilding post-violation trust in B2C electronic commerce. *Journal of Organizational End User Computing,* 21(1), pp. 60-74.

Libert, Beck & Wind, 2016. The network imperative: How to survive and grow in the age of digital business models. *Harvard Business Review Press.*

Lin, 2011. Technological adaptation, cities, and new work. *Review of Economics and Statistics,* 93(2), pp. 554-574.

Li, Su, Zhang & Mao, 2018. Digital transformation by SME entrepreneurs: A capability perspective. *Information Systems Journal,* 28(6), pp. 1129-1157.

Little, Bovaird & Widaman, 2006. On the merits of orthogonalizing powered powered and product terms: Implications for modeling interaction terms among latent variables. *Structural Equation Modeling,,* 13(4), pp. 497-519.

Liu, Marchewka & Ku, 2004. American and Taiwanese perceptions concerning privacy, trust, and behavioral intentions in electronic commerce.. *Journal of Global Information Management,* 12(1), pp. 18-40.

Loebbecke & Picot, 2015. Reflections on societal and business model transformation arising from digitization and big data analytics: A research agenda. *The Journal of Strategic Information Systems,* 24(3), pp. 149-157.

Loebbecke & Picot, 2017. Reflections on societal and business model transformation arising from digitization and big data analytics: a research agenda. *The Journal of Strategic Information Systems,* 24(3), pp. 149-157.

Lohmöller, 1989. *Latent variable path modeling with partial least squares.* Berlin: Springer-Verlag Berlin Heidelberg GmbH.

Loiseau, et al., 2016. Green economy and related concepts: An overview. *Journal of cleaner production,* Volume 139, pp. 361-371.

Lounsbury, Saudargas & Gibson, 2004. An investigation of personality traits in relation to intention to withdraw from college. *Journal of College Student Development,* 45(5), pp. 517-534.

Lyon, 2014. Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big data & society,* 1(2).

Madden, 2012. From Database to Big Data. *IEEE Internet Computing,* 16(3), pp. 4-6.

Madden, n.d. *Pew Research Center.* [Online]
Available at: https://www.pewresearch.org/internet/2014/11/12/public-privacy-perceptions/

Majchrzak, Markus & Wareham, 2016. Designing for digital transformation: lessons for information system reasearch from the study of ICT and societal challenges. *MIS quarterly,* 40(2), pp. 267-277.

Maknkopf, 2019. The '4th wave od industrial revolution. *EuroMemo Group,* Volume 1.

Maler, 2012. Smart mobility. *eJournal of eDemocracy & Open Government,* 4(1).

Malhotra, Kim & Agarwal, 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research.*

Manovich, 2011. Trending: the promises and the challenges of big social data. *Debates in the digital humanities,* 2(1), pp. 460-475.

Manyika, Chui & Miremadi, 2017. A Future that Works: AUtomation, Employment and Productivity. *McKinsey Global Institute Research, Tech. Rep,* Volume 60.

Marcus & Davis, 2014. Eight (No, Nine!) Problems with Big Data. *The New York Times,* 6(4).

Markus, 2015. New games, new rules, new scoreboards: the potential consequences of big data. *Journal of Information Technology,* 30(1), pp. 58-59.

Markus & Topi, 2015. Big Data, Big Decisions for Science , Society, and Business. *National Science Foundation.*

Marshall, et al., 1992. Distinguishing optimism from pessimism: Relations to fundamental dimensions of mood and personality.. *Journal of Personality and Social Psychology,* 62(6), p. 1067.

Martin, 2015. Ethical Issues in the Big Data Industry. *MIS Quarterly Executive,* Volume 2, p. 14.

Martin, Borah & Palmatier, 2017. Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing,* 81(1), pp. 36-58.

Matarazzo, Penco, Produmo & Quaglia, 2021. Digital transformation and customer value cration in Made in Italy SMEs: A dynamic capabilities perspective. *Journal of Business Research,* Volume 123, pp. 642-656.

Matt, Hess & Benlian, 2015. Digital transformation strategies. *Business & Information Systems Engineering,* 57(5), pp. 339-343.

Matt, Hess & Benlian, 2015. Digital transformation strategies.. *Business & Information Systems Engineering,* 57(5), pp. 339-343.

May, Wirtz & Williams, 2007. Consumer Online Privacy Concerns and Responses: A Power-Responsibility Equilibrium Perspective. *Journal of the Academy of Marketing,* 35(4), pp. 572-585.

McAfee & Brynjolfsson, 2012. Big Data: The Management Revolution. *Harvard Business Review,* 90(10), pp. 60-68.

McFarland, 2012. Unauthorized Transmission and Use of Personal Data.

McKnight, Choudhury & Kacmar, 2002. Developing and validating trust ,easures for e-commerce: An integrative typology. *Information systems research,* 13(3), pp. 334-359.

Mele, C., 2020. *Internet of things* [Interview] 2020.

Mell & Grance, 2011. The NIST Definition of Cloud Computing.

Metcalf & Crawford, 2016. Where are human subjects in Big Data research? The emerging ethics divide. *Big Data & Society,* 3(1).

Metzger & Suh, 2017. Comparative Optimism About Privacy Risks on Facebook. *Journal of Communiaction,* 67(2), pp. 203 - 232.

Michael & Miller, 2013. Big data: new opportunities and new challenges. *Computer,* 46(6), pp. 22-24.

Miller, 1971. The Assaults on Privacy: Computer, Data Banks and Dossiers. *University of Michigan Press.*

Milligan, 2003. Optimism and the five-factor model of personality, coping, and health behavior. *Dissertation Abstracts International.*

Milne & Boza, 2000. Trust and concern in consumers' perceptions of marketing information management practices. *of Direct Marketing,* 13(1), pp. 5-24.

Mitchell & Dacin, 1996. The Assessment of Alternative Measures of Consumer Expertise. *Journal of Consumer Research,* 23(3), pp. 219-239.

Mlne & Culnan, 2004. Strategies for reducing online privacy risks: Why consumers read (or Don't Read) online privacy notices.. *Journal of Interactive Marketing,* 18(3), pp. 15-29.

Montes, Sand-Zantman & Valletti, 2017. The value of personal information in markets with endogenous privacy.

Moretti, 2010. Local Multipliers. *American Economic Review,* 100(2), pp. 373-377.

Mosavi & Vaezipour, 2013. Developing Effective Tools for Predictive Analytics and Informed Decisions. Technical Report. *University of Tallinn, Technical Report.*

Mothersbaugh, Foxx, Beatty & Wang, 2012. Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information. *Journal of Service Research,,* 15(1), pp. 76-98.

Neumeier, Wolf & Oesterle, 2017. *The manifold fruits of digitalization – Determining the literal value behind.* St. Gallen, University of Augsburg.

Newell & Marabelli, 2015. Strategic opportunities (and challenges) of algorithmic decision-making: a call for action on the long-term societal effects of 'datification. *The Journal of Strategic Information Systems,* 24(1), pp. 3-14.

Newell, S. & Marabelli, M., 2014. *The Crowd and Sensor Era: Opportunities and Challenges for individuals, Organization, Society and Researchers.* Auckland, Thirty Fifth International Conference on Information Systems.

Newman, P., 2020. *THE SMART SPEAKER REPORT: Smart speakers could be the fastest-growing digital platform ever — here's how to engage with customers through the devices.* [Online] Available at: https://www.businessinsider.com/smart-speaker-report?IR=T

Ng & Wakenshaw, 2017. The Internet-of-Things: Review and research directions. *International Journal of Research in Marketing,* 34(1), pp. 3-21.

Norberg, Horne & Horne, 2007. The privacy paradox: personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs,* 41(1), pp. 100-126.

Pagani & Pardo, 2017. The impact of digital technology on relationships in a business network.. *Industrial Marketing Management ,* Volume 67, pp. 185-192.

Park, 2013. Digital literacy and privacy behavior online. *Communication Research,* 40(2), pp. 215-236.

Parker, Van Alstyne & Choudary, 2017. *Platform revolution: How networked markets are transforming the economy and how to make them work for you..* New York: W. W. Norton & Company, Inc..

Perloff, 2009. Mass media, social perception, and the third-person effect. *Media effects: Advances in theory and research,* Volume 3, pp. 252-268.

Peterson, 2000. The future of optimism. *American Psychologist,* 55(1), p. 44.

Peterson & Vaidya, 2003. Optimism as virtue and vice. In E. C. Chang & L. J.Sanna (Eds.). *Virtue, vice, and personality: The complexity of behavior,* pp. 23-37.

Petracca, Ciani, Cuccinello & Tarricone, 2020. Harnessing Digital Health Technologies During and After the COVID-19 Pandemic: Context Matters. *Journal of medical Internet research,* 22(12).

Petronio & Gaff, 2010. Managing privacy ownership and disclosure. *Family communication about genetics: Theory and practices,* pp. 120-135.

Petronio & Lewis, 2010. Medical disclosure in oncology: Families, patients, and providers. *Family communication and health transitions. New York: Peter Lang Publishing,* pp. 269-296.

Petronio & Reierson, 2009. Regulating the privacy of confidentiality: Grasping the complexities through communication privacy management theory. *Uncertainty, information management, and disclosure decisions: Theories and application.*

Petronio & Reierson, 2009. Regulating the privacy of confidentiality: Grasping the complexities through communication privacy management theory. *Uncertainty, information management, and disclosure decisions: Theories and application,* pp. 365-383.

Polacco & Backes, 2018. The Amazon Go Concept: Implications, Applications, and Sustainability. *Journal of Business and Management,* 24(1), pp. 79-92.

Pope, 2012. Legal fundamentals of surrogate decision making.. *Chest ,* 141(4), pp. 1074-1081.

Puri, 2013. How Online Retailers Use Predictive Analytics To Improve Your Shopping Experience.. *Journal of Retailing,* 93(1), pp. 79-95.

Purra & Carlsson, 2016. Third-Party Tracking on the Web: A Swedish Perspective. *IEEE,* pp. 28-34.

Purwanto, Zuiderwijk & Janssen, 2020. Citizens' Trust in Open Government Data: A Quantitative Study about the Effects. *The 21st Annual International Conference on Digital Government Research,* pp. 1-9.

Rachels, 1976. Why privacy is important. *Philos Public Affairs ,* pp. 323-333.

Rajaraman, 2016. Big Data Analytics. *TDWI best practices report, fourth quarter,* 19(4), pp. 1-34.

Raul L. Katz, 2017. Economic impact of digital transformation on the economy. *ITU, GSR-17 Discussion paper.*

Richard & King, 2014. Big Data Ethics. *Big Data & Society,* 1(2).

Richman & Leary, 2009. Reaction to: Discrimination, Stigmatization, Ostracism, and Other Forms of Interpersonal Rejection: A Multimotive Model. *Psychological Review,* 116(2), p. 365.

Rigdon, 2012. Rethinking partial least squares path modeling: In praise of simple methods. *Long Range Planning,* 45(5-6), pp. 341-358.

Rigdon, et al., 2014. Conflating antecedents and formative indicators: A comment on Aguirre-Urreta and Marakas.. *Information Systems Research,* 25(4), pp. 780-784.

Robertson, 2015. *Holacracy: The new management system for a rapidly changing world..* New York: Henry Holt and Company.

Russom, 2011. Big Data Analytics. *TDWI best practices report, fourth quarter,* 19(4), pp. 1-34.

Saarikko, Westergren & Blomquist, 2020. Digital Transformation: Five recommendations for the digital conscious firm. *Business Horizons,* 63(6), pp. 825-839.

Sachs & Lawrence, 2012. Smart Machines and Long-Term Misery. *NBER WORKING PAPER SERIES,* Issue 18629.

Santoro, 2020. Covid-19: il tracciamento dei contatti e il supporto delle nuove tecnologie. *Ricerca & Pratica ,* 37(2), pp. 78-81.

Sarstedt, Ringle, Henseler & Hair, 2014. On the emancipation of PLS-SEM: A commentary on Rigdon (2012). *Long Range Planning,* 47(3), pp. 154-160.

Scharf, 2007. Report Casts Doubt on the Impact of Data Breaches on Identity Theft. *Internal Auditor,* 64(4), pp. 23-24.

Scheier & Carver, 1992. Effects of optimism on psychological and physical well-being: Theoretical overview and empirical update. *Cognitive Therapy and Research.*

Scheier & Carver, 1992. Effects of optimism on psychological and physical well-being: Theoretical overview and empirical update. *Cognitive Therapy and Research,,* 16(2), pp. 201-228.

Schilling & Izzo, 2017. *Gestione dell'innovazione.* New York: McGraw-Hill Education.

Schoeman & Ferdinand, 1984. Privacy: philosophical dimensions. *American Philosophical Quarterly,* 21(3), pp. 199-213.

Scott & Walsham, 2005. Reconceptualizing and managing reputation risk in the knowledge economy: Toward reputable action. *Organization Science,* 16(3), pp. 308-322.

Sebastian, et al., 2017. How big old companies navigate digital transformation. *MIS Quarterly Executive,* 16(3), pp. 197-213.

Segerstrom, Castañeda & Spencer, 2003. Optimism effects of cellular immunity: Testing the affective and persistence models. *Personality and Individual Differences,* 35(7), pp. 1615-1624.

Selander & Jarvenpaa, 2016. Digital action repertoires and transforming a social movement organization.. *Mis Quarterly,* 40(2), pp. 331-352.

Sengupta, 2013. Staying Private on the New Facebook. *New York Times,* Volume 7.

Sharpe, Martin & Roth, 2011. Optimism and the Big Five factors of personality: Beyond Neuroticism. *Personality and Individual Differences,* 51(8), pp. 946-951.

Shmueli & Koppius, 2011. Predictive Analytics in Information Systems Research. *MIS quarterly,* pp. 553-572.

Shoenbachler & Gordon, 2002. Trust and consumer willingness to provide information in database-driven relationship marketing. *Journal of interactive marketing,* 16(3), pp. 2-16.

Sia, Soh & Weill, 2016. How DBS Bank pursued a digital business strategy. *MIS Quarterly Executive,* 15(2).

Sign & Hess, 2017. How chief digital officers promote the digital transformation of their companies.. *MIS Quarterly Executive ,* 16(1).

Singh & Singh, 2012. Big Data Analytics. *Information Computing Technology,* Volume 4.

Solove, 2003. Identity Theft, Privacy, and the Architecture of Vulnerability. *Hastings Law Journal,* 54(1227).

Solove, 2011. Nothing to hide: False tradeoff between privacy and security. *Yale University Press.*

Solove, 2017. A Brief History of Information Privacy Law. *PROSKAUER ON PRIVACY .*

Someh, Breidbach, Davern & Shanks, 2016. *Ethical implications of big data analytics.* Istambul, ECIS.

Someh, Davern, Breidbach & Shanks, 2019. Ethical Issues in Big Data Analytics: A Stakeholder Perspective. *Communications of the Association for Information Systems,* 44(1), p. 35.

Srivastava, et al., 2006. Optimism in close relationships: How seeing things in a positive light makes them so. *Journal of Personality and Social Psychology,* 91(1), p. 143.

Srivastava & Shainesh, 2017. Bridging the service divide through digitally enabled service innovations: evidence from Indian health care service providers.. *Mis Quarterly,* 39(1), pp. 245-268.

Stahl, Timmermans & Mittelstadt, 2016. The Ethics of Computing: A Survey of the Computing - Oriented Literature. *ACM Computing Surveys,* 48(4), pp. 1-38.

Stahl & Wright, 2018. Ethics and Privacy in AI and Big Data: Implementing Responsible Research and Innovation. *IEEE Security & Privacy,* 16(3), pp. 23-33.

Stats, I. L., 2020. *Internet Live Stats.* [Online]
Available at: https://www.internetlivestats.com/
[Accessed 29 12 2020].

Steuber & Solomon, 2012. Relational uncertainty, partner interference, and privacy boundary turbulence: Explaining spousal discrepancies in infertility disclosures.. *Journal of Social and Personal Relationships,* 29(1), pp. 3-27.

Svahn, Mathiassen, Lindgren & Kane, 2017. Mastering the digital innovation challenge. *MIT Sloan Management Review,* 58(3), p. 14.

Tan, Pan, Lu & Huang, 2015. The role of IS capabilities in the development of multi-sided platforms: the digital ecosystem strategy of Alibaba.com. *Journal of the Association for Information Systems,* 16(4), p. 2.

Tanriverdi & Lim, 2017. How to survive and thrive in complex, hypercompetitive, and disruptive ecosystems? The roles of IS-enabled capabilities. *Asociation for Information System.*

Tene & Polonetsky, 2013. A theory of creepy: technology, privacy and shifting social norms. *Yale JL & Tech,* Volume 16, p. 59.

Terry, 2017. Regulatory disruption and arbitrage in health-care data protection. *Yale J. Health Pol'y L. & Ethics,* 17(143).

Thompson, Petronio & Braithwaite, 2012. An examination of privacy rules for athletic/academic advisors and college student-athletes: A communication privacy management perspective. *Communication Studies.*

Thompson, Petronio & Braithwaite, 2012. An examination of privacy rules for athletic/academic advisors and college student-athletes: A communication privacy management perspective. *Communication Studies,* 63(1), pp. 54-76.

Thorson, 2015. Investigating adult children's experiences with privacy turbulence following the discovery of parental infidelity.. *Journal of Family Communication,* 15(1), pp. 41-57.

Tissera, Thelijjagoda & Goonathilake, 2017. User-centric privacy preservation solution to control third party access in digital databases. *International Journal of Advances in Engineering & Technology,* 10(1), p. 30.

Tokic & Pecnik, 2011. Parental behaviors related to adolescents' self-disclosure: Adolescents' views. *Journal of and Personal Relationships,* 28(2), pp. 201-222.

Tomlinson & Mayer, 2009. The role of causal attribution dimensions in trust repair,. *Academy of Management Review,* 34(1), pp. 85-104.

Töytäri, et al., 2017. *Overcoming institutional and capability barriers to smart services.* Hawaii, Association for Information System.

Trabucchi, Buganza & Pellizzoni, 2017. Give away your digital services: Leveraging big data to capture value New models that capture the value embedded in the data generated by digital services may make it viable for companies to offer those services for free. *Research-Technology Management,* 60(2), pp. 43-52.

Treccani, n.d. *Treccani.* [Online]
Available at: https://www.treccani.it/vocabolario/privacy

TRUSTe, 2014. *TRUSTe.* [Online]
Available at: http://info.truste.com/lp/truste/Web-Resource-HarrisConsumerResearchUS-ReportQ12014_LP.html

Tucker, 2014. Social Networks, Personalized Advertising and Privacy Controls. *Journal of Marketing Research.*

Tucker, 2014. Social Networks, Personalized Advertising and Privacy Controls. *Journal of Marketing Research,* 51(5), pp. 546-562.

Tu & Piramuthu, 2020. On addressing RFID/NFC-based relay attacks: An overview. *Decision Support Systems,* 129(113194).

Turkle, 2016. Reclaiming Conversation: The Power of Talk in a Digital Age. *Penguin Random House,.*

Tyler & Kramer, 1996. Wither Trust?.

Vendrell-Herrero, Bustinza, Parry & Georgantzis, 2017. Servitization, digitization and supply chain interdependency.. *Industrial Marketing Management,* Volume 60, pp. 69-81.

Venkatraman, 2017. The Digital Matrix: New Rules for Business Transformation Through Technology. *Escritos Contables y de Administración,* 8(1), pp. 89-92.

Verhoef, et al., 2021. Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research,* Volume 122, pp. 889-901.

Vial, 2019. Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems,* 28(2), pp. 118-144.

Vidal, 2017. Tsunami of data could consume one fifth of global electricity by 2025. *Climate Home News,* Volume 11.

Voigt & von dem Bussche, 2017. Special Data Processing Activities. In: Voigt & v. d. Bussche, eds. *The EU General Data Protection Regulation (GDPR) .* s.l.:Springer, pp. 235-243.

Watson, 2017. Preparing for the cognitive generation of decision support.. *MIS Quarterly Executive,* 16(3).

Wenzel Egan & Hesse, 2018. Tell me so that I can help you": private information and privacy coordination issues in context of eldercare. *Journal of Family Communication,* 18(3), pp. 217-232.

West, 2016. *Internet shutdowns cost countries $ 2.4 billion last year,* Washington, DC: Center for Technological Innovation at Brookings, Washington, DC.

Westin, 1967. Privacy and Freedom. *Washington and Lee Law Review,* 25(1), p. 166.

Wiener, et al., 2012. Targeting the Right Crowd for Corporate Problem Solving - a Siemens Case Study with TechnoWeb 2.0. *In International Technology Management Conference,* pp. 239-347.

Wixom & Markus, 2017. To develop acceptable data use, build company norms. *Research Briefing of the Center for Information System Research,* 17(4).

Wixom & Ross, 2017. How to monetize your data. *MIT Sloan Management Review ,* 58(3).

Wold, 1985. Encyclopedia of statistical sciences. *Partial least squares,* pp. 581-591.

Wu, Huang, Yen & Popova, 2012. The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior,* 28(3), pp. 889-897.

Wulf, Mettler & Brenner, 2017. Using a digital services capability model to assess readiness for the digital consumer. *MIS quarterly executive,* 16(3), pp. 171-195.

Xu, 2012. Reframing privacy 2.0 in online social network.. *Journal of Constitutional Law,* 14(4), pp. 1077-1102.

Yeow, Soh & Hansen, 2017. *Aligning with new digital strategy: a dynamic capabilities approach,* s.l.: s.n.

Yeow, Soh & Hansen, 2018. Aligning with new digital strategy: a dynamic capabilities approach. *The Journal of Strategic Information Systems,* 27(1), pp. 43-58.

Zakir, Seymour & Berg, 2015. Big Data Analytics. *Issues in Information Systems ,* 16(2).

Zakir, Seymour & Berg, 2015. Big Data Analytics. *Issues in Information Systems,* 16(2).

Zanon, R., 2020. *Digital Dictionary.* [Online]
Available at: https://www.digitaldictionary.it/blog/report-digital-2020-scenario-digitale-mondo-e-italia#:~:text=Sono%20quasi%204%2C54%20miliardi,9%25%20circa%20rispetto%20al%202019.
[Accessed 16 1 2021].

Zhu & Furr, 2016. Product platforms: Making the leap. *Harvard business review,* 94(4), pp. 72-78.

Ziefle, Halbey & Kowalewski, 2016. Users' Willingness to Share Data on the Internet: Perceived Benefits and Caveats. *IoTBD,* pp. 255-265.

Zuboff, 2015. Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology,* 30(1), pp. 75-89.

Zuckerman, 2003. Optimism and pessimism: Biological foundations. In E. C. Chang & L. J. Sanna (Eds.),. In: Chang & Arbor, eds. *Optimism & pessimism: Implications for theory, research, and practice..* Washington, DC: American Psychological Association, pp. 169-188.

Zviran, 2008. User's perspectives on privacy in web-based applications. *Journal of Computer Information Systems,* 48(4), pp. 97-105.

APPENDICE A - QUESTIONARIO

Genere

- Uomo
- Donna
- Preferisco non specificarlo

Età in anni compiuti

- <18
- 18-25
- 26-35
- 36-45
- 46-55
- 55-65
- >65

Come sei venuto a conoscenza di questo sondaggio?

- E-mail
- Linkedin
- WhatsApp
- Instagram
- Facebook
- Telegram
- Di persona

Qual è il titolo di studio più alto che hai conseguito?

- Diploma di scuola secondaria di primo grado o inferiore
- Diploma di scuola secondaria di secondo grado
- Laurea triennale
- Laurea specialistica
- Master o superiore

Skip To: End of Survey If Qual è il titolo di studio più alto che hai conseguito? = Diploma di scuola secondaria di primo grado o inferiore

Qual è la tua professione?

- Studente
- Studente / lavoratore
- Impiegato
- Libero professionista
- Disoccupato

Con quale frequenza navighi su internet (motori di ricerca, social networks, mail etc.) al giorno?

- < 1 ora
- Tra le 2 e le 5 ore
- tra le 5 e le 8 ore
- tra le 8 e le 12 ore
- > 12 ore

Skip To: End of Survey If Con quale frequenza navighi su internet (motori di ricerca, social networks, mail etc.) al giorno? = < 1 ora

Quanto ritieni di essere informato riguardo il tema della raccolta dei dati personali online?
(1= Per nulla informato, 7= Totalmente informato)

- 1
- 2
- 3
- 4
- 5
- 6
- 7

Da dove deriva la tua conoscenza riguardo il tema della raccolta dati online?
Puoi selezionare più risposte.

6. Notiziari, giornali, telegiornali
7. Internet, web
8. Esperienza personale
9. Scuola, università
10. Famiglie, amici
11. Termini e condizioni di utilizzo

Per ciascuna delle seguenti affermazioni, indica il tuo grado di accordo o disaccordo.
(1 = Totalmente in disaccordo, 7 = Assolutamente d'accordo)

- Non mi crea alcun problema rilasciare le mie informazioni personali online
- È probabile che in futuro continuerò a rilasciare le mie informazioni personali online
- Ho intenzione di continuare a rilasciare le mie informazioni personali online
- Sono sensibile al modo in cui le aziende gestiscono le mie informazioni personali online
- È importante mantenere intatta la mia privacy dalle società online
- Rispetto ad altre persone, per me la privacy personale online è molto importante.
- Sono preoccupato per le minacce alla mia privacy personale online
- Mi sento sfruttato per come le mie informazioni personali online vengono impiegate da parte dei social networks che utilizzo

- Mi sento sfruttato per come le mie informazioni personali online vengono impiegate da parte dei motori di ricerca che utilizzo
- Mi sento sfruttato per come le mie informazioni personali online vengono impiegate da parte dei browser Internet che utilizzo
- Mi sento sfruttato per come le mie informazioni personali online vengono impiegate da parte dei provider dei servizi telefonici che utilizzo
- Seleziona "2" come risposta a questa domanda
- Quando penso a come le mie informazioni personali online vengono gestite sono più predisposto a fornire informazioni veritiere
- Quando penso a come le mie informazioni personali online vengono gestite fornisco di proposito informazioni personali non veritiere
- Quando penso a come le mie informazioni personali online vengono gestite penso che vada bene dare informazioni personali fuorvianti
- Ritengo di avere il controllo su cosa succede alle mie informazioni personali online
- Spetta a me stabilire quanto un entità può utilizzare le mie informazioni personali online
- Ho voce in capitolo su come le mie informazioni personali online vengono usate
- Ho voce in capitolo sulla condivisione delle mie informazioni personali online con altri.
- Le informazioni personali online in possesso dei social networks che utilizzo mi fanno sentire sicuro
- Le informazioni personali online in possesso dei motori di ricerca che utilizzo mi fanno sentire sicuro
- Le informazioni personali online in possesso dei browser Internet che utilizzo mi fanno sentire sicuro
- Le informazioni personali online in possesso dei provider di servizi telefonici che utilizzo mi fanno sentire sicuro
- Seleziona "2" come risposta a questa domanda
- Ho maggiori probabilità di avere un'esperienza negativa sulla privacy rispetto agli altri utenti a seguito dell'utilizzo dei social networks
- Ho maggiori probabilità di avere un'esperienza negativa sulla privacy rispetto agli altri utenti a seguito dell'utilizzo dei motori di ricerca
- Ho maggiori probabilità di avere un'esperienza negativa sulla privacy rispetto agli altri utenti a seguito dell'utilizzo dei browser di ricerca

- Ho maggiori probabilità di avere un'esperienza negativa sulla privacy rispetto agli altri utenti a seguito dell'utilizzo dei provider di servizi telefonici

Le attività di gestione delle mie informazioni personali online da parte dei social networks a cui le rilascio sono:

	1	2	3	4	5	6	7	
A me non chiare								A me chiare
Confuse								Dirette
Difficili da comprendere								Facili da comprendere
Vaghe								Trasparenti

Le attività di gestione delle mie informazioni personali online da parte dei siti internet e dei motori di ricerca a cui le rilascio sono:

	1	2	3	4	5	6	7	
A me non chiare								A me chiare
Confuse								Dirette
Difficili da comprendere								Facili da comprendere
Vaghe								Trasparenti

Le attività di gestione delle mie informazioni personali online da parte dei provider di servizi telefonici a cui le rilascio sono:

	1	2	3	4	5	6	7	
A me non chiare								A me chiare
Confuse								Dirette
Difficili da comprendere								Facili da comprendere
Vaghe								Trasparenti

I social networks a cui rilascio le mie informazioni online sono:

	1	2	3	4	5	6	7	
Disonesti								Onesti
Falsi								Sinceri
Manipolativi								Non manipolativi
Non affidabili								Affidabili

I siti internet e i motori di ricerca a cui rilascio le mie informazioni online sono:

	1	2	3	4	5	6	7	
Disonesti								Onesti
Falsi								Sinceri
Manipolativi								Non manipolativi
Non affidabili								Affidabili

I provider di servizi telefonici a cui rilascio le mie informazioni online sono:

	1	2	3	4	5	6	7	
Disonesti								Onesti
Falsi								Sinceri
Manipolativi								Non manipolativi
Non affidabili								Affidabili

Genere

- Uomo
- Donna
- Preferisco non specificarlo

Età in anni compiuti

- <18
- 18-25
- 26-35
- 36-45
- 46-55
- 55-65
- >65

Provincia di residenza

_____

Qual è il titolo di studio più alto che hai conseguito?

- Diploma di scuola secondaria di primo grado o inferiore
- Diploma di scuola secondaria di secondo grado
- Laurea triennale
- Laurea specialistica
- Master o superiore

Reddito familiare

- < 15.000,00 €
- 15.000 - 49.999,00 €
- 50.00,00 € - 79.999,00 €
- 80.000,00 € - 99.999,00 €
- > 100.000,00 €