Dipartimento di Economia e Management.
Cattedra di Economia e Gestione delle Imprese.

L’economia digitale e l’introduzione del GDPR:

RISCHI ED OPPORTUNITÀ PER LE IMPRESE.

RELATORE

Prof.ssa Maria Isabella Leone

CANDIDATO

Lorenzo Marmorato
Matricola: 199211

ANNO ACCADEMICO 2017 – 2018

Indice

INTRODUZIONE.

Il 3 Luglio del 2018 si è tenuto al centro congressi di Milano il forum dell'economia digitale, "*The future of tomorrow*".
Il manifesto di questo evento recitava le seguenti, testuali, parole: "La storia dell'uomo è costellata di rivoluzioni. […] L'evoluzione non è sempre lineare ma porta con sé sviluppo e benessere. […] Il nostro primo passo è guidare il cambiamento. Le competenze digitali sono l'alfabeto dell'evoluzione. […]Il Piano industriale dell'Italia dei prossimi dieci anni non può non affrontare il nodo dell'evoluzione digitale. La rivoluzione, infatti, è quella che esplode e non è facile governare, ma si rischia solo di subire o contenere. L'evoluzione è invece un processo, a volte silenzioso, altre più evidente, che si allarga come un fiume, dalla sorgente alla foce. Sta a noi costruire quelle competenze digitali su cui edificare il futuro […]". (autori vari, Manifesto FED, 2018)

Quanto alla base del forum tenutosi al MIco è fondamentale per una nuova interpretazione dell'economia, un'interpretazione in chiave moderna: il processo di digitalizzazione tenutosi negli ultimi decenni ha infatti portato le competenze digitali ad avere un ruolo di primo rilievo; ora non sono più una qualità aggiuntiva che un'impresa può detenere nel proprio interno oppure no, oggi queste competenze sono le solide fondamenta sul quale porre le basi per i vantaggi competitivi e per il successo aziendale.

Il seguente elaborato sarà composto da quattro capitoli: verranno analizzati i cambiamenti che l'informatica ha portato nell'economia.

Nel primo capitolo sarà necessario discutere della *digital business transformation* e dei cambiamenti che questa comporta per le attività economiche.

Sarebbe sbagliato da parte delle imprese italiane, partendo dalle piccole finendo alle big companies, adottare un comportamento apatico e passivo a questa evoluzione che ormai è entrata nella sua fase più viva.

È fondamentale, adesso, capire quando è iniziato questo cambiamento e perché ad oggi il digitale assume questa notevole importanza. È necessario comprendere a che punto sono le imprese italiane nell'adattamento a queste nuove tecnologie con un focus sulle PMI: questo perché, come è noto, l'esistenza delle ultime è vitale per la nostra economia; seguendo i dati della Confcommercio del 2009, su una totalità di 4.338.766 imprese in Italia ben 4.335.448 sono piccole e medie imprese, ben il 99,9%. (Ufficio studi ConfCommercio, 2009)

Inoltre, verranno sottolineate alcune delle caratteristiche ritenute essenziali per le imprese che hanno l'intenzione di operare anche, o soprattutto, nel digitale: queste saranno esposte con relativi esempi di aziende che hanno avuto successo apportando dei cambiamenti interni proprio per accogliere al meglio queste nuove tecnologie digitali

ma non mancheranno i casi fallimentari di imprese che non hanno creduto nella scienza tecnologica.

Questo primo capitolo si concluderà con una panoramica sulle PMI in Italia e come si stanno adattando alla nuova era che presenta si dei vantaggi ma anche numerosi rischi.

Il secondo capitolo offrirà una panoramica sul ruolo e l'importanza che ricoprono i dati al giorno d'oggi. Sarà introdotto il concetto dei Big Data e quello del *machine learning*, il quale da molti è ritenuto il "futuro" per l'analisi dei dati.

Particolare attenzione verrà concessa anche alle figure aziendali che hanno a che fare con lo studio delle informazioni possedute da un'azienda e come questa può ottenere un valore da esse, la cosiddetta *data monetization.*

La chiusura di questo capitolo avrà un taglio meno scientifico rispetto al resto della tesi e si concentrerà sul caso *"Cambridge Analytica"* il quale, sebbene sia stato trattato da tutti come un ratto di dati (*data breach*), spiega come non c'è stata alcuna falla all'interno di Facebook ed il tutto sia stato (più o meno) legale. Tale episodio è importante ai fini dell'elaborato poiché spiega come le nostre informazioni possano essere colte non necessariamente in via illegale e senza il nostro consenso.

Con lo scoppio della vicenda "Cambridge Analytica" gli utenti hanno sentito aumentare il bisogno di tutela per i propri dati personali: il 25 Maggio 2018, dopo diversi anni di sviluppo e perciò molto prima che scoppiasse lo "scandalo" che ha investito Facebook, è entrato in vigore in tutti gli stati dell'Unione Europea il Regolamento Generale sulla Protezione dei Dati, tradotto in inglese "*General Data Protection Regulation"* e da qui prende l'abbreviazione che l'ha fatta conoscere ai più, GDPR.

Successivamente, nel terzo capitolo, vedremo nei dettagli la normativa e l'impatto che questa può avere nell'economia in generale, analizzando sia come si adatteranno le piccole e medie imprese, sia come si adatteranno le grandi imprese e i provider di dati come, per l'appunto, colossi del calibro di Facebook e Google.

È bene, inizialmente, scrivere in grandi linee cosa rappresenta questo regolamento.

Il GDPR va a sostituire la Direttiva Europea in merito alla protezione dei dati 95/46/EC risalente al 1995. Fondamentalmente non vi sono cambiamenti radicali rispetto alla vecchia normativa, quindi in grandi linee i principi cardine sulla privacy e sulla protezione dei dati sono rimasti gli stessi. Tuttavia delle migliorie sono state necessarie anche a fronte dei cambiamenti e delle evoluzioni tecnologiche che si sono verificate negli ultimi anni.

Gli obiettivi principali del regolamento sono sostanzialmente due: il primo è quello di dare ai propri cittadini un controllo più completo sui propri dati personali, mentre il secondo ha lo scopo di semplificare il quadro normativo per le imprese che gestiscono

questi dati. Ad essere soggetto di questo GDPR sono tutte le imprese che vendono beni o servizi, a pagamento e non. È, quindi, d'obbligo per le imprese rivedere le proprie policy e, qualora ce ne fosse il bisogno, adeguarle alle richieste del regolamento. Se il tutto non venisse rispettato allora si potrebbe incorrere in una multa di un ammontare complessivo di venti milioni di euro oppure, in alternativa, al 4% del fatturato annuo globale.

Gli aspetti innovativi che possiamo riscontrare sono due, oltre le sanzioni: l'extraterritorialità ed il consenso.

La normativa si applica a tutti i paese facenti parte l'Unione Europea, a prescindere dal Paese in cui l'azienda ha la propria sede legale: se queste ultime monitorano i dati degli utenti residenti in Europa allora dovranno attenersi al GDPR.

Tutte le società che raccolgono i dati devono saper spiegare in maniera molto semplice le condizioni che regolano il trattamento, nonché la raccolta, dei dati: è loro responsabilità, infatti, usare un linguaggio comprensibile a tutti gli utenti, non equivoco, affinché essi possano dare il loro consenso.

È necessario anche affermare che comunque il GDPR è solo un tassello di un mosaico molto più grande creato dall'Unione Europa: per comprendere al meglio come si è giunti a questo punto è necessario, almeno nella parte iniziale di tale capitolo, analizzare il contesto normativo e politico in cui questo è nato e quindi analizzare *in primis* quella che ad oggi è conosciuta come Agenda digitale europea.

Nel quarto ed ultimo capitolo verrà approfondita la figura del DPO: nei fatti il *Data Protection Officer* nasce proprio con l'introduzione del GDPR è quindi opportuno stabilire nel migliore dei modi quale sia il suo ruolo all'interno dell'azienda.

In sostanza si noterà che la figura non è totalmente innovativa. In seguito verranno analizzate alcune peculiarità di questo ruolo come quando un individuo deve essere designato a ricoprirlo, da chi deve essere nominato e quali debbono essere le sue competenze.

CAPITOLO 1: "LA BUSINESS DIGITAL TRANSFORMATION"

1.1 Introduzione alla digital transformation.

Credere che la rivoluzione digitale per le imprese sia stato qualcosa di improvviso sarebbe sciocco: questi sono cambiamenti che avvengono lentamente, fanno un passo alla volta per arrivare lontano dopo decenni e senza dover nemmeno mai giungere, necessariamente, ad un traguardo.

Secondo quanto scritto da Fausto Colombo nel manuale del corso di alta formazione UPA, questa rivoluzione è in atto ormai da tempo ed ha significato una novità radicale nel modo di vivere: dalla cultura all'approccio al lavoro passando per l'economia.

Il docente universitario afferma che la tecnologia ha cambiato tutto connettendo vari *device* tra di loro grazie all'utilizzo della rete e moltiplicando, perciò, i canali d'accesso all'informazione: i mezzi di comunicazione in nemmeno mezzo secolo sono cambiati profondamente e le informazioni vengono trasmesse attraverso un linguaggio di base fatto di numeri, i *bit*.

A detta sua questa rivoluzione inizia verso la fine degli anni'60, nel 1969 per essere precisi, quando ARPA (Advanced Research Project Agency), dopo aver stretto collaborazione con varie università americane, riesce finalmente ad elaborare una rete per le telecomunicazioni. Questo progetto inizialmente aveva scopi militari e fu pensato durante la Guerra Fredda ma, nei fatti, ricoprirà un grandissimo ruolo nella società civile moderna: è nato internet, una "*interconnessione globale tra reti informatiche di natura ed estensione diversa*". (Colombo F. , 2016)

Nel frattempo anche i dispositivi iniziano ad evolversi e nel 1966 la nostrana Olivetti produce la Olivetti 101, un lontano antenato del PC, che sarebbe fondamentalmente una calcolatrice programmabile da scrivania, la prima nel mondo. Nel 1977 Steve Jobs e Steve Wozniac realizzarono il primo computer *user-friendly* con Apple II, quindi l'utente inizia a diventare, molto lentamente, co-protagonista di questa rivoluzione; la svolta decisiva ci sarà negli anni '80 quando vengono introdotti nel mercato i primi dispositivi leggeri e mobili. (Colombo, 2016)

Nei tempi moderni l'innovazione più importante è stata senza dubbio Facebook e l'introduzione anche di altri social network: è da qui, infatti, che il consumatore inizia ad approcciarsi in maniera differente alle aziende e viceversa. Secondo Guido Di Fraia ciò è proprio merito dei social: si assiste al decadimento del paradigma "comunicazione-potere" e perciò le imprese perdono il potere della comunicazione in favore dei clienti, ora ciò che essi vogliono sarà comunicato direttamente da loro. Secondo questa concezione la differenza tra il commercio offline e quello online risiede proprio nella comunicazione. Il senso che deve essere dato a quest'utlima, però, non deve essere limitato solamente al marketing ma anche ai feedback che le imprese ricevono sui loro servizi o sui loro prodotti: l'azienda offline di parecchi anni fa, qualora avesse creato un prodotto o un servizio a dir poco fallimentare, non avrebbe mai subito un eco negativo pari all'attività promozionale, mancavano i mezzi; l'online porta le imprese di oggi che immettono sul mercato prodotti fallimentari a subire ripercussioni negative dovute ad un malcontento dei consumatori espresso sui social, questa espressione sarà esponenzialmente più grande rispetto all'attività di promozione del prodotto, ciò per via del fatto che nell'era di internet e del commercio digitale fra cliente e rivenditore si inseriscono altri soggetti, i clienti passati, che possono influenzare le performance dell'impresa dando pareri agli altri utenti, siano essi positivi o negativi. (Di Fraia, 2016)

È, ovviamente, notabile come il marketing sia stato solamente il primo dei tanti processi aziendali a digitalizzarsi, o comunque ad essere quello che fino ad ora ha subito di più gli effetti di questo fenomeno, ma ad esso sono seguiti anche altri processi aziendali. Uno di questi per esempio è il *costumer care:* in chiave *social* anch'esso. Secondo uno studio promosso da ***McKinsey&Co*** è emerso come le imprese potrebbero risparmiare in maniera approssimativa intorno ai 1300 miliardi all'anno qualora digitalizzassero al massimo livello possibile i processi aziendali. Tuttavia, secondo anche quanto scrive Chiara Colombo, alcuni processi interni all'impresa ,consolidati ormai da tanti anni, sono difficili da rinnovare in chiave aziendale e l'incaricato a guidare questo cambiamento dovrà farlo facendo permanere un equilibrio fra la convenienza del rinnovamento e l'abitudine del processo ben radicato.

Secondo il pensiero della docente universitaria questa "trasformazione" deve passare per tre tappe indispensabili:

1) Tutte le organizzazioni hanno un determinato grado di trasformabilità, quindi studiare e sfruttare quest'ultimo;
2) Bisogna individuare gli elementi da cui partire e perciò il cambiamento deve iniziare con un'attenta analisi della struttura organizzativa;
3) Il risultato deve essere efficace ed una sintesi coerente con gli obiettivi prefissati.

Tuttavia si possono sempre correre dei "rischi": quello proveniente dall'alto e quello proveniente dal basso. Con il primo si vuole intendere che i processi aziendali non possono essere innovati solamente dall'alto, apponendo buon conto delle solide basi teoriche, perdendo però di vista quella che è realtà aziendale; il secondo comporta l'affidamento dell'innovazione dei processi soltanto alle parti che ne portano avanti gli interessi, la partecipazione di questi può essere molto utile però è fondamentale che sia guidata dall'alto. (Colombo C. , 2016)

Quindi, questo cambiamento della tecnologia avvenuto con il tempo è metaforicamente paragonabile alla cosiddetta "lama a doppio taglio": le imprese hanno più facilità a relazionarsi con il cliente, a capire ciò che esso vuole ma qualora tutto ciò non sia prodotto in maniera soddisfacente le ripercussioni per l'impresa saranno altamente negative. Inoltre adattare i processi aziendali alle nuove tecnologie può risultare difficoltoso. È necessario affermare, però, che tutto sommato quella della tecnologia, per le imprese, è un'opportunità. "We are entering a new age where people participate in the economy like never before. […] new forms of mass collaboration are changing how goods and services are invented, produced, marketed […] This change presents far-reaching opportunities for every company and person who gets connected" (D. Tapscott, 2006)

Queste opportunità di cui si è discusso ci mettono di fronte a due differenti filoni interpretativi da prendere in considerazione dati i cambiamenti a cui siamo stati posti davanti da questa rivoluzione ("*digital disruption")*: il primo filone è portato avanti da studiosi come Tapscott o Siegel i quali affermarono che questi cambiamenti digitali hanno come diretta conseguenza la nascita di una "nuove economia" (*new economy)*, per poter avere la meglio sui propri *competitors* in tale contesto bisogna saper seguire nuove regole e nuovi principi poiché le basi dell'attività d'impresa nate con il

"fordismo" non sono più applicabili; al secondo filone appartengono economisti del calibro di Porter e Rosabeth Moss Kanter, provenienti da scuole di pensiero più consolidate, che sostengono che i principi tradizionali sui quali si basavano le imprese non sono interamente "da buttare" in favore di nuovi principi, tuttavia c'è bisogno di una rivalutazione o di una integrazione dei principi "classici" in chiave moderna. (Genco, 2002)

Ovviamente come riporta Genco nel suo scritto, "Il management d'impresa fra *old* e *new economy* : nuovi principi o nuove soluzioni?", è necessario prima dare una definizione al termine *new economy* per poter analizzare al meglio il tema in questione. Una delle definizioni che sono state date con il tempo, seppur prettamente focalizzata sull'aspetto tecnologico, metteva in risalto come l'utilizzo di internet a partire dalla seconda metà degli anni '90 abbia fatto fare un "salto di qualità" alle imprese quanto a facilità di uso degli strumenti resi disponibili dalle ICT e l'abbattimento dei costi proveniente da questi ultimi. La *new economy* era considerata, quindi, niente più che un sinonimo del concetto di *digital economy*, almeno secondo questa visione. Se intesa in questo modo, la "nuova economia", offre l'opportunità alle imprese di esplorare nuovi mercati ma al tempo stesso apre a nuove minacce: nuovi concorrenti, nuovi intermediari, nuovi soggetti di domanda. Ma, d'altronde, offre anche delle opportunità come già ampiamente detto: le imprese si relazionano in un nuovo modo sia con i clienti, sia fra di loro, sia con altri soggetti facenti parte l'ambiente competitivo, ci si relaziona quindi in un modo differente grazie ad internet ed, inoltre, la tecnologia viene utilizzata anche per aumentare l'efficienza degli altri processi aziendali. Partendo soltanto da queste basi, numerosi studiosi hanno ipotizzato che si fosse entrati nella cosiddetta "era dell'accesso" in cui le regole dell'economia classica sarebbero state sovvertite totalmente. In questo nuovo ordine la proprietà dei mezzi di produzione e dei beni durevoli sarebbe stata considerata un limite alle possibilità di manovra, di flessibilità e di innovazione strategica mentre l'accesso alle reti telematiche sarebbe stato considerato l'elemento caratterizzante di questa nuova era economica. (Rifkin, 2000)

Comunque collegare il concetto di *new economy* soltanto ad una questione tecnologica è un errore senza ombra di dubbio, infatti è qualcosa di più grande: è il passaggio da

quello che era un sistema economico basato sulla produzione di massa e sul fordismo ad un nuovo sistema basato sullo sfruttamento della conoscenza per fini produttivi, sulla flessibilità e sul concetto di "reti d'impresa". Quest'ultime che costituiscono delle relazioni fra imprese e, per forza di cose, anche le relazioni con i clienti costituiscono l'ossatura della *network economy*, un sistema economico basato su soggetti che intrattengono dei rapporti continui, interattivi e collaborativi.

Associare, dunque, la *new economy* ai concetti di *digital economy* e di *network economy* presuppone ampliare la definizione data in precedenza e, quindi, associarla non solo alle nuove tendenze tecnologiche ma anche ad alcuni aspetti di carattere organizzativo. Nell'individuazione di questa nuova ed ulteriore componente della nuova economia la letteratura economico-manageriale è concorde su un aspetto: questa *new economy* ha portato ad una dematerializzazione dei fattori produttivi su i quali si basano i vantaggi competitivi dell'impresa in questione. La "conoscenza", intesa come risorsa, diventa perciò vitale per le imprese ed è un fattore produttivo-chiave.

Per concludere, quindi, queste innovazioni che hanno portato alla nascita di una nuova economia comportano un approccio tradizionale ma adattato ai tempi nei quali viviamo oppure la creazione di regole totalmente nuove?

Secondo quanto scritto ciò dipende, in sostanza, dalla definizione che si è pronti a dare al concetto di *new economy.* Se ci si soffermasse allo strato superficiale, quello analizzato per primo, nel quale si associa la *digital economy* a questa nuova era economica, allora si può affermare che la questione principale per la dirigenza dell'impresa è quello di risolvere i tradizionali problemi di gestione ma adottando nuove soluzioni. L'organizzazione dell'impresa può aumentare la propria efficienza e la propria efficacia grazie all'adozione di nuove tecnologie. Si deve sempre tener conto, però, che la tecnologia di per sé non è mai fonte di un vantaggio competitivo ma è la capacità di presidio dei processi-chiave (come il rapporto con i clienti o la gestione della catena di fornitura) modificati dall'uso della tecnologia a fornire un vantaggio all'impresa. Se, invece, ci si vuole addentrare in un'analisi più profonda dell'economia per capire i cambiamenti in atto nei sistemi produttivi e di consumo dei paesi industrializzati la risposta sarà senza ombra di dubbio diversa e ambigua. Diversa poiché la nuova economia è caratterizzata da un ruolo-chiave della conoscenza

rispetto a quanto accadeva nella scorsa era economica, in cui la varietà era ridotta al minimo. Proprio per questo motivo possiamo dire che oggigiorno è la conoscenza ad essere una fonte di sviluppo, di innovazione e di vantaggio competitivo. Ambigua perché non ci sono ricette precodificate: il panorama varia in continuazione per via della capacità creativa ed innovativa degli attori che lo frequentano. È difficile trovare soluzioni immediate ai problemi dell'impresa come, invece, poteva accadere fino a qualche decennio fa. Il panorama di riferimento sarà modellato in continuazione dalle imprese e dai portatori di conoscenza che decidono di aggregarsi a progetti condivisi di creazione di nuove opportunità, nuove esperienze, nuove soluzioni e nuovi prodotti. (Genco, 2002)

1.2 Business digitali.

Ad oggi sono numerose le imprese che hanno come mezzo principale d'azione il web: fra le tante ricordiamo dei colossi come Amazon, Netflix e Airbnb. Da notare che tutte e tre operano in settori differenti. Ciò non fa altro che sottolineare come lo "stare nel mercato" sia radicalmente cambiato nel tempo. Questo comprende anche le piccole e medie imprese che operano principalmente nei settori tradizionali dell'economia: vecchi e potenti colossi come Blockbuster sono stati spazzati via da quelle che fino a pochi anni fa erano imprese emergenti, del calibro di Netflix. Il discorso potrebbe ovviamente continuare comprendendo anche altri settori, non solo quello dell'entertainment, tipo quello dei mezzi di trasporto (Uber che contrasta i tradizionali taxi) o dell'alloggio (Airbnb che contrasta i tradizionali hotel). Ecco, se si pensa che quello raggiunto negli ultimi anni è il punto massimo della "*digital disruptive era*" ci si sbaglia di grosso: secondo degli studi della *Global Center for Digital Business Trasformation* il digitale sovvertirà ulteriormente le leggi del mercato rendendo il 40% degli *incumbent* orfani della propria posizione di mercato in favore, presumibilmente, di giganti che stanno ancora emergendo o che devono ancora emergere. Tutto ciò ricorda vagamente quanto successo nel diciottesimo secolo con la seconda rivoluzione industriale. (Dell'Olio, 2016)

È impossibile pensare che le imprese tradizionali restino immobili dinnanzi a questi cambiamenti, come già detto in precedenza. Tuttavia è sbagliato da parte di un'impresa

credere che semplicemente portando il suo vecchio modello di business "online" allora si è "al passo con i tempi". Spesso e volentieri i proprio modelli devono essere ripensati e innovati affinchè possano adattarsi a questa nuova società digitale. Alessandro D'Adda, partner di *MBS Consulting*, ha delineato quattro fondamentali caratteristiche che devono essere rispettate da ogni impresa che vuole disegnare una strategia digitale. Analizziamole anche con relativi esempi. (D'Adda, 2017)

Velocità e agilità.

Il mercato odierno richiede alle imprese velocità ed agilità, questo presuppone una macchina operativa ben funzionante ma anche la capacità da parte dell'azienda di saper cambiare idea, seguendo i trend del mercato, in maniera rapida e applicarla nella migliore delle maniere rivedendo i modelli di business dove necessario.

Saper mettersi in discussione quindi è vitale. Gli esempi lampanti li possiamo trovare più che nelle companies che hanno avuto successo, in quelle che hanno fatto della lentezza e della rigidità le fondamenta per il loro fallimento. I casi che potremmo evidenziare sono quelli di Nokia e Kodak, due aziende che non avrebbero bisogno di presentazioni: la prima era la regina della telefonia dagli anni Novanta fino ai primi anni del nuovo millennio; la seconda era un colosso nel settore delle macchine e pellicole fotografiche.

Nokia, come detto, era una potenza incontrastata nel settore della telefonia. I primi problemi iniziarono a nascere con l'introduzione degli smartphone e il prepotente ingresso nel mercato della Apple. La lentezza ad innovare la propria piattaforma, il proprio ecosistema applicativo ed un hardware innovativo la portarono a perdere la propria posizione di leadership. Il vero e proprio problema, però, è che questa lentezza non era dovuta a delle mancanze di competenze da parte dell'azienda finlandese ma una paralisi manageriale di fronte al cambiamento del mercato.

Kodak, è un caso addirittura più eclatante. L'impresa americana aveva inventato la fotografia digitale già dal 1975 ed in uno studio interno all'impresa, datato 1981, era comprensibile che questa innovazione avrebbe cambiato totalmente il mercato nel

futuro immediato. Tuttavia il management vide nel digitale dell'epoca solamente una opportunità eccessivamente rischiosa dato che i profitti aziendali provenivano principalmente da carte fotografiche, pellicole e macchinette fotografiche consumabili. Proprio per questo la dirigenza non credeva che questo azzardo valesse la pena e ci fu un'ostinazione da parte loro a difendere la propria rendita di posizione: purtroppo per loro la scelta fu sbagliata.

Innovazione.

Le tecnologie digitali spingono sempre più in alto il livello di innovazione all'interno delle imprese. L'eterogeneità e la velocità con il quale questa innovazione avviene rende ormai parzialmente obsoleto il vecchio approccio aziendale per quanto riguarda, appunto, le innovazioni: i soli centri di ricerca e sviluppo (R&D) interni e le partnership con le università diventano ormai insufficienti.

Per comprenderlo basta andare a leggere i recenti dati su *crunchbase.*

Crunchbase è una base dati gestita da TechCrunch riguardante molte fra le *startup* più importanti a livello mondiale; i cambiamenti di questo database sono sempre analizzati da un moderatore prima di essere accettati ed i dati sono sempre rivisti dagli editori per assicurare che siano aggiornati. (TechCrunch) Lo stesso D'Adda la definisce come "*la bibbia online sull'innovazione e le operazioni di Venture Capital per osservare alcuni dati interessanti*". (D'Adda, 2017)

I dati di cui si è fatto riferimento poche righe più sopra affermano:

1) Amazon ha effettuato quattro acquisizioni nel 2016 ed una ad inizio 2017;
2) Google ha effettuato diciassette acquisizioni solo nel 2016 ed una ad inizio 2017;
3) Apple ha effettuato ben otto acquisizioni nel 2016 ed una ad inizio 2017;
4) Facebook ha effettuato sei acquisizioni nel 2016.

In sostanza non importa quanto il reparto interno di "ricerca e sviluppo" delle imprese sia forte, il mercato richiede alle aziende di fare degli acquisti esterni che non derivino,

quindi, da partnership accademiche e da studi interni. Gli acquisti in questione possono essere di natura tecnologica, possono essere competenze oppure brevetti. Questo modello è chiamato "*open innovation"* ed è un fenomeno ben appurato nelle parti della Silicon Valley e che pian piano sta prendendo piede non solo in diversi paesi, ma anche in diversi ambiti.

Uno di questi ambiti è certamente quello assicurativo. Allianz ed AXA, per citarne due, sono alcuni big del settore assicurativo in Europa ed hanno costituito dei fondi di venture capital per investire nelle *insurtech*, startup ad altro contenuto tecnologico ed innovativo che operano appunto nel settore citato sopra. Ovviamente non basta l'acquisizione di una di queste startup per innovare un'impresa: è, nei fatti, compito del management internalizzare queste imprese mantenendo la natura innovativa di queste. Il compito non è facile come sembra per via dei modelli tradizionali organizzativi che di certo non facilitano il dialogo e l'innovazione digitale.

Customer centric.

È necessario per tutte le imprese di questo secolo concentrarsi in maniera ossessiva sul cliente. Ciò è normale per i tempi in cui viviamo dato che la clientela oggi è abituata ad avere tutto, subito (o comunque nel minor tempo possibile), al miglior prezzo possibile. Inoltre si deve anche considerare che il web permette di acquistare un determinato bene o servizio sempre ed ovunque.

Questo porta le imprese a cercare di capire come offrire la miglior esperienza ed il miglior livello di servizio al cliente. Tale visione della clientela è vera per tutti i settori di mercato.

Le grandi aziende del 21° secolo si concentrano in maniera maniacale su questo aspetto e due dei molteplici esempi che possono essere fatti sono il già citato Amazon e Uber, startup che fa concorrenza ai classici taxi e che di recente ha sollevato non pochi dibattiti. Entrambe le imprese hanno un ottimo livello di *user experience*.

Le caratteristiche che sono necessarie per una buona *user experience* sono:

1) Velocità, il cliente digitale è un cliente che non ha voglia di perdere tempo;
2) Informazione, il cliente non vuole sorprese, soprattutto spiacevoli; vuole poter controllare la posizione del pacco, controllare le recensione sull'autista che verrà a prenderlo oppure le recensioni della cucina da cui ha ordinato il suo pasto;
3) Praticità, il cliente è contrario alle perdite di tempo inerenti ai pagamenti e perciò per facilitare il tutto numerose aziende permettono il pagamento tramite la carta che sarà memorizzata nell'account del cliente.

Ovviamente anche i players tradizionali si muovono in questa direzione, come è naturale che sia. Le dichiarazioni di Mark Parker, CEO di Nike, ci permettono di capire ancora meglio ciò. Il sessantaduenne ha infatti affermato: *"Il digitale ci permette di approfondire la relazione che abbiamo avviato con i consumatori rendendola ancor più su misura rispetto ai loro bisogni".*

Nike si è infatti mossa creando un intero ecosistema digitale, chiamato "*Nike+"*: si è andati oltre il singolo prodotto e grazie alla partnership con Apple il brand sportivo statunitense è più vicino al cliente, a differenza di altre imprese o settori dove la logica del prodotto è ancora ben radicata e non viene data grande importanza alla figura del consumatore ed alla relazione che può essere instaurata con esso.

Datacentric.

Sebbene questo argomento sarà trattato in via più amplia nel capitolo successivo è bene anticipare quella che, probabilmente, è la caratteristica più importante che deve avere un'impresa nell'era digitale.

È normale amministrazione quindi per un'azienda lavorare e consumare una mole gigantesca di dati che poi saranno utilizzati per migliorare, innovare e, se necessario, ripensare il proprio modello di business. Una delle companies che è possibile prendere ad esempio come utilizzatrice e consumatrice di enormi quantità di dati è Amazon, passata da essere un puro *retailer* online ad una delle più grandi compagnie di Big Data nel mondo.

I passi principali che ha seguito il colosso statunitense, modello per altre imprese, sono i seguenti:

1) Offerta di un catalogo online almeno dieci volte più grande rispetto a quello di un competitor fisico con i prezzi inferiori al 10%;
2) Creare una community di blogger o acquirenti che valutino i prodotti offerti, il comportamento dell'utente (serie storica degli acquisti, interazione nella piattaforma web, *etc…)* ed i dati generati dal network "collaborativo" della community permettono un altissimo livello di personalizzazione nel suggerimento dei prodotti da comprare anche sotto forma di bundle;
3) Un corretto utilizzo dei dati generati per aumentare l'esperienza d'acquisto per il cliente ed il *customer care*, quello di Amazon è attualmente il migliore al mondo, facendo accedere i dipendenti alla *knowledge base* aziendale per assistere nel migliore dei modi i consumatori che richiedono assistenza (tramite mail, telefono o chat) affinché sia possibile dare la risposta più precisa e soddisfacente possibile;
4) Apertura dei propri servizi e gli algoritmi di big data alle altre aziende, ciò può risultare utile ai piccoli distributori che potrebbero così riuscire a capire meglio i bisogni ed i comportamenti dei consumatori, tutto questo può avvenire tramite AWS, il più grande servizio di *cloud computing* e *storage online* del mondo.

La suddetta caratteristica ovviamente può e deve essere ampliata anche alle imprese tradizionali che cercano di essere al passo con i tempi. Come esempio può essere preso in considerazione Ford che ha scommesso su questa transizione prima utilizzando i dati per migliorare la gestione della *supply chain*, in seguito anche per disegnare nuovi modelli di auto ed ora per reinventare il proprio modello di business. Nelle ultime presentazioni il top management di Ford ha sottolineato, infatti, come la *connectivity* sia alla base del futuro dell'azienda.

Ovviamente bisogna sottolineare il fatto che lo studio dei dati comporta anche l'assunzione di alcuni rischi da parte del management dell'impresa: un player digitale deve saper prendere delle decisioni sulle evidenze mostrate dai dati stessi anche se questi portino le scelte aziendali future ad essere contro il "paradigma" corrente e comunemente accettato dall'impresa. È inutile investire nelle infrastrutture e nelle tecnologie digitali, ottenere molti dati (non sempre tutti utili) ma affidarsi sempre all'esperienza passata per guidare l'azienda. (D'Adda, 2017)

In linea con quanto affermato precedentemente ormai quasi tutti i settori economici si stanno adeguando a questo nuova era del digitale. Secondo quanto riportato da *Il Sole 24 Ore* la media degli investimenti in tecnologie digitali, solo in Italia, da parte delle imprese negli anni 2015-2018 sarà del +2,4% ma alcuni settori supereranno facilmente questa percentuale. I casi in questione sono i settori della sanità (+3,6%), dei trasporti (+3,7%), energia ed utilities (+4,3%) ed infine il settore bancario, assicurativo e finanziario (+3,4%). Questi settori percorrono la via dell'innovazione digitale per non perdere posizioni rispetto ai propri concorrenti mondiali.

La situazione è differente per altri settori in cui la crescita attesa è meno incisiva rispetto ai precedenti. La pubblica amministrazione, infatti, non vedrà un aumento degli investimenti nell'innovazione digitale come nei campi elencati in precedenza, ciò è dovuto principalmente al nodo legato ai fondi: per la Difesa e le amministrazioni centrali i numeri non saranno critici, sebbene inferiori alla media, e si attesteranno sul +2% nel triennio 2015-2018; lo scenario sarà, invece, diverso per gli enti locali che, stretti dai tagli del Patto di stabilità, soffriranno una limatura negli investimenti sul digitale (-1,5%).

La maggior parte degli investimenti puntano alla digitalizzazione dei processi per migliorare e diffondere ulteriormente il rapporto con i clienti; nel mentre si assisterà all'avanzata del *cloud computing*, dei big data e delle inevitabili e indispensabili sicurezze di queste soluzioni.

In linea generale, escluse quindi le crescite previste nel suddetto triennio, vediamo come il settore delle telecomunicazioni (TLC) è il settore che investe di più nel digitale con una spesa approssimativa di 8,1 miliardi nel 2016: l'intento delle imprese operanti in questo settore è ampliare la profilazione della clientela e delle abitudini dei loro consumi.

In termini di spesa si piazza al secondo posto il settore manifatturiero. L'industria sta accelerando gli investimenti per quanto riguarda la gestione della catena di distribuzione. Tuttavia è attesa una ulteriore crescita nelle spese sul digitale per quanto

riguarda l' IoT (*Internet of Things*) che porterà ad una maggiore automazione industriale e ad una più corretta gestione di vita del prodotto.

Terzo settore per investimenti è il settore bancario e finanziario: il mondo del credito nonostante l'arrivo di player non tradizionali e competitors scomodi è pronto a migliorare l'operatività ed i servizi alla clientela. La spesa complessiva si aggirerà intorno ai 6,8 miliardi che supporteranno l'automazione delle filiali e l'ulteriore sviluppo dell'internet banking. In una situazione analoga si trova il campo assicurativo, volto a ridurre i rischi e migliorare la gestione del rischio grazie all'IoT. (Netti, 2016)

1.3 Le PMI digitali in Italia.

La digitalizzazione rappresenta una grandissima opportunità per le piccole e medie imprese italiane, permettendo loro di crescere e di guardare al futuro.

Secondo molti il digitale coinvolge sempre più le PMI nel digital marketing e le aziende che ne fanno uso sono raddoppiate dal 2013 al 2016 (dal 27% al 58%); tuttavia, non bisogna soffermarsi solo sul marketing, dato che nei dati di un'indagine Doxa per Groupon è stato evidenziato come il digitale è ritenuto fondamentale dall'81% delle PMI.

L'indagine è stata portata avanti su di un campione di novecento imprese e lo scopo era quello di capire a che punto fosse la digitalizzazione in Italia, confrontando anche i dati con quelli degli anni precedenti.

Tra i *tool* digitali a giocare un ruolo di primo piano è Facebook (89% dello sforzo di "promozione digitale") (Salerno, 2017). Di questo ne è consapevole anche Luca Colombo, country manager di Facebook, il quale però ha affermato che le opportunità del digitale e dell'industria 4.0 passano forzatamente per internet e se questo non c'è vengono a mancare anche le basi di una evoluzione dell'industria italiana; bisogna concentrare le proprie energie sulla connettività e perciò sull'introduzione della banda larga. (Colombo L. , 2017)

L'Europa sono anni che si è mossa in questa direzione ma bisogna anche stare attenti: in Italia è già presente da anni un fenomeno di *"digital divide"*. Questo fenomeno indica il

differente utilizzo delle infrastrutture digitali all'interno di uno stesso paese: differente utilizzo che crea una marginalizzazione di alcuni territori. I dati italiani ad oggi non sono confortevoli dato che si riscontra una differenza del 12% nell'accesso a internet tra le regioni del Nord e quelle del Mezzogiorno: l'introduzione di una banda larga, se non controllata nel migliore dei modi, rischia di spingere ancor più nella deriva aree che a malapena possono contare sulla connessione di base. Sarebbe, quindi, opportuno che la Commissione europea valuti l'accesso ad internet non tanto per cittadini raggiunti, è ovvio che nelle grandi metropoli (in Italia parliamo di città del calibro di Roma e Milano) sarà più facile raggiungere gli utenti, quanto più per le aree raggiunte. (Monti, 2016)

Nonostante la consapevolezza delle imprese sull'importanza del web, la percentuale di imprese che hanno un sito internet è rimasta invariata dal 2013 al 2016: parliamo del 63% circa. Nonostante il 50% degli imprenditori ritiene che un approccio digitale riesca a influenzare maggiormente i clienti, nei dati si riscontra che una strategia digitale porti solamente, in media, il 28% di nuovi clienti. La situazione delle PMI italiane per quanto riguarda il digitale è sicuramente in netto sviluppo ma è ovvio che ci siano ad oggi delle forti barriere ancora da abbattere: il 48% degli intervistati dichiara di non sentirsi a proprio agio con gli *online tools* mentre il 98% delle PMI che non sono ancora online preferiscono avere un rapporto diretto con i clienti. (Salerno, 2017)

La discriminante, secondo questa indagine, nell'evoluzione delle PMI è data dal divario generazionale fra diversi imprenditori, dove gli anziani sono i più restii all'utilizzo di nuove tecnologie a differenza dei più giovani. Questo è quanto dichiarato dal research executive di Doxa, Sara Silvestri, che aggiunge in seguito: "[…] non è ancora partita in Italia una fase di digitalizzazione concreta ed effettivamente applicata al business, a causa di barriere culturali ancora radicate e di scarsa conoscenza degli strumenti del mondo digitale." (Salerno, 2017)

Il report Senaf presentato a Marzo 2018 all'inaugurazione di MECSPE di Parma ha evidenziato come su un campione di 253 aziende del settore della meccanica il 51,4% di esse ha consapevolezza delle opportunità che la tecnologia presenta sul mercato; una percentuale simile di imprese si autodefinisce innovativa. Le aree più digitalizzate sono quella inerente ai canali di vendita e alle relazioni con i clienti, seguita dall'area della

progettazione e dello sviluppo ed, infine, l'area della relazione con il fornitore. (Bacchetti & Zanardini., 2018)

Per favorire le imprese a digitalizzarsi sono anche state poste delle agevolazioni dal Piano Nazionale "Industria 4.0", come l'iper ammortamento dei macchinari funzionali alla digitalizzazione: questo ha il ruolo di incentivare e supportare le imprese che investono in beni immateriali (sistemi IT e *software*), beni materiali e beni strumentali nuovi, funzionali alla trasformazione tecnologica e digitale dei processi produttivi; comporta una supervalutazione del 250% degli investimenti nei beni precedentemente elencati e possono accedervi tutti i soggetti titolari di reddito d'impresa. (Ministero dello Sviluppo Economico, 2017)

Dati importanti sono riscontrabili anche per quanto riguarda la formazione interna del personale, il 63% delle imprese dedica più di dieci ore a dipendente, questo anche per contrastare i rallentamenti di questa evoluzione che possono essere dovuti alle poche competenze interne e alla poca digitalizzazione delle imprese con le quali si collabora. Secondo il parere della maggior parte degli intervistati chi guida questa innovazione digitale è l'imprenditore (il 55,2% degli intervistati ha risposto in tal modo), seguito dal direttore IT/responsabile dei Sistemi Informativi (38,7%). Questa figura, in effetti, ha ricoperto un ruolo di notevole importanza a partire dagli ultimi anni, soprattutto nelle piccole e medie imprese del settore meccanico: gli investimenti nella sicurezza informatica, nei *cloud* e nella connettività sono aumentati e sono destinati a salire ancor di più[1]. (Redazione QuiFinanza, 2018)

Riprendendo gli studi di Zanardini e Bacchetti sull'industria 4.0 nel campo manifatturiero possiamo generalizzare affermando che sono presenti sei cluster i quali possono essere ottenuti incrociando le tecnologie conosciute dalle imprese con quelle effettivamente applicate da esse.

[1] Quanto scritto è tratto da un articolo della redazione di Qui Finanza, disponibile al seguente indirizzo: *https://quifinanza.it/pmi/industria-pmi-trasformazione-digitale-in-italia/179974/*

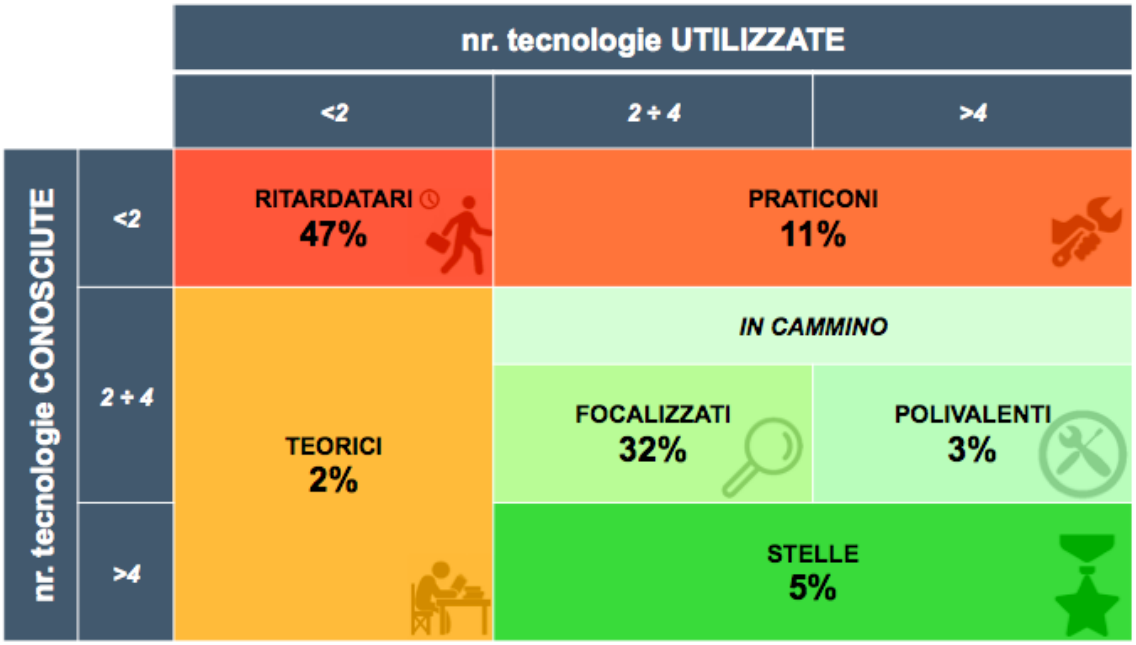

Tabella 1. Rappresenta le aziende e la loro categoria in base alle tecnologie conosciute ed a quelle utilizzate. (Fonte: https://www.agendadigitale.eu/industry-4-0/aziende-industry-4-0-italiane-quali/)

Dalla tabella sovrastante possiamo, quindi, già vedere quali sono le categorie che definiscono le imprese secondo questo incrocio:

1) I ritardatari, sono le aziende più lontane dal modello dell'industria 4.0 e riluttanti ad un grande utilizzo della tecnologia;
2) I praticoni, le aziende che hanno deciso di lanciare almeno due progetti pilota con l'utilizzo di nuove tecnologie;
3) I teorici, aziende che approcciano quasi tutte le tecnologie disponibili senza però aver implementato seriamente alcun progetto;
4) I focalizzati, queste aziende stanno seguendo il "cammino" verso Industria 4.0 pur facendo ricorso ad una gamma limitata di tecnologie che utilizzano;
5) I polivalenti, simile alla categoria precedente ma a differenza di quest'ultima utilizzano un maggior numero di tecnologie, consapevoli del fatto che devono saper impiegare tutte le tecnologie a disposizione in maniera armonica;
6) Le stelle, sono i modelli ai quali ispirarsi lungo il percorso della digitalizzazione, conoscono ed impiegano tutte le tecnologie digitali con benefici concreti.

Le percentuali evidenziate nella tabella di cui sopra si riferiscono a quante delle 105 imprese tenute come riferimento stanno muovendo dei passi concreti verso il paradigma 4.0: solo il 35% è già in cammino.

Secondo quanto scritto dai due ricercatori, percorrere la strada che porta alla digitalizzazione: *"[...]vuol dire applicare in modo pervasivo all'interno dei propri processi diverse tecnologie digitali, in grado di comunicare e scambiare dati e informazioni per prendere decisioni rapide e consapevoli, gestire in tempo reale cambiamenti improvvisi del contesto, essere flessibili nell'applicare le modifiche necessarie, nonché garantire livelli di efficienza e sostenibilità (sempre più) elevati."* (Bacchetti & Zanardini., 2018)

Non basta, perciò, adottare solamente una o due tecnologie innovative per rispondere a specifiche esigenze di singoli reparti o aree di business senza una vera interconnessione: questo è l'avvertimento dei due studiosi dei laboratori RISE. Inoltre è emerso che le imprese maggiormente informatizzate e sempre all'avanguardia da un punto di vista storico sono quelle più orientate al paradigma 4.0.

Quindi ciò che viene messo in evidenza da questo studio è che le dimensioni contano: di fatti le categorie più lontane dall'industria 4.0 (Ritardatari, Praticoni e Teorici) sono per il 75% PMI che quindi appaiono meno pronte alla trasformazione sia in termini di risorse investibili che in termini culturali.

Si veda il grafico seguente.

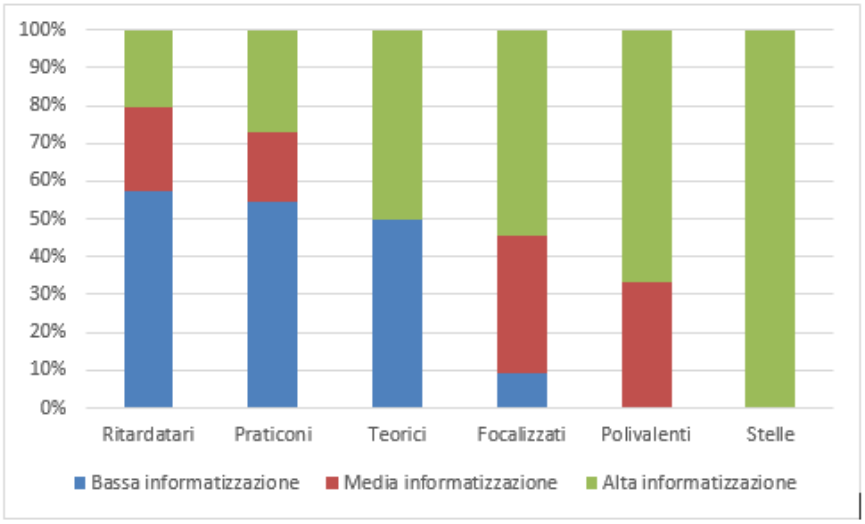

Grafico 1. Rappresenta come l'alta informatizzazione porti le aziende ad utilizzare tutte le tecnologie a loro disposizione e conosciute, nonché il livello di maturità digitale delle imprese. (Fonte: https://www.agendadigitale.eu/industry-4-0/aziende-industry-4-0-italiane-quali/)

L' "ordine" di innovare, soprattutto nei casi di imprese medio-piccole, proviene direttamente dal vertice aziendale con un classico "*top-down*". Di fatti le innovazioni hanno, ovviamente, un impatto sulle tecnologie utilizzate e per forza di cose sul modo di lavorare, delle imprese e delle persone, ed è perciò ragionevole che questo "comando" provenga dalle parti alte dell'azienda, vincendo così le eventuali resistenze iniziali al cambiamento e definendo subito la nuova identità dell'impresa. Nel 60% dei casi accade così. In un altro 20% questo cambiamento è affidato totalmente ai capi funzione ed in un altro 20% il ruolo è affidato all'area IT ed ai loro responsabili.

Una volta determinata l'innovazione verso la quale si intende procedere e perciò la nuova identità aziendale è lecito domandarsi a chi spetterà, dunque, la *governance* di questi progetti di innovazione digitale.

Secondo il campione preso come riferimento dai due studiosi del laboratorio RISE di Brescia non tutte le aziende, nemmeno il 35% in cammino verso Industria 4.0, hanno una figura *ad hoc* che si dedica a tempo pieno all'innovazione: solamente il 15% delle imprese intervistate ha, infatti, una figura che si dedica a tempo pieno in questo compito; in un altro 35% dei casi questa figura coincide con quella di un

process owner che però ci si dedica solo in via parziale. La restante parte (50%) non ha alcun dipendente adibito a tale ruolo.

La volontà di cambiare quindi deve venire da una figura di alto rilievo o proprio dal vertice aziendale: questa figura deve essere in grado di tracciare una *vision* e guidare il personale verso il conseguimento dell'obiettivo prefissato.

L'intera organizzazione aziendale deve abbracciare le nuove tecnologie ed il paradigma 4.0, a fronte della persona-guida decisa e sicura. Sarà necessario rivedere i processi ed i ruoli dei vari dipendenti e probabilmente anche riqualificare le competenze di quelle risorse che non risultano essere in linea con le nuove tecnologie.

Per far sì che l'impresa sia al passo con i tempi è, quantomeno, necessario che il percorso di adeguamento sia stato già intrapreso in modo tale che gli sforzi debbano essere meno intensi e le tempistiche meno lunghe. È bene, dunque, che l'azienda sia dotata di processi adeguatamente informatizzati e integrati tra di loro.

È impensabile, infatti, connettere personale, stabilimenti differenti, linee produttive, attrezzature, intere filiere logistiche e coordinarne le attività in maniera armonica, senza che nessuna di queste attività sia stata sufficientemente e adeguatamente informatizzata in precedenza.

Quindi, per concludere è bene dire che il percorso verso il paradigma 4.0 non è un'autostrada che può essere percorsa al massimo della velocità.

Sono presenti, in sostanza, numerosi cambiamenti di diversa natura e di diversa entità, tutti da integrare in maniera armonica e, soprattutto, graduale. (Bacchetti & Zanardini., 2018)

Di fatti il Piano Nazionale "Industria 4.0", lanciato dal MISE nel 2016, cerca di non far pesare eccessivamente questa rivoluzione digitale alle imprese e affianca loro altri due soggetti fondamentali: i *Competence Center* ed i *Digital Innovation Hub* (DIH).

I primi sono poli di ricerca e innovazione legati alle aziende e alle università, in grado di fornire competenze e "*facilities"* sulle tecnologie in vista di industria 4.0; sono frutto di partenariati pubblico-privato tra uno o più centri di ricerca o università e una o più imprese. Proprio queste strette interconnessioni tra le università, perciò la ricerca, e le imprese, quindi il lavoro, può dar forma a quella che sarà la fabbrica del futuro in versione "*research factory"* distribuita: un luogo che va oltre i confini fisici dove manifattura e ricerca si uniscono. Sono già tante le eccellenze universitarie che hanno avanzato proposte per la creazione di un Competence Center.

I DIH *"collaborano con i Competence Center e forniscono servizi alle imprese valorizzando i vari attori dell'ecosistema dell'innovazione digitale"*. Questi hanno una dimensione regionale o interregionale e non sono previsti fondi pubblici nazionali per la loro costituzione; per sostenersi devono far leva infatti su risorse regionali derivanti da fondi regionali europei e dai fondi interprofessionali. È fondamentale ai fini della riuscita della loro *mission* la partecipazione di potenziali investitori come i *venture capital*, le banche e le fondazioni. (Pepe, 2018)

CAPITOLO 2: "I DATI: L'ORO MODERNO".

2.1 I Big Data: definizione e importanza dei dati.

La prima domanda che è opportuno porsi è la seguente: cosa sono i Big Data?

Come il nome lascia di per sé intuire i Big Data sono volumi molto grandi di dati possano essi essere strutturati, come i database per esempio, oppure non strutturati, quindi si intendono immagini ed email. Questi dati, come già sottolineato in precedenza, interessano in particolar modo alle imprese. Le ultime hanno un particolare interesse nel modo in cui i dati collezionati saranno poi utilizzati: vengono costruiti degli appositi algoritmi che studiano delle molteplici variabili in poco tempo con poche risorse computazionali. Da questi studi, successivamente, verranno prese delle decisioni che hanno il compito di implementare il modello di business dell'azienda. Inoltre possono essere utilizzati anche per analizzare altri aspetti importantissimi come la riduzione dei costi, quella dei tempi o la creazione di offerte mirate per i clienti. Attualmente il più evidente e noto utilizzo di questi strumenti viene effettuato per permettere alle aziende di capire in anticipo i futuri acquisti della clientela: questo è possibile poiché vengono studiati gli oggetti comprati in precedenza sul sito in questione oppure il tempo di permanenza in determinate pagine del catalogo online.

Tutto ciò è noto ormai da tempo e l'importanza che ricoprono questi strumenti per le imprese fu ripresa da Umberto Rapetto in un articolo per il Sole 24 Ore in cui scrisse: *"[…]Le informazioni che riguardano ciascuno di noi sono la linfa del business perché consentono di calibrare la produzione industriale, orientare gli sforzi commerciali, individuare le tendenze al consumo e tener d'occhio gusti e mode. Chiunque voglia metter sul mercato prodotti e servizi considera i dati personali una bussola e guarda con interesse chi ne macina per via telematica enormi quantità procedendo anche a selezioni e aggregazioni. […]"* (Rapetto, 2012)

Questi Big Data sono ormai utilizzati in numerosi settori. Di seguito verrà fatto qualche esempio. (Mangia, 2016)

1) Settore bancario, ogni giorno le banche si interfacciano con una mole di dati non trascurabile e perciò nasce in loro la necessità di organizzarli in maniera

differente. Proprio per questo motivo i Big Data in tale settore vengono utilizzati per capire al meglio le preferenze dei clienti, aumentare la loro soddisfazione e ridurre al minimo i rischi legati alle frodi o alle transizioni.

2) Settore sanitario, in questo campo è opportuno che il tutto sia fatto nel modo più veloce possibile, oltre che in maniera trasparente. Se i Big Data sono organizzati in maniera efficiente gli operatori del settore possono analizzare in maniera ancor più accurata la storia del paziente migliorando le cure dello stesso.
3) Settore scolastico, i Big Data possono avere un impatto notevole nel sistema scolastico dato che sarà possibile valutare quali sono gli studenti a rischio e quali sono, invece, quelli che stanno facendo degli adeguati progressi. Il tutto faciliterà anche le esaminazioni del curriculum degli alunni.
4) Settore dell'industria retail, questo è senz'altro l'esempio più evidente dato che i *retailer* hanno bisogno dei dati dei loro clienti per migliorare il commercio dei loro prodotti e, possibilmente, "riportare indietro" i clienti che nel tempo sono andati perduti.

Queste enormi quantità di dati sono spesso definiti dalle cosiddette "tre V": Velocità, Volume e Varietà.

La prima fa riferimento alla velocità con cui i dati vengono generati e poi trasmessi: bisogna essere consapevoli del fatto che oggigiorno questi vengono trasmessi con una scioltezza inimmaginabile e perciò devono essere anche trattati con altrettanta sveltezza. Come detto in precedenza gli elementi analizzati dalle imprese possono essere di natura strutturale o non strutturale: è bene, dunque, che le aziende siano pronte a lavorare con una grande varietà di dati. Infine, il volume: in passato immagazzinare ed avere accesso a così tanti dati sarebbe stato stato irrealizzabile ma ciò è stato reso possibile grazie ai vari servizi di *clouding* ed alla virtualizzazione che hanno facilitato i processi di raccolta. (Mangia, 2016)

Il mercato dei Big Data sta crescendo con il tempo e in Italia nel 2016 aveva un valore complessivo di 183 milioni di euro secondo quanto scritto dall'osservatorio della digital innovation del politecnico di Milano. Per forza di cose, quindi, anche le figure legate a questi iniziano ad emergere ed i profili più richiesti dalle imprese sono fondamentalmente quattro secondo un articolo di Laura Zanotti:

1) Data Architect, progetta i sistemi dei dati;
2) Data Scientist, analizza il valore dei dati raccolti con l'utilizzo di algoritmi sempre più complessi;
3) Data Engineer, sviluppano prodotti di scouting o di analisi molto specifici e sono in grado di identificare le soluzioni basate sui dati;
4) Business Translator, figure che dispongono sia competenze tecniche che competenze relative al business in cui operano. (Zanotti, 2017)

Quanto detto nelle ultime righe ci permette di capire che, sostanzialmente, i big data altro non sono un insieme di dati dormienti e disordinati all'interno di una impresa e queste figure, o addirittura alcuni programmi ed algoritmi, sono necessari per ordinarli ed interrogarli fornendo alle aziende le previsioni richieste per il futuro.

Le imprese più avanzate in termini digitali e tecnologici ormai non utilizzano più alcune delle personalità precedentemente accennate per via del fatto che è possibile direttamente "istruire" per esperienza i computer grazie ad un particolare metodo di analisi dei dati chiamato *machine learning.*

Questo insegna alle macchine a svolgere dei compiti per cui non sono state programmate, con il tempo, proprio come un bambino, l'oggetto sarà in grado di svolgere compiti man mano più difficili.

L'esempio più utilizzato tra gli addetti ai lavori per spiegare il *machine learning* è il cosiddetto "esempio del cane e del gatto": in questo caso l'utente pretende che il proprio computer riconosca la differenza tra un cane ed un gatto e per consentire ciò fornisce alla macchina le coordinate necessarie per cogliere la differenza tra i due animali. È giusto porsi come domanda che ruolo abbiano i big data i tutto ciò. Per semplificare al massimo questo esempio si pensi al fatto che i dati posseduti sono l'esperienza del computer e colleghiamo a ciò le immagini dei due tipi di animali sul computer. A questo punto subentrano i big data: più dati avrà il computer (perciò più sono varie le fonti dei dati stessi), nel caso preso ad esempio più immagini si avranno, più sarà possibile "allenarlo" a carpire le differenze nella maniera più accurata. Gli algoritmi, i procedimenti di calcolo che permettono di separare i cani ed i gatti, rappresentano

l'intelligenza del computer: sarà infatti possibile alla macchina classificare una grande quantità di informazioni per arrivare a differenziare cani e gatti.

L'esempio fatto in questo caso è ovviamente molto semplice e volutamente banale, nei fatti il *machine learning* permette al computer di svolgere in meno tempo compiti che per l'uomo sarebbero complicati o ripetitivi ed è quindi fondamentale per un'impresa odierna dotarsi di queste tipologie di processi.

In molti si sono soffermati sull'importanza di questo argomento dato che per anni una buona *business analytics* ha rappresentato la fonte di un vantaggio competitivo per le imprese dato che dall'analisi si poteva ricavare il valore dei dati che poi sarebbe andato ad aumentare l'efficienza aziendale (accennato anche in precedenza) o ad aumentare le entrate monetarie dell'azienda in questione. Il *machine learning* permette difatti di apprendere in continuazione dai dati e di cogliere informazioni nascoste e sconosciute, estraendo del valore da essi anche se inizialmente (come già affermato) le macchine non erano programmate per farlo.

Secondo una indagine portata avanti in tutta Europa da IDC (International Data Corporation), società statunitense fondata nel 1964 e specializzata nelle ricerche di mercato nell'ambito di IT e di innovazione digitale, molte aziende concedono una grande attenzione all'AI e al *machine learning* nel contesto dell'operatività aziendale.

Tante delle aziende prese a riferimento per l'indagine erano italiane e i dati emersi sono i seguenti: il 40% di queste imprese del Bel Paese si aspettano che già dal 2018 queste nuove tecnologie possano avere un impatto significativo nel modo di fare business; il 32% delle aziende crede che i risultati saranno evidenti intorno al 2020-2021 e perciò tra circa due anni; solo il 12% degli intervistati afferma che l'impatto di queste tecnologie sarà chiaramente visibile non prima del 2022, se non addirittura 2024, quindi si parla di un arco di tempo che oscilla dai tre ai cinque anni; per concludere, il 16% delle imprese è convinta del fatto che gli impatti sul business saranno poco evidenti nel

breve periodo e la loro importanza inizierà ad assumere valore non prima dei cinque anni[2]. (Redazione TechEconomy, 2018)

2.2 Ottenimento del valore per le aziende dai Big Data e Big Data Analysis.

Dopo una visione sul significato del concetto generale di Big Data è opportuno stabilire la finalità di questa analisi di dati: sebbene sembri scontata molte volte non lo è.

Se lo scopo per il quale viene effettuato lo studio di questi elementi non risulta essere ben specificato il rischio che si corre, molto elevato, è quello che il CIO (chief information officer) e l'IT vadano avanti per la loro strada realizzando una Big Data architecture eccellente ma non allineata ai bisogni aziendali[3]. (Redazione ZeroUno, 2017)

Secondo quanto dichiarato da alcune aziende durante un sondaggio del 2015 a *Forrester*, compagnia specializzata nelle ricerche e nei sondaggi fondata nel 1983 negli USA, i casi di utilizzo della Big Data Analysis rientrano in tre gruppi principali. (Forrester's Global Business Technographics Data And Analytics Survey, 2015)

Il primo è il gruppo denominato "conoscenza e servizio clienti": è noto da tempo, infatti, che le analisi dei dati vengono effettuate per lo sviluppo dei prodotti, dei progetti di marketing e vendite oppure per l'ottimizzazione della digital experience. Tutto ciò è stato anche evidenziato nel precedente paragrafo essendo, con molte probabilità, uno dei motivi principali dell'utilizzo della Big Data Analysis.

Nel secondo raggruppamento troviamo la "sicurezza ed altre performance applicative". Per prevenire i problemi nell'erogazione dei servizi e monitorare gli eventi in modo tale da avere una flessibilità che permetta una risposta in tempi quasi immediati sono utilizzate la *predictive anaytics* e l'analisi dei big data sul funzionamento dell'IT. I

[2] Quanto scritto è tratto da un articolo della redazione di TechEconomy, disponibile al seguente indirizzo: *https://www.techeconomy.it/2018/07/24/cambiano-le-imprese-machine-learning-analytics/*

[3] Quanto scritto è tratto da un articolo della redazione di ZeroUno, disponibile al seguente indirizzo: *https://www.zerounoweb.it/analytics/big-data/come-fare-big-data-analysis-e-ottenere-valore-per-le-aziende/*

modelli di analisi vanno ovviamente discussi con i responsabili della sicurezza e dei servizi. Questi modelli si serviranno verosimilmente dei data-log generati da server e dispositivi di rete per valutare il livello delle prestazioni.

Il terzo ed ultimo gruppo è "efficienze e rischi operativi". Il rischio finanziario è qualcosa di molto importante per le aziende, soprattutto nei tempi recenti e gran parte degli esempi di Big Data Analytics realizzati hanno il compito di ridurre proprio questa tipologia di rischio. L'efficienza e la *risk reduction* non sono fondamentali solo in questo campo, nei fatti ricoprono una notevole importanza anche nella gestione del personale, in quella della supply chain e nell'asset management. Un approccio globale a questi problemi deve considerare lo scambio di idee con i business partner, la condivisione dei dati all'interno dell'azienda nonché il tracciamento dei risultati utili avuti dopo l'applicazione delle azioni successive allo studio di questi dati.

In seguito sarà presentato un grafico che presenta tutte le voci, le quali ovviamente appartengono alle tre macrocategorie appena citate, che rappresentano i casi di utilizzo dei Big Data.

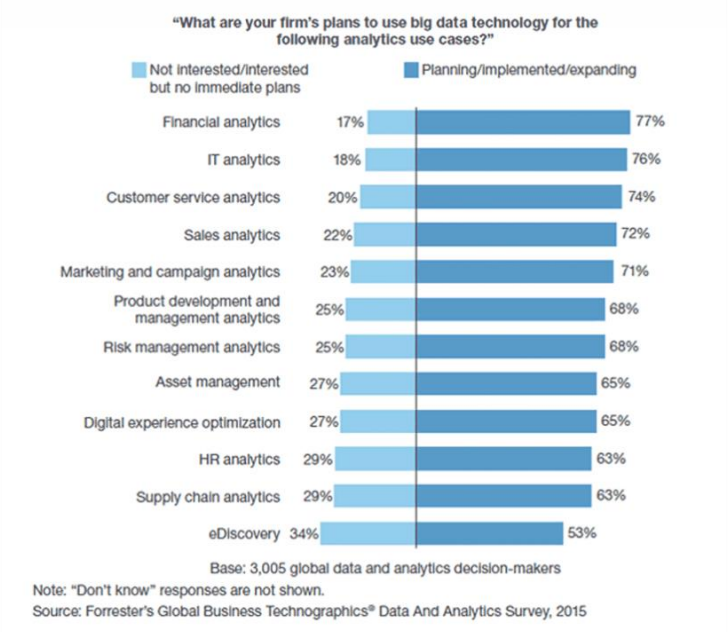

Grafico 2. Casi di utilizzo dei Big Data nelle aziende. (Fonte: Forrester's Global Business Technographics Data And Analytics Survey, 2015; disponibile anche su https://www.zerounoweb.it/analytics/big-data/come-fare-big-data-analysis-e-ottenere-valore-per-le-aziende/)

Ovviamente dopo un'attenta analisi dei dati è necessaria anche una buona gestione di essi. Il *Data Management* negli ultimi anni ha assunto un ruolo di rilievo nelle aziende ed è, perciò, necessario tener conto di alcune vitali considerazioni che devono essere valutate come priorità per una ottimale gestione dei Big Data. Queste ultime sono fondamentalmente quattro.

Innanzitutto è fondamentale per le imprese assumere una logica di *continuous improvement* ("miglioramento continuo") e quindi identificare tutte le nuove fonti di dati e incorporarle nel Data Management. Ciò è necessario dato che le fonti di Big Data continuano ad evolversi e crescere: queste sono generate non solo da *app* interne all'impresa ma anche da risorse pubbliche, come possono essere tutti i social media, piattaforme mobile ma anche, sorprendentemente, dai sensori (*Internet of things)* che possono essere trovati all'interno, per esempio, di alcuni store.

Da qualche anno, inoltre, è possibile mantenere i dati catturati a basso costo grazie a tecnologie come *Apache Hadoop*, cosa impensabile fino a poco tempo fa. È necessario, quindi, che l'impresa ottenga quanti più dati possibili e li immagazzini, dato che è difficile valutare a priori la loro utilità soprattutto poi se depauperati dal contesto. Una volta disponibili e contestualizzati è doveroso trarre un significato da essi.

Dopodiché, come è normale che sia, bisogna analizzare in via scientifica i dati ottenuti per arricchirli di senso "utile" e non "ovvio": l'obbiettivo dei progetti di Big Data analytics è vedere come quanto accaduto possa aiutare a prendere decisioni per il futuro, sia immediato che non. È possibile optare per differenti approcci: i cosiddetti approcci "descrittivi" (*descriptive analytics),* i quali permettono grazie all'uso di appositi strumenti orientati di descrivere la situazione passata e attuale dei processi aziendali e delle aree funzionali ed inoltre di visualizzare questi dati in maniera sintetica e grafica; approcci "predittivi" *(predictive analytics),* sono strumenti che utilizzano tecniche matematiche come la regressione e modelli predittivi per analizzare i dati e "rispondere" a domande inerenti gli scenari futuri aziendali; approcci "prescrittivi" *(prescriptive analytics),* ossia sfruttano applicazioni avanzate della Big Data analytics per poi generare delle *insights,* conoscenze utili ai fini del processo decisionale sulla base delle analisi svolte. L'Osservatorio Big Data Analytics & Business Intelligence del Politecnico di Milano nel 2016 ha effettuato una ricerca per notare come questi

differenti approcci fossero diffusi nel panorama italiano. La sintesi della ricerca è che le grandi imprese ormai utilizzano moltissimo queste analisi dei dati a differenza delle piccole e medie imprese. Entrando più nello specifico è possibile affermare che la *descriptive analytics* è presente nell'89% delle organizzazioni tenute in considerazione per la ricerca, la *predictive analytics* è l'area che suscita, ad oggi, maggior interesse nell'ambito della gestione dei Big Data (diffusione pari al 59%) sebbene il suo uso non sia ancora ben radicato nelle aziende come nei fatti accade per l'approccio descrittivo. La *prescriptive analytics* è ancora poco presente nelle imprese e, nel caso lo fosse, si limita ad esserlo a livello pilota. Per quanto riguarda le PMI lo scenario cambia drasticamente: solo un'azienda su tre utilizza un approccio descrittivo e nella maggior parte dei casi questa è di media dimensione; l'utilizzo dei modelli *predictive* è ancora limitato a poche organizzazioni mentre quello *prescriptive* è, ancora, per lo più sconosciuto. Nel 2016 in Italia la spesa per l'*analytics* da parte delle imprese, sia grandi che medio-piccole, è stata di 905 milioni di euro come è possibile vedere dal grafico sottostante. (Fabbri, 2017)

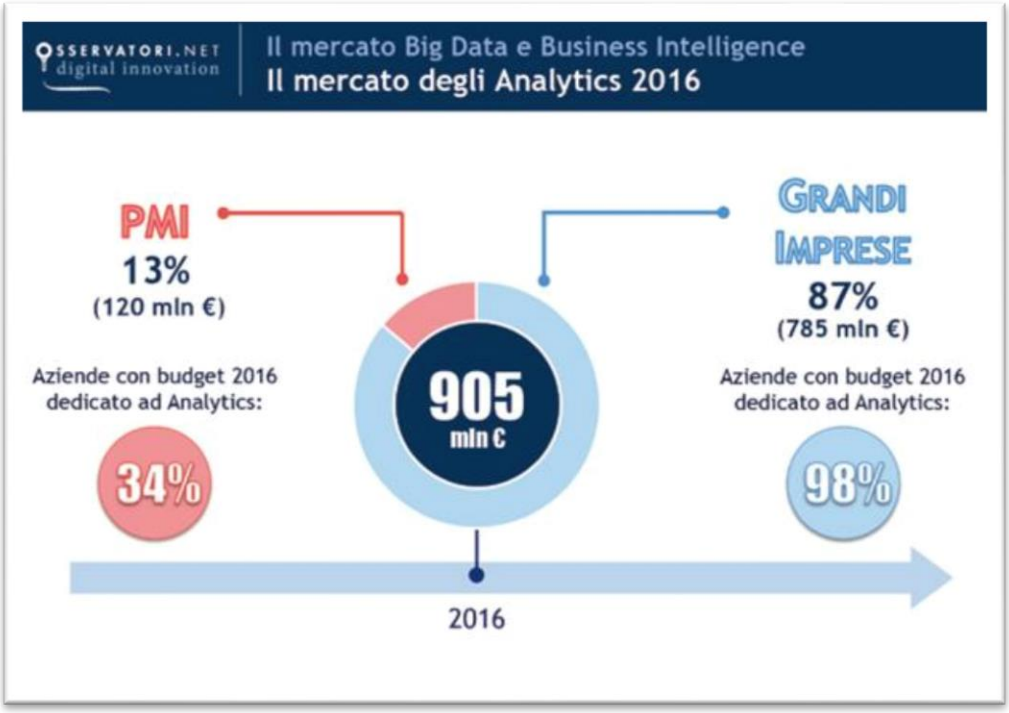

Grafico 3. **Indica le spese delle imprese (PMI e grandi imprese) in Big Data e Business Intelligence nel 2016. (Fonte:https://www.digital4.biz/marketing/big-data-e-analytics/big-data-cosa-sono-e-perche-grazie-alle-analitiche-il-business-continua-a-crescere/)**

Riuscire ad utilizzare i precedenti approcci richiede nuove, determinate, competenze: queste sono possedute dai *data scientist* (figure viste anche in precedenza) che con l'utilizzo di determinati algoritmi, *machine learning algorithms*, possono generare informazioni utili che favoriscono la competitività e la redditività aziendale.

Infine, è fondamentale liberare e rendere disponibili i dati in maniera veloce a tutti coloro che ne hanno bisogno: è necessario dotare la piattaforma di gestione dei big data di funzionalità innovative che possono rendere accessibili e disponibili i dati lungo tutti i livelli aziendali. Non è consigliabile per un'impresa, infatti, avere dei Big Data in database non condivisi e non integrabili dato che peggiorerebbe la sua efficienza[4]. (Redazione ZeroUno, 2017)

Per concludere è necessario elencare quali sono i vantaggi ai quali una buona analisi dei dati può portare.

Innanzitutto uno dei benefici può essere l'aumento del fatturato: a volte bastano i dati (giusti) sintetizzati in un'analisi quantitativa per far crescere il volume di vendite oppure per valutare la dimensione di un mercato.

Inoltre tramite la Big Data analysis si può permettere alle imprese di prevedere la domanda per i propri prodotti e servizi. Ancora meglio: l'analisi dei dati estranei alle vendite può rilevare interessi e intenti dei potenziali consumatori altrimenti non facilmente denotabili e rende possibile valutare la *"fitness"* dell'offerta, ossia il grado con cui si accoppiano le cose che già sono note sul ciclo di vita del cliente e quelle che verranno scoperte.

In terzo luogo: è possibile dare più valore all'account management ed ottimizzare il loro lavoro analizzando i dati relativi alle operazioni tra venditori e clienti ed integrandoli con ciò che l'azienda conosce del cliente al di fuori del rapporto di business (fusioni, assunzioni e finanziamenti ad esempio), focalizzando la relazione B2B (Business-to-Business) sui reciproci obiettivi.

[4] Quanto scritto è tratto da un articolo della redazione di ZeroUno, disponibile al seguente indirizzo: *https://www.zerounoweb.it/analytics/big-data/come-fare-big-data-analysis-e-ottenere-valore-per-le-aziende/*

Sempre collegato all'account management è possibile utilizzare la *big data predictive analytics* per analizzare l'enorme mole di dati interni ed esterni che si hanno sulle relazioni intrattenute con i rivenditori per essere pronti a soddisfare una loro richiesta nel minor tempo possibile o, meglio ancora, prevenirla fornendo un'offerta adatta. Ciò è, in sostanza, molto simile a quello che accade nella vendita B2C (Business-to-Consumer) per quanto riguarda le analisi marketing con le conseguenti promozioni "mirate".

Un ultimo beneficio potrebbe essere l'opportunità di apertura a nuovi business. In moltissimi casi se ne parla riferendosi alla vendita di nuovi prodotti e nuovi servizi che si intende immettere sul mercato dopo un'attenta visione dei dati. Ma questo discorso vale anche per le aziende che hanno intenzione di allargare il mercato puntando su nuovi clienti. Il caso che viene tipicamente riportato come esempio è quello dell'impresa attiva sui grandi utenti che intende rivolgersi anche alle PMI e che, perciò, dovrà elaborare un business model calibrato su di esse. (Redazione ZeroUno, 2017)[5]

2.3 Data monetization: il nostro valore ed i colossi mondiali del settore.

Come scritto in precedenza i dati ricoprono un ruolo di fondamentale importanza nelle aziende odierne ed il proseguire dell'era digitale non fa altro che aumentare la loro rilevanza: è intuibile che la compravendita delle informazioni dei clienti di una determinata compagnia è solo una parte marginale di questo business. La rivoluzione digitale, come già evidenziato prima, ha creato nuovi paradigmi e accelerato la corsa allo sviluppo di nuove tecnologie e algoritmi che rendano possibile ordinare milioni di dati, provenienti da fonti differenti, in fretta per realizzare campagne marketing sempre più mirate; dal canto loro le aziende devono essere abili nello studio di questi dati per riuscire ad influenzare le abitudini di consumo dei loro clienti o, quantomeno, prevederle recando, però, una particolare attenzione sull'utilizzo di queste informazioni. È doveroso sottolineare che è possibile cadere nell'abuso dei dati personali raccolti: ciò

[5] Quanto scritto è tratto da un articolo della redazione di ZeroUno, disponibile al seguente indirizzo: *https://www.zerounoweb.it/analytics/big-data/come-fare-big-data-analysis-e-ottenere-valore-per-le-aziende/*

potrebbe diventare ancora più grave se vi fossero di mezzo anche dei minori. (Rusconi, 2013)

Tuttavia è anche bene specificare che, almeno fino al 2013, negli USA non vigeva una vera e propria "legge guida" che riguardava questo utilizzo dei dati: erano i data broker stessi che si davano delle linee guida da rispettare come non ricavare informazioni sui minori e sulle specifiche condizioni di salute ed economiche di una persona. (Steel, 2013)

In un articolo datato 12 Giugno 2013 del Financial Times è stato dichiarato da alcune compagnie, come *LeadsPlease.com,* che lavorano nella compravendita dei dati quanto fosse il costo delle informazioni di una singola persona. È stupefacente sapere che i dati di milioni di utenti vengono venduti dalla suddetta compagnia per meno di un dollaro, più precisamente: i dati di mille persone ritenute poco influenti vengono vendute per circa mezzo dollaro (0,44 euro) mentre i dati di mille persone ritenute "influenti" costano 0,75 dollari, ossia 0,66 euro. Dave Morgan fondatore di una delle prime compagnie ad utilizzare il *web surfing data* (praticamente i dati provenienti dai siti visitati dagli utenti) per creare annunci online mirati ha dichiarato una volta intervistato: *"You're not worth much".* (Steel, 2013)

Il Financial Times stesso ha elaborato un semplice programma nel quale, immettendo alcuni dati, esce il valore effettivo delle informazioni inerenti quell'utente.

Nonostante un valore apparentemente basso, il mercato dei dati è un mercato che muove miliardi di dollari ogni anno. Uno dei colossi del brokeraggio dei dati, *Acxiom*, ha un fatturato annuo che va oltre il miliardo di dollari e possiede un database con informazioni su circa 700 milioni di persone. Queste imprese fondamentalmente si prendono la briga non solo di raccogliere questi dati ma anche di aggregarli e, soprattutto, trasformarli in un bene rivendibile sul mercato. (Rusconi, 2013)

Prende, quindi, da qui origine la cosiddetta *Data monetization*, ossia l'opportunità per alcune imprese di vendere i dati a loro disponibilità, talvolta anche "grezzi", in cambio di entrate monetarie.

Nel report annuale del 2017 l'Osservatorio "Big Data Analytics & Business Intelligence" della School of Management del Politecnico di Milano è possibile trovare scritto riguardo la *data monetization*: *"la capacità di identificare relazioni nascoste nei dati a disposizione delle organizzazioni, infatti, non consente solo di ottimizzare i processi ed aumentare la competitività, ma permette di aprire nuove opportunità di generazione di valore".* (Fabbri, 2017)

Dunque la vendita dei dati è uno dei business più importanti oggigiorno: tuttavia è da tenere bene a mente il fatto che questi scambi non vengono effettuati solo tra aziende nate proprio per questo business e terze parti. Come scritto in precedenza oggi hanno una vitale rilevanza tutte le tipologie di dati, soprattutto quelli immessi dagli utenti sui loro profili social.

Detto ciò è impossibile negare che alcuni colossi di questo settore sono Facebook, Google e Amazon. Come guadagnerebbero altrimenti?

Fare i conti diventa a questo punto molto semplice: la prima delle aziende sopracitate ha un valore che va oltre i 500 miliardi di dollari ma gli unici asset patrimoniali significativi per essa sono i dati che maneggia. (Barberio, 2018)

Per quanto riguarda le altre due potenze assolute di questo business:

- Amazon, numero uno mondiale del commercio elettronico, ha basato la propria potenza proprio sulla capacità di personalizzare ogni messaggio per gli utenti dipendentemente dal numero di dati posseduti su di essi;
- Google ha, per esempio, il monopolio della pubblicità mondiale insieme a Facebook e deve oltre il 90% del suo fatturato proprio a quest'ultima. Questa posizione è stata creata grazie al possedimento, da parte del colosso americano, dei dati degli utenti che permettono l'indirizzamento personalizzato della pubblicità e del marketing online. I dati vengono raccolti grazie alle ricerche fatte sul motore di ricerca, tramite le navigazioni online più in generale, grazie al tracciamento negli smartphone con sistema operativo Android ed infine dagli account Gmail. (Barberio, 2018)

Una domanda che è lecito porsi, comunque, potrebbe essere di fatti: come fanno esattamente queste grandi compagnie, come nel caso di Google, ad avere una tale semplicità di accesso ai nostri dati?

Umberto Rapetto lo scrisse sul Sole 24 Ore nel 2012.

"La semplice connessione comporta «dichiarazioni spontanee» previste dalle procedure tecniche che sono alla base del collegamento che altrimenti non potrebbe stabilirsi. Il webmaster "dall'altro lato" vede il numero Ip del visitatore, riconosce il provider, definisce un preliminare posizionamento geografico, identifica e interpreta i "cookie" presenti sul pc, vede quale sistema operativo e quale browser sono usati dall'utente, prende nota della provenienza (da quale sito si è arrivati) e della successiva destinazione (dove si continua a navigare), scheda le ricerche che vengono effettuate e cataloga le pagine visitate, memorizza i "post" e ogni sorta di messaggio, immagazzina ogni operazione di selezione o gradimento, tiene in evidenza i contatti e ne disegna la rete.

L'insieme delle informazioni va a fare perno su una voce univoca, ovvero un codice identificativo alfanumerico che costituisce il Dna dell'utente. Attorno a questo dato si va ad aggrappare tutto quel che nel tempo è stato, viene e verrà raccolto direttamente o acquisito da terzi. Sovente gli utilizzatori di social network, di portali o altre piattaforme telematiche abbondano nel fornire elementi conoscitivi sul proprio conto." (Rapetto, 2012)

Quindi, in sostanza, la navigazione così come la conosciamo necessita di alcune "dichiarazioni spontanee", per usare le parole utilizzate anche in precedenza, che portano alla creazione di una sorta di "Dna" dell'utente: questo verrà poi utilizzato dalle imprese per le campagne marketing oppure per monetizzare, vendendo questi dati a terze parti.

Per concludere è bene accennare al fenomeno della *data monetization* attraverso i vari settori. (Della Mura, 2018)

- TELCO, in questo settore è possibile utilizzare la *data monetization* in due differenti modi: il primo metodo è chiamato "diretto", si racchiudono i dati

anonimizzati in cluster differenziati per età, sesso e posizione, dopodiché questi saranno rivenduti ad altri operatori per lo sviluppo di nuovi servizi; il secondo metodo comporta un'analisi in merito all'orario delle chiamate, alla loro durata, alla loro destinazione così come alla loro qualità nonché ai loro disturbi, tutto ciò potrebbe portare ad un miglioramento del servizio incrociando i dati relativi al cliente con quelli relativi alla rete.

- MANUFACTURING, le aree in cui viene concentrato un maggior focus nel settore manifatturiero sono quelle che guardano principalmente alla supply chain, alle analisi predittive ed alla riduzione degli scarti e degli errori di produzione. Di fatti le aziende di questo settore oggi basano molto delle loro strategie focalizzandosi sui dati raccolti dai dispositivi o dai sensori all'interno della supply chain o lungo le linee di produzione, questi dati saranno poi integrati con altri dati (strutturati o non strutturati) provenienti da altre fonti. La possibilità di accedere in tempo reale a questa vastità di dati permette alle aziende di prendere decisioni operative più efficaci oppure di sviluppare nuovi servizi, il tutto contenendo i costi ma aumentando la competitività. In questo specifico caso il *data monetization* non produce un aumento del fatturato ma, dato un decremento degli investimenti, un aumento del ROI.
- BANKING & FINANCE, dato che le banche sono i principali fornitori dei servizi di pagamento riescono ad avere a disposizione più di chiunque altro dei dati che possono facilitare la comprensione di comportamenti di acquisto e dei macro trend emergenti. Questi dati provenienti da attività interne possono essere incrociati con altre informazioni provenienti da fonti esterne (tipo social media o dataset geo-economici) per creare un quadro generale della clientela: questi dati, resi anonimi, possono aumentare il fatturato degli intermediari finanziari se venduti a dei *merchant* per ottimizzare le loro operazioni oppure effettuare delle integrazioni fra servizi. In alternativa la data monetizzazione interna si può tradurre nella possibilità di offrire dei nuovi servizi ai consumatori ma anche di preservare i servizi esistenti con strumenti antifrode, basati sull'analisi del comportamento degli utenti e supportati da tecniche di *machine learning* e *cognitive services.*

- RETAIL, è il settore che per primo, probabilmente, ha compreso quale importanza potessero ricoprire i dati e si è servito immediatamente di questa "miniera d'oro". Le informazioni riguardanti gli utenti servono per capire al meglio quali possono essere le loro abitudini e le loro preferenze. Aumentare il fatturato è quindi possibile tramite la vendita dei dati, che devono essere necessariamente anonimizzati, ai fornitori per aiutarli a intendere il livello di gradimento dei loro vari prodotti nonché per dare una mano nell'elaborazione di strategie promozionali corrette. Gli insights sono fondamentali anche per l'ottimizzazione delle operazioni interne con l'obiettivo di migliorare la *shopping experience* del consumatore oppure per creare una profilo più completo e dettagliato del cliente stesso, in alternativa possono anche condurre all'elaborazione di strategie di marketing come il *cross-selling* o l'*up-selling.* (Della Mura, 2018)

2.4 Il caso Cambridge Analytica: perché i nostri dati non sono sempre al sicuro.

Per concludere questo capitolo è bene scrivere di quello che in molti hanno definito un esempio di "violazione dei dati" oppure di una "falla" nel sistema di Facebook: il caso "Cambridge Analytica".

Prima di analizzare la vicenda è bene fare una premessa: del seguente episodio sarà sottolineato la facilità con la quale determinate aziende avrebbero potuto raccogliere dati di milioni di utenti in maniera legale (ma non troppo), di come queste tecniche possano anche essere utilizzate per scopi di "marketing" ed, infine, quali sono state le reazioni di Facebook come azienda e del mercato in generale.

Questa introduzione era necessaria visto il modo in cui questo scandalo è nato, per questioni politiche, ma è bene vedere il nocciolo della questione che è anche abbastanza semplice da cogliere: i nostri dati non sempre sono al sicuro.

I soggetti della vicenda sono fondamentalmente quattro: Facebook, il provider di questi milioni di dati, Cambridge Analytica ed infine noi, gli utenti.

Il primo tassello di questo caso è Facebook che come visto in precedenza ha la vendita di dati agli inserzionisti come attività *core* del suo business. Tutto ciò è normale dato che nessuno degli utenti con un profilo paga nemmeno un centesimo per scambiare messaggi con amici oppure postare immagini, video o musica e perciò gli utenti "pagano" fornendo i loro dati all'azienda americana: essi sono per quest'ultima gli unici asset patrimoniali che possiede (come scritto prima). La quantità di informazioni riguardanti gli utenti sono di rilevante importanza dato che oltre due miliardi di persone sono iscritte a Facebook e circa il 70% di esse si connette al social network almeno una volta al giorno. Questo più o meno per rendere l'idea dell'enorme mole di dati con la quale l'azienda creata da Mark Zuckerberg lavora quotidianamente. (Barberio, 2018)

Il secondo tassello di questo caso è senza ombra di dubbio Cambridge Analytica: questa è una società fondata nel 2013 dal miliardario statunitense Robert Mercer che ha come attività principale quella di raccogliere dati dai social networks sui loro utenti. In sostanza questa azienda ha il compito di studiare i post che guadagnano più "likes", quelli più commentati, da dove vengono condivisi i post pubblicati per poi, tramite l'utilizzo di determinati algoritmi o modelli, creare dei "profili" psicologici di ogni utente con un approccio molto simile a quello della psicometria. Maggiori sono i post analizzati più accurato sarà il profilo psicometrico di ogni utente. Ovviamente l'attività della suddetta azienda non si conclude qui: nel tempo ha acquistato altri dati provenienti da altre fonti, i cosiddetti "broker di dati". Tutto questo, anche alla luce di quanto scritto fino ad ora, è legale e lo fanno ormai moltissime aziende, anche piccole. Le informazioni raccolte riguardano principalmente le abitudini dei soggetti (come carte fedeltà di determinati store o acquisti portati a termine online) e sono, ovviamente, del tutto anonime. Cambridge Analytica compra milioni di questi dati, sebbene siano una mole straordinaria di informazioni del tutto anonimizzate è difficile pensare che la società britannica non riuscisse ad rielaborare il profilo psicologico di almeno un singolo utente utilizzando i modelli e gli algoritmi a loro disposizione. Anzi, stando alle dichiarazioni di Michal Kosinski, ricercatore di Cambridge che si occupa dei modelli e degli algoritmi menzionati precedentemente, tracciare il profilo psicologico di un utente è molto semplice: bastano sessantotto likes su Facebook per capire il colore della pelle dell'utente e il suo orientamento sessuale senza averlo nemmeno mai visto; con settanta "mi piace" si può conoscere una persona quanto la conoscono i suoi amici più fidati;

rispettivamente centocinquanta e trecento likes portano il modello a conoscere la persona come la conoscono i suoi genitori e la sua compagna o compagno. (Krogerus, 2017) Secondo l'azienda britannica ciò che loro fanno è solamente un "*microtargeting"* comportamentale, ossia fare leva non solo sui gusti dell'utente ma anche sulle sue emozioni per poi creare una pubblicità altamente personalizzata: questa tecnica è il presente ed il futuro del marketing. Avere a disposizione milioni di informazioni permetterebbe ad una determinata azienda di applicare questa tecnica ed avere successo nella maggior parte dei casi dato che, stando a quanto detto da Kosinski, si arriverebbe a conoscere l'utente quasi meglio di quanto lui conosca sé stesso, non a caso i modelli sviluppati da Cambridge Analytica devono saper prevedere ed anticipare le reazioni dei clienti. (Menietti, 2018)

Il terzo individuo di questa vicenda è stato il provider dei dati, colui che ha reso possibile l'utilizzo di queste informazioni da parte di Cambridge Analytica. Tale soggetto ha un nome ed un cognome: Aleksandr Kogan. Quest'uomo nel 2014 era anche lui un ricercatore a Cambridge e in quello stesso anno decide di creare un'app chiamata "*thisisyourdigitallife"* ("questa è la tua vita digitale"). Questa applicazione prometteva di produrre profili psicologici e di previsione del comportamento studiando semplicemente le attività online. Per utilizzarla bastava semplicemente accedervi tramite Facebook, usando quindi il "*Facebook connect"* che permette di iscriversi ad un sito o ad una applicazione senza inserire una mail ma semplicemente entrandovi con l'app del social network stesso. L'applicazione di Kogan, come molte altre, era gratuita anche se in realtà gli utenti "pagavano" con i loro dati: si aveva accesso alla mail, all'età, al sesso ed altre informazioni contenute sul profilo Facebook dell'utente. All'epoca l'azienda di Zuckerberg permetteva ai gestori delle applicazioni di poter raccogliere anche alcuni dati sugli amici della persona che si era appena iscritta all'app, senza che loro ne fossero consapevoli, moltiplicando così le informazioni disponibili: questa pratica verrà ritenuta, in seguito, troppo invasiva da Facebook vietando quindi l'accesso a tali dati. Nel 2015 erano circa duecentosettantamila le persone iscritte a *"thisisyourdigitallife"*, questo rese possibile a Kogan avere a disposizione i dati di circa cinquanta milioni di utenti Facebook, seguendo le stime del New York Times, fra cui le loro immagini, i posti da loro visitati, i loro interessi ed il luogo in cui vivono.

Il caso scoppia quando Kogan viola i termini d'uso di Facebook condividendo tutte le informazioni disponibili con Cambridge Analytica: il social network vieta, infatti, ai gestori delle applicazioni di vendere i dati che hanno ricavato a parti terze per il semplice motivo che, qualora qualcuno avesse bisogno dei dati che Facebook ha a disposizione, dovrebbe chiedere all'azienda di Mark Zuckerberg stessa senza eludere questo ostacolo e comprandoli da un gestore di app. Le possibili sanzioni nelle quali si rischia di incorrere se non si rispettano i *"terms of use"* imposti dall'azienda americana sono la sospensione dell'account e la fine del modello di business, qualora questo si basasse sui dati e sulla possibilità di accesso all'applicazione tramite il social di Facebook.

In sostanza: la piattaforma di Zuckerberg è stato "violata" senza che ci fosse alcuna falla. Le preoccupazioni per gli utenti non devono essere rivolte verso la fragilità della sicurezza di Facebook, piuttosto devono rivolgersi al fatto che una volta iscritti al social chiunque può impossessarsi delle informazioni immesse su di esso, siccome ormai ci sono vere e proprie società che vendono dati e questi sono alla base dell'economia, di fatti vengono raccolti, immagazzinati e studiati per poi vendere un prodotto a chi è dall'altra parte dello schermo. Marco Montemagno, opinionista di Sky TG 24 nonché ex giornalista della stessa emittente, in un video postato sui suoi canali social l'indomani dell'accaduto afferma che la parte veramente lesa di questa vicenda è un quarto soggetto: l'utente; in particolar modo colui che condivide tutto su sé stesso senza alcun freno, l'utente medio. (Montemagno, 2018)

Il caso da noi analizzato è scoppiato, come detto in precedenza, per motivi politici: Cambridge Analytica, secondo l'inchiesta del New York Times e del Guardian ha avuto un ruolo rilevante nella vittoria di Donald Trump ai danni di Hillary Clinton nelle elezioni presidenziali statunitensi del 2016. Non bisogna però tralasciare il fatto che tale metodologia viene utilizzata più che in politica nel marketing: tutte le aziende tech guadagnano grazie ai dati ed esiste un intero ecosistema di società che lucra vendendo le nostre informazioni, senza che ciò sia illegale ovviamente anche per via del fatto che ormai il "dato" è alla base della nuova era economica e tecnologica.

Per concludere è bene chiedersi quali sono state le reazioni di Facebook e del mercato dopo che tutto ciò è accaduto.

Partiamo dall'azienda di Mark Zuckerberg: la reazione immediata dopo lo scoppio dello scandalo è stata la sospensione di Cambridge Analytica da Facebook, proprio da parte dell'azienda americana. Sebbene questo possa sembrare ovvio non lo è affatto. Christopher Wylie, ex dipendente di Cambridge Analytica e principale fonte del Guardian per questa inchiesta, ha infatti dichiarato che Facebook era a conoscenza da circa due anni di questo problema dato che l'azienda britannica, per evitare la sospensione, si autodenunciò alla società di Zuckerberg affermando di essere in possesso di dati ottenuti violando le condizioni d'uso e di averne disposto subito la distruzione. La sospensione è arrivata, ma solo nel 2018: il 16 Marzo per essere precisi, una volta venuti a conoscenza dell'imminente pubblicazione degli articoli da parte del New York Times e del Guardian. (Menietti, 2018)

In secondo luogo pare ci siano state delle pressioni da parte di Facebook alle testate citate in precedenza poco prima dell'uscita degli articoli affinché non fosse usato il termine "falla": come spiegato prima, nei fatti, non c'è stata alcuna falla dato che l'integrità di Facebook non è stata violata in alcun modo. Facendo leva su questo motivo la società americana ha tentato più volte di ridimensionare l'accaduto e tranquillizzare i proprio utenti che mai nessuno avrebbe "craccato" la sicurezza del social network per antonomasia. Tuttavia è impossibile non parlare di "falla", perché questa c'è ed è evidente: non si trovava nel server ma nei termini d'uso dato che questi consentivano una raccolta spropositata di informazioni di alcuni utenti senza che loro fossero a conoscenza di nulla.

Infine, è interessante anche vedere come ha reagito il mercato nella scoperta di questa "falla" di Facebook. Il titolo dell'azienda nell'apertura della Borsa la settimana seguente allo scoppio di questo "caso" ha perso oltre il 7%, monetizzando il tutto si tratta di circa 25 miliardi di dollari. Ciò significa che gli azionisti vedono minacciato il modello di business di Facebook dopo l'evento che ha interessato l'impresa e Cambridge Analytica. (Barberio, 2018)

Tuttavia per Facebook sarebbe anche controproducente, ormai, cambiare il modello di business: un domani Mark Zuckerberg potrebbe decidere che, dati gli avvenimenti recenti, è meglio per l'azienda non vendere più i dati degli utenti agli inserzionisti. Per evitare la chiusura del social network o la mancanza di profitto si potrebbe optare per un

modello di business in cui il dato è “segreto”, quindi Facebook evita, per esempio, di tracciare i movimenti dei propri utenti ma in cambio viene chiesta una “tassa d’iscrizione”: se una persona volesse iscriversi al social senza permettere che questo usi i propri dati vendendoli ad altri per scopi pubblicitari deve pagare una somma (per esempio cento euro) ogni anno. Ma effettuare un cambio del genere, soprattutto per questa azienda che ha un valore di oltre cinquecento miliardi, è molto difficile poiché è probabile che si incorra in alcune complicazioni come ad esempio gli azionisti che potrebbero intentare una causa ai danni dell’azienda stessa dato che vedrebbero “uccisa” la loro “gallina dalle uova d’oro”. (Montemagno, 2018)

Dopo questo avvenimento sono state numerose le campagne a favore della tutela dei dati da parte dei giganti del web. Il dato più rilevante per le aziende e per gli utenti italiani, però, è stata l’entrata in vigore del regolamento europeo sulla protezione dei dati personali a partire dal 25 Maggio scorso.

CAPITOLO 3: "GDPR: ANALISI ED IMPATTI".

3.1 Agenda digitale europea.

L'innovazione ha sempre avuto un ruolo di primo piano nell'Unione Europea, sin dalla creazione di quest'ultima: nella nuova era del digitale, caratterizzata da un mondo sempre più interconnesso e dalla "società dell'informazione", viene imposta prepotentemente una rapidità nelle scelte da effettuare ai decisori europei. Negli anni Ottanta veniva portato avanti il cosiddetto *modello lineare di innovazione* (Vitali, 2013) in cui si cercava di sostenere la ricerca scientifica pura mediante finanziamenti e sostegno agli investimenti, diretti nella maggior parte dei casi a centri di ricerca pubblici.

Con il passare del tempo questo metodo inizia a divenire obsoleto: negli anni Novanta con l'affermazione delle tecnologie dell'informazione e della comunicazione (TIC, oppure in inglese ICT, *Information and Communications Technology)* e dell'economia digitale. Il precedente approccio metodologico viene rimpiazzato da quello che viene, invece, chiamato *"metodo multidirezionale"*. È possibile trovare delle differenze notevoli, come per esempio il fatto che i finanziamenti ed i sostegni agli investimenti non vengano più effettuati a favore dei centri di ricerca universitari: essi vengono indirizzati alle imprese con lo scopo di supportare progetti maggiormente orientati al mercato. (Monti, 2016)

Tuttavia la vastità di questa rivoluzione tecnologica e la sua complicatezza hanno imposto ai decisori europei di focalizzarsi sulla nuova tecnologia digitale. Data, infatti, l'assoluta importanza di questa per le politiche innovative europee è stato ritenuto opportuno concedere al digitale una maggiore importanza sottoscrivendo quella che di fatto viene definita l' *"Agenda Digitale Europea"*.

Questa necessità nacque in seguito alle trasformazioni che la vita di tutti i giorni ha subito, in particolar modo sotto un punto di vista economico e sociale: si sta sviluppando una società basata sull'informazione in cui il management, la qualità e la velocità di circolazione dei dati diventano una condizione fondamentale per la competitività di un intero paese. La rivoluzione del digitale non merita di essere sottovalutata, non solo per le opportunità che può presentare ma anche per i rischi connessi ad essa: il più grande è quello di vedere sparire i mestieri tradizionali mettendo così in difficoltà le piccole e medie imprese non ancora attrezzate per concorrere in un mercato globalmente interconnesso.

In questo quadro sono i decisori dell'Unione Europea che devono tenere in considerazione questi cambiamenti e cercare di capirli ma anche assicurare un contesto normativo e politico in grado di facilitare e favorire questa trasformazione in atto.

Il documento da cui si è partiti per arrivare, ai giorni nostri, all'agenda digitale è il Libro Bianco della Commissione Europea *"Crescita, competitività e occupazione. Le sfide e le vie da percorrere per entrare nel XXI secolo"* scritto nel 1993: si inizia a delineare un contesto normativo e politico nuovo, la Commissione Europea considerava le tecnologie ICT nell'ambito di un obiettivo più grande riguardante la promozione della competitività fra imprese in Europa e nel mondo. (Monti, 2016)

L'Europa aveva iniziato la preparazione a quella che sarebbe stata una grande serie di trasformazioni.

Nello scritto veniva sottolineata l'importanza di creare una serie di infrastrutture d'informazione che avrebbero permesso una crescita economica e una coesione sociale e territoriale. Tale obiettivo, così ambizioso, necessita il sostegno di interventi che avrebbero permesso di arrivare alla creazione di uno spazio comune di informazione, il quale avrebbe aumentato la produttività e la competitività delle aziende piccole e medie. Le azioni proposte nel Libro Bianco redatto dalla Commissione erano le seguenti:

- Una maggiore apertura alla concorrenza, che avrebbe permesso di fornire una vastità di servizi al miglior costo di mercato;
- Lo sviluppo di reti di supporto;
- Un coordinamento tra i fondi strutturali a disposizione e la politica di telecomunicazione.

Con l'inizio del nuovo millennio fu avviata una nuova strategia con l'intento di migliorare il piano d'azione sulle ICT: fu avviata la strategia di Lisbona nella quale veniva stabilito di rendere l'Europa l'economia più dinamica e competitiva al mondo in grado di cogliere le opportunità che derivavano da internet e dall'economia digitale più in generale. (Monti, 2016)

Le principali vie d'azione rispetto al documento redatto nove anni prima erano le seguenti:

- Piani d'investimento sulle risorse umane, in modo tale da facilitare l'ingresso dei giovani e dei lavoratori più anziani nell'era del digitale;
- Promuovere l'uso di internet, incoraggiando i consumatori a comprare prodotti online e sostenendo le PMI nel passaggio al digitale;
- Assicurare un accesso più sicuro, veloce ed economico ad internet, migliorando il coordinamento a livello europeo e introducendo più concorrenza nelle reti di accesso a livello locale.

Tre anni dopo, a Siviglia, la Commissione Europea approva quella che è la naturale continuazione di *eEurope 2002*, ossia *eEurope 2005*. L'obiettivo principale era quello di coniugare maggiormente il potenziale di tutte le nuove tecnologie con un aumento della produttività economica ed il miglioramento dei servizi in termini qualitativi.

In particolar modo questo documento prevedeva: la costruzione di infrastrutture di informazione sicure e protette che proteggessero i dati degli utenti, in particolar modo contro attacchi hacker e criminali; l'introduzione di una banda larga entro il 2005 in tutte le scuole, università e centri di amministrazione pubblici.

A questo documento succederà l' *"i2010 – Una società europea dell'informazione per la crescita e per l'occupazione"*, redatto nel 2005. Anche in esso viene ribadito come le ICT sono fondamentali per un miglioramento di qualità della vita per tutti i cittadini europei facilitando anche la coesione sociale ed economica. Le priorità messe in evidenza erano le seguenti:

- Creare un mercato digitale unico;
- Promuovere gli investimenti in ICT e l'innovazione per facilitare la crescita economica;
- Istituire una società europea dell'informazione, capace di collegare i concetti della crescita e dell'occupazione con il concetto dello sviluppo sostenibile.

La vera e propria *"Agenda Digitale Europea"* verrà pubblicata solo nel 2010, ben diciassette anni dopo l'inizio della costruzione di un contesto politico e normativo volto a sostenere l'ingresso nella nuova era digitale; questa è parte di un percorso ancora ben lontano dalla conclusione. Essa è stata introdotta con una comunicazione della Commissione Europea il 19 Maggio del 2010 ed è una delle sette "iniziative faro" dell'Agenda "Europa 2020" : ha un ruolo fondamentale nello sviluppo delle ICT a livello europeo ed ha il compito di facilitare la crescita intelligente, inclusiva e sostenibile per tutti gli Stati membri facenti parte della Comunità. Secondo tale documento con una maggiore diffusione delle ICT ed un utilizzo più efficace di esse sarà possibile affrontare meglio le nuove sfida che il panorama economico metterà di fronte ai cittadini europei. (Monti L. , Politiche dell'Unione Europea: la programmazione 2014-2020, 2016)

Affinché sia possibile realizzare gli obiettivi di *Agenda Digitale* è necessario che tutti gli attori e decisori europei contribuiscano alla sua realizzazione nonché al suo miglioramento per raggiungere un'economia sempre più connessa digitalmente.

Per raggiungere ciò sono state identificate delle specifiche aree d'azione. Quella di fondamentale importanza è il *Mercato digitale unico e dinamico* per sfruttare i benefici ed i vantaggi che questa nuova era digitale ci ha posto davanti: questo è necessario per via del fatto che i mercati online sono ancora divisi, non solo a livello europeo ma anche a livello intercontinentale da molte barriere che ostacolano l'accesso ad internet. Ormai la creazione di questo mercato unico non è più vista come un'aspirazione alla quale la Comunità Europea può ambire, bensì come un obbligo.

Le caratteristiche di questo mercato pensato dall'*Agenda* sono sostanzialmente due. La pima è la facilità di accesso: deve infatti essere possibile per i consumatori accedere

facilmente ai contenuti online quanto a quelli offline. L'altra fondamentale caratteristica è la semplificazione delle transazioni online a livello oltre i confini della propria nazione. Gli Stati membri e l'intera UE ha il ruolo di incoraggiare il commercio digitale, cosiddetto *e-commerce*. Nei fatti, anche se così non sembrerebbe, i consumatori non possono beneficiare di tutti i vantaggi del commercio online date le frammentazioni delle transazioni online che limitano le operazioni commerciali online in Europa. Tuttavia, come sottolineato anche più volte in precedenza, le difficoltà del mercato unico online non risiedono solo nella eccessiva frammentazione delle operazioni ma anche nella mancanza di fiducia da parte dei cittadini nel digitale e nel commercio elettronico. È necessario, quindi, un incremento di fiducia nel digitale da parte dei consumatori altrimenti lo sviluppo dell'economia sarà rallentato. Per giungere a ciò l'UE ha creato un contesto normativo in cui riconosce ai propri cittadini una serie di diritti riguardanti la libertà d'espressione e informazione ma anche (soprattutto) diritti alla riservatezza sui dati degli utenti nonché la protezione di questi ultimi: purtroppo non sempre i consumatori sono a conoscenza di ciò. Proprio per questo motivo un altro degli aspetti largamente rimarcati dell'*Agenda digitale* è il potenziamento della sicurezza digitale. I consumatori ed i fruitori delle ICT e delle tecnologie digitali devono sentirsi sicuri ogni volta che si collegano ad internet altrimenti la loro fiducia difficilmente aumenterà e lo sviluppo del mercato online sarà compromesso. Già dal 2010 quindi sono stati lanciati dei piani per proteggere le informazioni personali degli utenti e rafforzare la lotta alla criminalità informatica. Queste attività coinvolgono numerosi soggetti: dalle istituzioni nazionali e sovranazionali agli enti privati passando per gli stessi cittadini. (Monti, 2016)

Altro obiettivo di questa "iniziativa faro" è quello di garantire un accesso ad internet veloce e superveloce: probabilmente una delle sfide più importanti non solo dell'*Agenda* in questione ma di tutta la strategia che porta ad *Europa 2020*. L'obiettivo che è stato posto è quello di avere almeno una connessione superiore ai 30 Mbps per tutti, quindi un accesso alla banda larga veloce, e una connessione sopra i 100 Mbps per almeno la metà delle famiglie europee (banda ultralarga).

In tutto ciò l'*Agenda digitale europea* promuove anche l'alfabetizzazione e lo sviluppo delle competenze per la cittadinanza europea in modo tale da favorire l'inclusione sociale. Questo perché l'avanzare dell'era digitale, come spiegato in precedenza, comporta occasioni da sfruttare ma anche grandi rischi. Il mondo del lavoro ormai richiede delle minime competenze digitali che non tutti gli individui possiedono. Inoltre bisogna tener conto che alcuni dei lavoratori "over 50" qualora perdessero il loro attuale lavoro si potrebbero ritrovare in seria difficoltà nel caso non avessero delle *skills* digitali: questo potrebbe condurre anche ad un'esclusione non solo da un punto di vista professionale per questi soggetti ma anche da un punto di vista sociale. L'economia europea stessa soffre per alcune carenze in campo digitale e ICT sia per la mancanza di personale qualificato sia per la mancanza di strutture in grado di fornire competenze. Con l' *Agenda digitale europea* l'Europa si pone l'obiettivo di formare i propri cittadini,

in particolar modo la gioventù, ad utilizzare strumenti digitali e ICT ed aumentare le competenze già in loro possesso. Contemporaneamente sono stati proposti programmi volti a promuovere l'insegnamento di queste *skills* anche ad altre categorie di soggetti come i lavoratori over 50, detti anche in precedenza, o anziani e disabili. Questi programmi hanno l'obiettivo di far accedere alle potenzialità dell'economia digitale tutti i soggetti detti in precedenza.

È doveroso parlare dei progetti che l'Europa ha attuato per il programma *2020:* innanzitutto è possibile fare una divisione tra piani, quelli diretti e quelli indiretti.

I fondi diretti europei inerenti le nuove tecnologie dell'informazione sono tutti indirizzati al sottoprogramma *"Scienza di eccellenza"* e, più in particolare, alla finalità *"Research Infrastrucures"*. (Monti, 2016)

Per quanto riguarda i fondi SIE (strutturali e di investimento europei) a gestione decentrata, quelli gestiti dallo Stato membro in sostanza, è possibile affermare che essi sono suddivisi per tre obiettivi tematici (OT). Il secondo (OT2) è quello maggiormente impegnativo e sul quale il nostro Paese sta spendendo le forze: questo prevede il miglioramento dell'accesso alle tecnologie di comunicazione e dell'informazione, della qualità di esse e un loro maggiore impiego. I fondi stanziati per questo obiettivo hanno un valore complessivo di due miliardi di euro, l'87,71%, pari ad 1 miliardo e 845 mila euro, sono stanziati dal FESR (Fondo Europeo per lo Sviluppo Regionale) mentre la restante parte è stanziata dal FSE (Fondo Sociale Europeo). Tuttavia c'è la possibilità che alcuni interventi siano supportati dal FEASR (Fondo Europeo Agricolo per lo Sviluppo Regionale): questi fondi saranno impiegati nelle aree rurali a rischio di fallimento di mercato per raggiungere gli obiettivi, installando delle infrastrutture sui luoghi in questione, migliorando quelle esistenti oppure effettuando altri tipi di azioni.

Nel quadro di Europa 2020 l'Italia ha lanciato una propria strategia nazionale chiamata *"Agenda digitale italiana"* per promuovere le cultura e l'economia digitale: l' obiettivo di questa agenda non è solo quello di creare un ambiente che possa facilitare la crescita socio-economica della nazione grazie ad un uso più consapevole degli strumenti ICT ma c'è anche l'intenzione di recuperare quel gap digitale che c'è con altri Stati membri. (Monti, 2016)

I dati emersi grazie alle analisi e agli studi della Commissione Europea nella *Digital Agenda Scoreboard* del 2015 evidenziano, però, le difficoltà che il nostro Paese sta riscontrando nel raggiungimento dei suoi obiettivi, posizionandosi solamente al venticinquesimo posto rispetto gli altri Stati membri nella classifica di avanzamento delle agende digitali. (Monti L. , Politiche dell'Unione Europea: la programmazione 2014-2020, 2016)

Il nostro paese ha difficoltà per via del fatto che le infrastrutture digitali sono distribuite a macchia di leopardo su tutta la penisola, privilegiando i centri urbani ma danneggiando le aree rurali ed interne. Il divario digitale è, quindi, ben visibile non solo a livello nazionale ma anche a livello regionale e locale: questo è il dato che più preoccupa e che più allontana l'Italia da altri Stati membri. (Monti, Pepe, & Rizzuti, 2015)

I piani principali del Bel Paese rimangono comunque due, fondamentalmente: la *Crescita Digitale* ed il *Piano Nazionale Banda Ultra Larga*, finanziati entrambi dal FESR. Questi sono importanti poiché, come accennato più volte anche precedentemente, le ICT hanno un carattere trasversale ed un miglioramento nel loro utilizzo potrebbe comportare altri benefici inerenti l'inclusione sociale, la competitività delle imprese, una maggiore occupazione e un miglioramento dei sistemi di formazione ed istruzione.

Per concludere questa panoramica sull'Agenda digitale italiana è bene sapere quali sono i risultati attesi (RA) di cui si compone l'OT2.

Il primo RA di questo obiettivo tematico (RA 2.1) consiste nella riduzione dei divari digitale nei territori nazionali e diffusione di connettività in banda larga ed ultra larga. Sono stati stanziati circa 800 milioni per raggiungere questo risultato, la maggior parte di essi (circa 635 milioni) andranno alle regioni meno sviluppate, come Basilicata e Puglia, mentre per quelle più sviluppate o comunque in transizione andranno circa 170 milioni. Coerentemente con i piani europei si intende dotare l'accesso alla banda larga veloce a tutti i cittadini e l'accesso alla banda ultra larga almeno alla metà dei cittadini.

Il secondo RA (RA 2.2) riguarda la digitalizzazione dei processi amministrativi e diffusione di servizi digitali pienamente interoperabili delle pubbliche amministrazioni a cittadini e imprese, soprattutto nel settore della sanità e della giustizia. Sono stati allocati circa 590 milioni di euro, l'80% di essi andrà a favore delle regioni meno sviluppate.

Il terzo RA (RA 2.3) è il potenziamento della domanda di ICT di cittadini e imprese in termini di utilizzo dei servizi online, inclusione sociale, e partecipazione in rete: l'ammontare complessivo è di circa 400 milioni di euro, tutti provenienti dal FESR. L'importo totale sarà diviso fra regioni meno sviluppate (310 milioni), regioni in transizione (18 milioni) e regioni sviluppate (67 milioni). (Monti L. , 2016)

Per concludere è possibile affermare che la sicurezza dei dati è sempre stata parte del secondo risultato atteso: tuttavia il GDPR è una normativa che nasce dopo i piani dell'Agenda digitale dato che le prime elaborazioni del nuovo regolamento sono state effettuate solo nel 2016. Questo, come evidenziato già in questo paragrafo, non esclude però che la tutela dei dati degli utenti sia stata da tempo una delle priorità per i legislatori e per i decisori della Comunità Europea.

3.2 GDPR: cambiamenti delle norme europee sulla privacy.

Dopo due anni di elaborazione il 25 Maggio 2018 è entrata in vigore in tutti gli Stati membri dell'Unione Europea la normativa GDPR, abbreviazione di *General Data Protection Regulation*. Fin da subito ha avuto un'importanza rilevante dato che avrebbe cambiato molte delle "regole del gioco" per il commercio online e non solo.

Questa normativa ha il compito di tutelare le persone fisiche per quanto concerne il trattamento e la circolazione dei loro dati personali.

Come spiegato sul sito dell'Agenda digitale europea: *"Il GDPR nasce da precise esigenze, come indicato dalla stessa Commissione UE, di certezza giuridica, armonizzazione e maggiore semplicità delle norme riguardanti il trasferimento di dati personali dall'UE verso altre parti del mondo"*. (Natale & Longo, 2018)

L'obiettivo finale della suddetta normativa è quello di proteggere i dati personali degli utenti europei nell'era della digitalizzazione e dei social network: caso ha voluto che questa entrasse in vigore poco dopo lo scoppio del caso "Cambridge Analytica" e quindi nelle settimane "roventi" per quanto riguardava il tema della privacy.

È necessario, innanzitutto, analizzare questo regolamento per capire come i soggetti che ne saranno "colpiti" in qualche modo (utenti e aziende) dovranno comportarsi.

Prendendo direttamente dal testo emanato dall'UE l'articolo 3 possiamo leggere *in primis* chi saranno i destinatari di queste norme:

"1. Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.

2. Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:

a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure

b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

3. Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico." (Commissione Europea, 2018)

In sostanza questo articolo afferma che saranno soggetti a queste regole, fondamentalmente, due tipi di individui: titolari e responsabili stabiliti in UE senza che vengano rilevati il chi ed il dove vengono indirizzati questi trattamenti, insomma basta che l'impresa in questione operi entro i confini dell' Unione Europea; titolari e responsabili che non sono operanti nei confini dell'Unione, ma in questo caso viene stabilito verso chi è effettuato il trattamento, ossia soggetti che si trovano nell'UE (anche qualora essi non siano cittadini), ai quali vengono offerti beni o servizi o, in alternativa, si monitora il loro comportamento. In questa seconda ipotesi rientrano verosimilmente tutte le companies statunitensi che operano in Europa offrendo beni e servizi. (Troiano, 2017)

Nel terzo comma viene illustrato un caso più raro e particolare: possono essere soggetti a questa regolamentazioni anche chi pur non essendo stabilito nei confini dell'Unione Europea è soggetto al diritto di uno Stato che invece ne fa parte, seguendo i principi del diritto internazionale pubblico.

Sebbene questo articolo possa sembrare di una semplicità disarmante non è assolutamente così: un anno prima della pubblicazione del GDPR i dubbi sorti in merito a quest'ultimo e verso chi applicarlo sono stati molteplici. La questione che ha suscitato e suscita tuttora delle polemiche risiede nel fatto che questa è una "normativa madre" e non sarà uguale per ogni Stato membro: nei fatti ogni Paese avrà degli spazi per interventi normativi che potranno permettere di precisare le regole del GDPR. Così facendo, però, si corrono non pochi rischi. Senza ombra di dubbio il primo comporta un possibile "disallineamento" con la visione iniziale dell'UE riguardante la normativa. In secondo luogo possono emergere dei contrasti tra il GDPR stesso e le leggi nazionali, qualora quest'ultime fossero scritte con poca attenzione. I primi Stati che si sono mossi per adeguare i loro regolamenti nazionali sulla privacy al GDPR sono Austria e Germania: verosimilmente queste saranno poi seguite anche da Francia e molti altri Stati membri. Ciò arreca confusione per il semplice motivo che sarà complicato stabilire quale regola sarà necessaria applicare ai trattamenti delle informazioni personali se quella nazionale o quella europea e, qualora risultasse coinvolta un'azienda statunitense, sarà invece opportuno utilizzare il regolamento comunitario oppure quello USA?

La risposta, in linea teorica, è meno complicata di quanto possa sembrare: in futuro si continueranno a studiare ventisette normative differenti sul *data protection* (ventotto se si vuol contare il Regno Unito prima che esca ufficialmente dall'UE). Le leggi nazionali dovranno sempre e comunque seguire quelle che sono le linee guida del regolamento

europeo in modo da armonizzare il contesto normativo come richiesto dagli operatori economici già da qualche anno.

Per quanto riguarda la disputa sulla legge da utilizzare in caso di azienda statunitense è possibile affermare che l'articolo 3 è stato scritto appositamente per questa eventualità e per chiarire ogni possibile dubbio.

Inoltre è necessario aggiungere che, come letto già nel primo comma del precedente articolo, qualora sia un'impresa europea a raccogliere i dati e trasferirli in un'area extracomunitaria, come gli Stati Uniti per non cambiare esempio, il GDPR potrà essere applicato anche su questa utilizzando strumenti come il *Privacy Shield*, alternativamente le *standard model clauses* oppure le *Binding Corporate Rules*[6], tutti già consolidati dalla normativa in via di abrogazione e che sono stati ripresi dalla nuova emanata il 25 Maggio. (Troiano, 2017)

Il decreto di adeguamento per il GDPR in Italia è stato approvato dal consiglio dei ministri l'8 Agosto 2018: tuttavia questa riforma per la privacy entrerà in vigore in maniera graduale per permettere ai soggetti interessati che operano nel Paese di adeguarsi a questi cambiamenti. Questo periodo transitorio garantito durerà un totale di otto mesi, da ciò è possibile affermare che il decreto entrerà in pieno vigore quando il 2019 sarà inoltrato: questo per via del fatto che le sanzioni per eventuali infrazioni sono molto aspre, si arriva fino ai venti milioni di euro, e perciò la Guardia di Finanza effettuerà ispezioni graduali proprio per permettere alle imprese di adattarsi al meglio. Il testo approvato dal Governo ha come denominazione *"Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché*

[6] I termini citati indicano degli strumenti volti a proteggere la privacy degli utenti europei qualora sia un'impresa europea a prendere dei dati e trasferirli al di fuori dell'UE. Il *privacy shield*, alternativamente chiamato in italiano "Scudo UE-USA per la Privacy" è un accordo stipulato tra la commissione europea ed il dipartimento del commercio degli USA con l'intento di tutelare la sicurezza dei dati personali dei cittadini europei qualora essi vengano trasferiti negli Stati Uniti per fini commericali.
Per altre aree con cui non è stato stipulato alcun tipo di accordo speciale l'Unione Europea può decidere di porre delle clausole, appunto le *standard model clauses*, le quali permettono alle informazioni personali di avere una adeguata salvaguardia in territori non coperti dalle normative europee. Per concludere: può accadere che un'azienda debba trasferire i dati di alcuni dei suoi clienti europei ad un'altra sede la quale, però, non si trova nei confini dell'UE ma in un Paese che non garantisce adeguati livelli di protezione delle informazioni degli utenti. In tal caso l'Unione Europea richiede delle regole aziendali interne (*"Binding Corporate Rules"*). Queste rappresentano una sorta di "codice di condotta" interno dell'impresa ed è compito di quest'ultima dimostrare che tale codice sia: vincolante per ogni sede aziendale e che disponga di tutti i principi inerenti la privacy come sicurezza e trasparenza. In questo regolamento interno sarà anche necessario inserire gli "strumenti di efficacia", quali sistemi di aggiornamento e sistemi di notificazione, che l'impresa detiene per tutelare al meglio le informazioni personali degli utenti.

alla libera circolazione di tali dati". Per rendere ufficiale l'entrata in vigore di questo decreto manca solo la pubblicazione di esso sulla Gazzetta Ufficiale anche se sembra più che altro una formalità e dovrebbe avvenire nelle prossime settimane o mesi. Per garantire una sorta di continuità con il Codice della Privacy precedente è stato deciso che per un periodo transitorio i provvedimenti decisi dal Garante e le autorizzazioni concesse da quest'ultimo permarranno salvo una successiva riesaminazione. (D'Andrea, 2018)

È opportuno in questa sede stabilire quali sono le differenze tra quello che era il Codice della Privacy, quindi la vecchia normativa, e il GDPR. È possibile sintetizzare le differenze nei seguenti punti (Schindhelm, 2018):

- Il Codice della Privacy prevedeva una serie di norme frammentate e differenti per ogni Stato membro mentre, come scritto sopra, il GDPR ha delle precise linee guida che tutti gli stati debbono seguire sebbene i decreti di adeguamento sarebbero poi stati differenti tra i diversi Paesi.
- L'informativa riguardante l'utilizzo dei dati nel Codice della Privacy era spesso lunga, con numerosi riferimenti normativi ed incomprensibile per l'utente medio ciò, come già accennato, non è possibile per il GDPR invece, dato che l'informativa deve essere fornita per iscritto, chiara, coincisa, con pochi riferimenti normativi e il più comprensibile possibile per l'utente.
- La vecchia normativa riconosceva ai soggetti numerosi diritti e la maggioranza di essi avevano origine giurisprudenziale mentre la nuova normativa oltre ai precedenti diritti vede la nascita di altri due diritti per l'utente, il diritto all'oblio e il diritto alla portabilità dei dati.
- Con il Codice della Privacy non era prevista nessuna figura di raccordo tra i soggetti del trattamento e l'autorità Garante; con il GDPR nasce una nuova figura chiamata DPO, letteralmente *Data Protection Officer*, che dovrà avere requisiti e competenze elevate mentre il suo ruolo è quello di collegamento tra alcune categorie di soggetti Titolari del trattamento e l'autorità Garante.
- Nel Codice della Privacy non vi era alcun obbligo di notifica qualora ci fossero state delle violazioni dei dati personali; con il GDPR è necessario allertare entro 72 ore l'autorità Garante (questo arco di tempo può aumentare solo se giustificato) dalla scoperta di un eventuale *data breach*, inoltre è necessario anche avvisare il soggetto interessato qualora questa violazione possa compromettere la sua libertà ed i suoi diritti.
- Il consenso nel Codice della Privacy doveva essere libero, specifico, informato e reso mediante un atto formale per l'accettazione del trattamento dei dati mentre per quanto riguarda il GDPR il consenso non solo deve essere libero, specifico ed informato ma anche inequivocabile.
- Le figure che potevano essere notate nel trattamento dei dati, per quanto riguarda il Codice della Privacy, erano fondamentalmente il Titolare del

trattamento, il Responsabile e l'Incaricato del trattamento; nella nuova normativa è stata eliminata a livello terminologico la figura dell'Incaricato anche se formalmente tale soggetto continua ad esistere dato che sia il Titolare che il Responsabile possono incaricare determinati soggetti per lo svolgimento di determinati compiti.

- Nella precedente normativa era previsto che il Titolare del trattamento si dotasse di un documento chiamato DPS (Documento Programmatico sulla Sicurezza), relativo al controllo del trattamento dei dati e la loro sicurezza in modo da evitare ogni possibile sanzione proveniente dall'Autorità. Tale documento sarà poi abrogato per alleggerire i Titolari in un'ottica normativa. Nel GDPR è stato istituito il "Registro delle Attività di Trattamento" un documento nel quale sia il Titolare che il Responsabile del trattamento possono annotare ed argomentare tutte le attività relative alla protezione dei dati e alla circolazione di essi per quanto li riguardano.
- Nel Codice della Privacy era previsto che prima dell'inizio di alcune attività di trattamento dei dati fosse necessario compiere un atto di notifica all'Autorità Garante della Privacy. Con questa nuova normativa non sarà necessario effettuare alcuna notificazione all'Autorità ma sarà necessario che il Titolare, oppure i suoi rappresentanti, detengano un registro sullo stampo del vecchio DPS sulle attività di trattamento poiché quando richiesto sarà necessario fornire le informazioni sulle misure di sicurezza adottate.
- Una differenza sostanziale tra le due normative risiede nel fatto che nel Codice della Privacy veniva considerata la sede del Titolare del trattamento per rendere il regolamento applicabile. Con il GDPR questo non accade più: sono soggetti a tale normativa tutti coloro che operano all'interno dell'Unione Europea anche se la sede non è all'interno dell'Unione. Ovviamente, come detto in precedenza, si è soggetti a questo regolamento anche se il trattamento dei dati non avverrà all'interno dell'UE purché vengano offerti beni e servizi ai cittadini della Comunità o in alternativa le informazioni su questi utenti servano a monitorare il loro comportamento.
- La privacy nella vecchia normativa era intesa come elemento finale dell'attività di trattamento, dato che gli eventuali vizi nel processo di raccolta dei dati potevano essere sanati anche dopo che i trattamenti erano già stati eseguiti; con il GDPR sono stati introdotti i principi di *"Privacy by design"* e di *"Privacy by default"* i quali indicano che i trattamenti debbono essere concepiti sin dal momento della loro ideazione nel rispetto delle regole fissate dal legislatore.

La nascita del GDPR, quindi, non ha fatto altro che introdurre alcune novità per certi versi mentre per altri ha sostanzialmente confermato o leggermente variato quelle che erano le precedenti leggi sulla privacy.

Tuttavia una delle differenze principali tra la vecchia e la nuova normativa, come scritto precedentemente, è la nascita di due nuovi diritti che vanno a favore degli utenti: il diritto all'oblio ed il diritto alla portabilità dei dati. La nascita di questi benefici per gli individui è dovuta alla rapida evoluzione tecnologica e alle sfide che questa ci pone davanti ogni giorno.

3.2.1 Il diritto all'oblio.

Quanto al primo è bene fare alcune precisazioni: non è difficile, infatti, confondere questo "diritto all'oblio" (oppure "diritto alla cancellazione") con un altro "diritto all'oblio", ossia che la notizia di cui si contesta l'esattezza non sia più accessibile dai motori di ricerca ("delinkizzata") in alternativa cancellata o rettificata. Questo non può far altro che riportare in mente ai più il caso "Google Spain" del 2014. In quell'occasione, in sostanza, la Corte di Giustizia Europea stabilì che Google fosse tenuto a rendere inaccessibile da link su motore di ricerca notizie inesatte e lesive per l'immagine di un individuo o, alternativamente, notizie ritenute non più d'interesse pubblico. L'aspra diatriba che si aprì in seguito riguardava il fatto se Google avesse dovuto "delinkizzare" le notizie che potremmo definire "contaminate" solo nei confini dell'Unione Europea oppure in tutto il mondo. Il colosso americano optò, ovviamente, per la prima opzione mentre l'Autorità Garante francese (CNIL) ritenne più opportuna la seconda opzione: ebbene non c'è risposta che possa mettere d'accordo tutti dato che in tempi recenti l'Autorità Garante italiana ha imposto la "delinkizzazione" oltre i confini del suolo europeo di una notizia su un cittadino italiano residente, però, negli USA. Questo è accaduto per via del fatto che costui sarebbe stato danneggiato dall'articolo in entrambi i contesti, europeo e statunitense. Data la particolarità del caso l'Autorità italiana è ben più allineata alla posizione del CNIL piuttosto che a quella di Google. Tuttavia il "diritto alla cancellazione" che è possibile leggere nell'articolo 17 del GDPR non ha nulla a che vedere con quanto detto poche righe indietro per essere chiari. Questo infatti indica il diritto di cancellazione dei dati di una persona fisica, esteso e regolato anche con riferimento alla società digitale. Per un verso questo articolo conferma ed adatta al mondo digitale una delle colonne portanti del diritto inerente alla cancellazione dei dati: quando quest'ultimi non sono più utili alle finalità per cui sono stati raccolti oppure quando viene revocato il consenso per il loro utilizzo è giusta la loro eliminazione. Secondo la nuova normativa è prevista la cancellazione dei dati qualora essi siano trattati illecitamente; viene aggiunta la cancellazione dei dati anche nei casi previsti esplicitamente dalle leggi dello Stato. Inoltre è vietato l'uso dei dati di minori di sedici anni senza il consenso di chi ne detiene la responsabilità genitoriale: qualora si venisse in possesso di questa tipologia di dati, essi dovranno venire cancellati; in secondo luogo è bene sottolineare il fatto che il limite d'età può essere posto dallo Stato membro purché il limite minimo non sia inferiore a tredici anni. La parte veramente innovativa di questo diritto contenuto nel GDPR, però, è un'altra: riguarda il dovere specifico del Titolare, il quale riceve una richiesta di cancellazione, di eliminare le informazioni in questione pubblicate da lui stesso. Secondo l'articolo 17 al

Titolare non viene solo imposto di cancellare i dati, di fatti egli deve ,*"tenendo conto della tecnologia disponibile e dei costi di attuazione"* (Commissione Europea, 2018), adottare *"misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali"* (Commissione Europea, 2018).

La norma in questione è molto complessa soprattutto nell'attuazione: in sostanza, infatti, viene richiesto al Titolare dei dati di fare da "intermediario" tra l'interessato (chi ha fornito i dati) e tutti coloro che si trovano a trattare i dati di quest'ultimo. Se le informazione sono state diffuse in via pubblica dal Titolare si presume che questo sia a conoscenza che altri titolari li stiano trattando. L'obbligo di "intermediazione" scatta sempre quando l'individuo richiede la cancellazione di qualsiasi copia o immagine dei suoi dati personali: viene valutata la richiesta di questa cancellazione dal Titolare a cui sono stati rilasciati per la prima volta i dati; una volta accettata questo deve essere a conoscenza degli altri soggetti che utilizzano i dati dell'utente in modo tale da inoltrare a loro la richiesta di cancellazione, la quale sarà valutata indipendentemente da ogni "sub" Titolare. Tuttavia la norma sembra porre dei limiti al dovere del Titolare che ha reso pubblici i dati: egli non sembra essere tenuto a comunicare all'utente di aver segnalato la richiesta di cancellazione delle informazioni ai "sub" titolari anche se, seguendo il principio di trasparenza dell'articolo 12 e quello dell'*accountability* dell'articolo 5, è lecito pensare che il dovere d'informativa debba comunque essere tenuto in considerazione; il Titolare ha soltanto il dovere di segnalazione e non quello di monitorare il comportamento degli altri titolari né di informare l'interessato su quest'ultimi; infine, è possibile affermare che il dovere di segnalazione può trovare un limite nella tecnologia a disposizione e nei costi se questi ultimi non siano ritenuti ragionevoli. (Pizzetti, 2018)

3.2.2 Il diritto alla portabilità dei dati.

Seguendo quanto scritto anche in precedenza il secondo diritto che è stato introdotto con il GDPR è quello di portabilità dei dati: questo è indicato nell'articolo 20 della normativa. Il primo comma stabilisce che qualsiasi soggetto che sia a conoscenza del fatto che i suoi dati sono oggetto di trattamenti automatizzati compiuti dal Titolare, autorizzati dal suo consenso o per contratto, è libero di chiedere che i dati da lui stesso forniti siano trasmessi ad un altro Titolare o a sé stesso senza impedimenti con un formato *"strutturato, di uso comune e leggibile da dispositivo automatico"* (Commissione Europea, 2018). Tale scrittura possiede una duplice funzione: quella di conferire un maggior potere di controllo al titolare dei dati e la possibilità di facilitare la trasmissione di quest'ultimi ad un altro Titolare, tale mansione in particolare ha il compito di facilitare la libera circolazione dei dati e lo sviluppo dell'economia digitale, favorendo la concorrenza fra i diversi fornitori di beni o servizi. Come per ogni nuova norma anche per questa, in un primo momento, sono emersi dei dubbi e delle incomprensioni: è lecito per un cittadino chiedersi quanto sia vasta la quantità di

informazioni trattate che egli possa richiedere di avere o di mandare ad un altro Titolare. In un primo momento si è pensato, in maniera erronea, che l'utente potesse richiedere non solo i dati da lui forniti ma anche tutte le informazioni da essi derivanti, in particolar modo le valutazioni che il Titolare ha compiuto sul soggetto stesso, siano queste positive oppure negative, ad esempio: se fosse ritenuto un buon pagatore oppure no, se fosse giudicato un paziente ad alto o basso rischio di malattia, *etc*. Ovviamente se tutto ciò diventasse possibile il diritto in questione assumerebbe una posizione di rilievo: tuttavia fornire questa mole di informazioni ad un consumatore sarebbe estremamente oneroso per un'impresa dato che sarebbero costrette ad utilizzare formati di uso comune per fornire i dati ma anche, e soprattutto, perché le valutazioni effettuate da un'azienda sono frutto di analisi basate sul ricorso a tecniche di Big Data e di Data Analysis che costituiscono un patrimonio per l'impresa e sono in molti casi frutti di opere d'ingegno di alto valore (tipo gli algoritmi). Come già accennato ciò non è minimamente possibile ed il diritto alla portabilità dei dati non arriva fino a tal punto. Questo fondamentalmente concede all'individuo un maggiore controllo sulle proprie informazioni dato che gli consente di sapere quali sono i dati trattati dal Titolare e di riceverli in un formato strutturato, di uso comune e leggibile in un dispositivo automatico oltre a poter richiedere che i suoi dati siano trasferiti ad un altro Titolare da lui stabilito. È doveroso, però, sottolineare il fatto che il diritto in questione può essere esercitato qualora venissero rispettate le seguenti due condizioni: il trattamento deve essere effettuato con mezzi automatizzati e la portabilità deve essere basata sul consenso dell'utente oppure su un contratto firmato dallo stesso. Dunque questo non è un diritto riconosciuto a tutti gli individui essendo indissolubilmente legato ai trattamenti automatizzati che caratterizzano la società digitale, proprio per quest'ultima caratteristica è stato definito "nuovo": in termini leggermente differenti e limitatamente ai servizi della società dell'informazione era già previsto nella direttiva "*e-privacy"* 2002/58/CE ed aveva come destinatari principali i provider telefonici. Ovviamente tale norma è stata modificata e riadattata con il GDPR. Il secondo paragrafo dell'articolo 20 del GDPR prevede un onere a cui i Titolari devono adempiere con particolare attenzione: la trasmissione dei dati da un Titolare da un altro per volontà dell'interessato. Il testo rimarca che questa deve avvenire solo se *"tecnicamente fattibile"* (Commissione Europea, 2018) dato che, qualora vi fosse una eccessiva complessità tecnica o addirittura un'impossibilità nella trasmissione dei dati dovuti ad inadeguatezze o difficoltà dei sistemi digitali, il Titolare può rifiutarsi di adempiere a quanto previsto dal nuovo regolamento. Inoltre è possibile affermare che il WP29 *(European Data Protection Board)* per facilitare i passaggi dei dati raccomanda che associazioni di imprese omogenee promuovano il più possibile l'adozione di formati standard che permettano l'esecuzione di questo diritto. È importante anche sottolineare il fatto che l'esercizio di questo diritto non implica una cancellazione dei dati dell'utente o un cambiamento del rapporto esistente tra quest'ultimo ed il Titolare: l'individuo può infatti richiedere la trasmissione dei dati per molte evenienze, di fatti tali informazioni possono risultare utili anche per firmare un contratto di fornitura di servizi totalmente

diversi da quelli erogati dal Titolare verso il quale è rivolta la richiesta. Seguendo quanto stabilito nel quarto comma dell'articolo l'esercizio del diritto di portabilità non deve ledere la libertà ed i diritti altrui. Per concludere è bene accennare ad una questione da molti ritenuta "spinosa" e riguardante tale articolo. Di fatti nel testo si specifica che questo diritto viene applicato ai dati dell'interessato e che sono forniti da lui stesso ad un Titolare per farli trattare in maniera automatizzata: si deve intendere quali sono i dati dell'interessato, da un lato, e quando essi possono essere intesi come forniti direttamente dallo stesso, nell'altro. Ragionevolmente questi sono dati che sono stati forniti dall'individuo al Titolare sotto richiesta di quest'ultimo in ragione del consenso prestato o del contratto stipulato, tuttavia quando il consumatore richiede indietro i propri dati oppure la loro trasmissione ad un altro Titolare è possibile che vengano comunicate anche informazioni riguardanti terze persone, data l'autorizzazione dell'individuo. Tuttavia, secondo quanto stabilito dalla WP29, i dati dei terzi, seppure oggetto di portabilità, non potranno essere utilizzati né dall'interessato né dal nuovo Titolare a meno che non sussista una base specifica, autonoma e diversa che autorizza il loro trattamento (art. 6 lettera a) e art.9): qualora essa non sussista allora sarà necessario informare esplicitamente i terzi, seguendo quanto scritto nell'articolo 14. (Pizzetti, Portabilità dei dati nel GDPR: cosa significa e cosa implica questo nuovo diritto, 2018)

Infine, per concludere questa panoramica sul GDPR, è necessario trattare un'altra delle tematiche più importanti: le sanzioni.

Nei fatti in precedenza è stato scritto delle numerose caratteristiche che distinguono il GDPR dai precedenti regolamenti sulla privacy: i macro temi, oltre alle sopracitate sanzioni, sono l'ambito territoriale di applicazione della norma, l'ottenimento del consenso e l'introduzione di una nuova figura, il DPO. Tutti già citati in precedenza.

Le violazioni del regolamento GDPR possono essere punite con vari gradi di sanzioni, sino ad arrivare a cifre molto elevate. Le trasgressioni che saranno sanzionate più aspramente, come la mancata acquisizione del consenso da parte dell'impresa, potranno essere punite con una multa pari a venti milioni di euro oppure, in alternativa, pari al 4% del fatturato annuo. Nei casi migliori possono esserci multe pari a dieci milioni di euro piuttosto che il 2% del fatturato annuo. Le imprese e gli enti, data l'introduzione del principio dell'*accountability* (responsabilizzazione dei titolari del trattamento), saranno i soggetti maggiormente colpiti seguendo quanto scritto sulla norma.

3.3 Impatti del GDPR sulle PMI.

Il GDPR è stato introdotto con una importante consapevolezza da parte dei membri dell'Unione Europea: esso, infatti, sarebbe servito per proteggere al meglio i dati degli utenti. Questa maggiore fiducia avrebbe poi permesso di sviluppare più in fretta il mercato digitale europeo in maniera senz'altro più sicura.

La nuova normativa europea inerente la protezione dei dati avrà sicuramente un importante impatto in ogni tipo di azienda. Questa situazione risulta sicuramente essere una conseguenza del fatto che nell'era digitale in cui viviamo le imprese ricorrono spesso e volentieri all'analisi delle informazioni sugli utenti a loro disposizione per commercializzare al meglio i propri prodotti: a questo proposito non possono essere ignorati i rischi che le nuove tecnologie portano con sé, come violazioni della privacy piuttosto che attacchi cyber.

Questi rischi sono una reale minaccia per ogni tipo di azienda, in particolar modo per quelle più piccole che hanno basato il loro business su una sola linea di prodotti o servizi e che possiedono risorse limitate, potendo compromettere la loro esistenza. Il regolamento ha, quindi, anche il ruolo di prevenire tali, spiacevoli, avvenimenti.

Come scritto in un articolo di Francesca Spidalieri è necessario distinguere tre fondamentali questioni inerenti questa normativa: il buono, il brutto ed il cattivo che la legge porta con sé per le PMI.

Il GDPR richiederà alle imprese, sia grandi che piccole, di effettuare dei cambiamenti non indifferenti nei loro protocolli di sicurezza, nel modo in cui vengono trattati i dati personali degli utenti e nella gestione generale delle ICT: tutto ciò per assicurare una giusta cura, una migliore custodia ed un adeguato controllo delle informazioni che hanno origine all'interno dei confini dell'UE.

Nonostante ciò a tutti questi buoni propositi è necessario affiancare il lato "brutto" del regolamento. In un versante è possibile trovare numerosi studiosi, avvocati *in primis*, i quali si chiedono se l'entrata in vigore del GDPR rappresenti realmente uno strumento per la protezione, nonché per identificare con chiarezza, delle informazioni personali di un utente: mettono perciò in dubbio l'efficacia e l'efficienza di tale normativa. Mentre nell'altro è possibile trovare tutti i titolari delle aziende, specialmente di piccole e medie imprese, che dovranno affrontare tutte le difficoltà del GDPR ed i suoi costi: sarà necessario adeguarsi ai cambiamenti procedurali e di organizzazione richiesti da quest'ultimo. Un esempio potrebbe essere quello riguardante l'obbligo di segnalazione e notifica di un ipotetico *data breach*: oltre a dover allertare l'Autorità Garante del Paese membro in cui si opera potrebbe dover essere necessario fare lo stesso con altri referenti, definiti *"point of contact"*, per ogni altro Stato membro. Trasmettere una tale quantità di informazioni potrebbe non essere agevole per una piccola impresa date le poche risorse e capacità a sua disposizione, considerato soprattutto che queste dovrebbero essere trasmesse in ventiquattro lingue differenti. Inoltre apportare cambiamenti significativi per un'azienda potrebbe voler dire rinunciare o rimandare gli investimenti verso lo sviluppo di nuove tecnologie e prodotti dal momento che sarà necessario investire budget, tempo e forze per adempiere ai nuovi obblighi derivanti dalla normativa europea che riguardano il trattamento e la mappatura dei dati nonché il

trasferimento transnazionale di quest'ultimi. Verosimilmente sarà l'area R&D (ricerca e sviluppo) ad essere maggiormente colpita da questo spostamento di risorse.

Il "cattivo" del GDPR è che la maggioranza delle piccole e medie imprese sono totalmente impreparate ed avranno numerose difficoltà ad applicare quanto previsto dalla normativa, soprattutto perché non dispongono delle capacità e delle risorse per creare programmi dettagliati per la sicurezza e per la privacy. Un altro problema risiede nel fatto che i titolari delle aziende non solo non sono preparati a questi cambiamenti ma non hanno nemmeno ben chiaro il regolamento. In alcuni casi non sono nemmeno coscienti di essere soggetti ad una nuova normativa che se non rispettata può costar loro molto caro. È bene ricordare che queste imprese hanno tempo fino ai primi mesi del 2019 per adeguarsi ed evitare delle aspre sanzioni. (Spidalieri, 2018)

Per quanto riguarda le PMI possono essere sottolineate quattro semplici regole per non temere il GDPR (Spidalieri, 2018):

1. Bisogna essere consapevoli dei tipi di informazioni che si detengono (ad esempio, *"personally identifiable information," "protected health information," "credit card information," etc.*), dove esse vengono custodite, chi ne ha accesso e come queste vengono protette.
2. È necessario capire quali sono i rischi ai quali si è esposti. In secondo luogo dovrà essere effettuata una valutazione delle misure tecniche e politiche di sicurezza esistenti, inclusi i piani di risposta ad eventuali incidenti ed il piano di continuità del business dopo un'interruzione. Una corretta allocazione delle risorse finanziare ed umane potrebbe minimizzare gli eventuali rischi. Infine tutti i dipendenti devono essere preparati ed aggiornati sul GDPR, nonché sulle modalità di protezione dei dati e di segnalazione delle violazioni.
3. Dimostrare una *"due-diligence"* della filiera e verificare che tutti i fornitori siano conformi a quanto scritto nel regolamento europeo onde evitare che essi stessi diventino la causa di un incidente informatico (*"third-party breach"*).
4. Infine, se si nota che è impossibile da parte dell'impresa ottenere e mantenere tutti i dati personali possibili relativi alla propria clientela per ragioni d'affari, sarebbe meglio non raccoglierli proprio o, in alternativa, cancellarli appena il loro trattamento è stato concluso.

È, inoltre, opportuno trattare in maniera più dettagliata i costi a cui andranno incontro molte delle imprese italiane e non dopo l'entrata in vigore di questa normativa.

Confesercenti, ad esempio, stima una spesa pari a due miliardi di euro per le imprese del nostro paese a causa del GDPR. IDC, nota società che effettua ricerche di mercato, parla di costi che si aggirano sui duecento milioni di euro: il 70% del loro campione ha dichiarato che avrebbe speso la maggior parte del budget destinato a questo "adeguamento" per implementare al meglio il sistema di notificazione di un eventuale *data breach*, dato che allertare le autorità competenti entro 72 ore dalla scoperta del

problema sembra essere la parte più "ostica" del nuovo regolamento sulla privacy. La parte rimanente avrebbe puntato ad implementare i sistemi di crittografia e mascheramento dei dati o in alternativa altri punti legati ai processi, come la gestione del consenso da parte dell'utente.

Nella realtà, come già accennato in precedenza, è piuttosto complicato che tutte le imprese d'Italia e d'Europa siano pronte entro il 2018 ad i cambiamenti apportati da questa nuova normativa. Seguendo quanto scritto in un rapporto *Capgemini* almeno il 48% delle aziende italiane ed il 25% delle aziende europee non saranno preparate per le variazioni derivanti dal GDPR entro la fine dell'anno. I dati, in effetti, corrispondo più o meno con quanto emerso ad inizio anno da un sondaggio di IDC in cui veniva dichiarato dal 60% delle imprese italiane prese in considerazione di essere in grado di adattarsi alle modifiche delle leggi europee sulla privacy entro il 25 Maggio del 2018, giorno in cui sarebbero entrate in vigore. La conclusione che è possibile trarre, sempre prendendo i dati *cum grano salis*, è che solo una piccola parte delle compagnie che si dichiaravano "pronte" non lo sono effettivamente state. (Vaciago, 2018)

Date queste premesse è anche bene sottolineare che il contesto italiano è difficilmente paragonabile ad altri Paesi europei data la proliferazione di piccole e medie imprese presenti sul nostro suolo: nel 2016 erano infatti 145 mila le PMI in Italia, numeri assolutamente unici che aiutano senz'altro a capire come il processo di "adeguamento" sarà differente per il Bel Paese.

Ad oggi non esistono dati reali inerenti le spese che queste imprese sosterranno per adattarsi al GDPR sebbene possa sembrare improbabile che una PMI con un fatturato non superiore ai cinque milioni di euro possa investire, complessivamente, oltre i 50 mila euro per l'adeguamento alla normativa ed oltre i 25 mila euro per la gestione ordinaria degli adempimenti previsti dal nuovo regolamento.

Una così ridotta capacità di investimento e risorse obbliga le nostre imprese ad effettuare strette maggiormente "strategiche". Possono infatti esserci due differenti approcci ai cambiamenti derivanti dal GDPR.

Il primo approccio è denominato *"legal".* Le società che puntano ad adottare tale metodo prediligono un adeguamento più formale che sostanziale della normativa. Ciò significa effettuare una revisione delle informative, delle *policies* dei dipendenti e delle regolamentazione del passaggio dei dati all'estero.

Il secondo tipo di approccio è chiamato *"tech"*. Con questo metodo, invece, molte imprese sfruttano la possibilità di riorganizzare le infrastrutture IT, spesso e volentieri inadeguate, per poter rispettare anche le misure minime che sono attualmente previste dal GDPR. Ciò significa creare sistemi di autorizzazione efficaci che altrimenti non esisterebbero (o sarebbero obsoleti), elaborare dei piani di *business continuity* e *disaster ricovery*, rimediare alla totale assenza di audit di seconda parte sui fornitori di servizi IT

ed infine adeguamento ed implementazione delle piattaforme *cloud* che non gestiscono il dato in maniera conforme con la normativa europea. (Vaciago, 2018)

I risultati di tale inadeguatezza, seguendo quanto scritto da IDC, porteranno il 78% delle imprese italiane a non essere pronte ai cambiamenti richiesti dalla nuova regolamentazione entro la fine del 2018.

Considerando che quasi certamente il budget, molto risicato, messo a disposizione dalle aziende rimarrà invariato (al massimo aumenterà in maniera non significativa) è possibile trovare tre soluzioni affinché le società risultino *compliant* al GDPR (Vaciago, 2018):

1. Scegliere un consulente. Questo nuovo regolamento comporta un differente paradigma nella gestione del dato ed il principio di *accountability* (essere in grado di dimostrare l'adeguatezza dei propri processi di *compliance*) pone l'esigenza di valutare in maniera molto attenta i professionisti che accompagnano l'impresa al processo di adattamento. Un incarico così delicato non può essere dato né ad un professionista del settore legale né esclusivamente ad una società informatica. La scelta dovrà ricadere su una figura o una proposta che riesca a contenere le due professionalità in maniera congiunta e coordinata.
2. Nomina di un DPO. È consigliabile per un'impresa nominare questa figura, che con il GDPR ha assunto una notevole importanza, il prima possibile evitando possibilmente di "pescare" all'interno dell'impresa stessa, a meno che non vi sia un soggetto con una competenza altamente specifica in materia. Qualora un'azienda avesse assunto un DPO prima di Maggio 2018 sarà agevolata data la possibilità di avere un maggiore raccordo tra questa figura ed i consulenti. Ciò potrebbe comportare un risparmio nella gestione futura degli adempimenti.
3. Investire in infrastrutture IT. Questo punto ha una rilevanza fondamentale e non deve essere sottovalutato. Si parta da un semplice presupposto: avere una soluzione *"low cost"* è difficile soprattutto quando si ha a che fare con l'adeguamento a standard internazionali in ambito IT. Il GDPR sotto questo punto di vista deve essere visto come una opportunità non solo per trattare in maniera adeguata i dati personali dei dipendenti o di terzi (clienti, fornitori, *etc.*) ma anche per costituire un sistema volto a proteggere il *know-how* aziendale, messo sempre più in pericolo da dipendenti poco fedeli oppure da cyber-criminali.

Per facilitare l'adeguamento a questo regolamento la Commissione Europea ha messo a disposizione sul suo sito ufficiale una serie di "domande frequenti" in modo da aiutare gli imprenditori ad adattarsi nel modo più veloce e facile possibile.

Ovviamente uno dei quesiti che ci si pone più ripetutamente è: *"le norme in questione si applicano a tutte le PMI?"*. (Commissione Europea, 2018)

La risposta che danno i legislatori è, ragionevolmente, negativa. Nei fatti l'applicazione della norma non dipende dalla grandezza dell'azienda ma dalla natura dell'attività di quest'ultima. Gli obblighi saranno più severi per quelle imprese che operano con i dati degli utenti e che ne mettono a repentaglio la loro libertà o i loro diritti; altri obblighi potrebbero non essere applicati ad alcuni tipi di PMI.

Ad esempio: le piccole e medie imprese che hanno al loro interno meno di duecentocinquanta dipendenti non sono tenute ad avere un registro delle loro attività di trattamento, a meno che il trattamento delle informazioni personali degli utenti non sia un'attività regolare e quindi costituisca una minaccia per i diritti e per la libertà di questi soggetti.

Proseguendo è possibile anche affermare che le PMI dovranno nominare un responsabile della protezione dei dati solo se il trattamento dei dati costituisce una delle attività *core* dell'azienda: in particolar modo, ovviamente, se questo avviene su larga scala. (Commissione Europea, 2018)

Per concludere: l'introduzione di nuovi diritti (*oblio* e *portabilità*) che impatto può avere sulle piccole e medie imprese?

È, infatti, possibile affermare che il diritto alla "portabilità dei dati" potrebbe favorire le piccole start-up verso una crescita più veloce. Avvalendosi proprio di questa portabilità dei dati esercitata a loro favore da parte dei clienti di imprese più strutturate ed avanti nell'analisi delle informazioni per fini valutativi, lo sviluppo dell'azienda subirebbe un'importante accelerazione e la stessa otterrebbe una maggiore competitività ma, nonostante tutto, manterrebbe dei grandi risparmi. (Pizzetti, Portabilità dei dati nel GDPR: cosa significa e cosa implica questo nuovo diritto, 2018)

3.4 Impatti del GDPR sulle multinazionali e sui grandi provider di dati.

È opportuno in questa sede esaminare anche cosa ha comportato l'introduzione del GDPR per i grandi provider di dati, quali possono essere società come Facebook e Google, ma anche per le compagnie multinazionali in generale.

Le questioni che necessitano una maggiore attenzione sono, indubbiamente, tre: i costi di adattamento a questo nuovo regolamento per le multinazionali e come queste hanno intenzione di adeguarsi alla legge; l'impatto che questa normativa ha avuto verso alcuni sistemi di contenimento delle informazioni per i provider di dati ma anche per le aziende stesse, in particolar modo il *cloud*; le reazioni di alcuni colossi del web come Facebook e Google.

Si analizzino quali saranno i costi che le multinazionali saranno tenute a sostenere.

Ernst & Young ha da poco pubblicato uno studio utilizzando un campione di seicento esperti di privacy dal quale emergono i seguenti dati (Vaciago, 2018):

- Circa il 75% delle multinazionali europee (sono considerate tali solo le aziende che hanno più di 75.000 dipendenti nel mondo) hanno previsto una spesa complessiva di cinque milioni di euro per l'adeguamento al GDPR oltre a l'assunzione di almeno due o tre dipendenti che si dedicheranno interamente al tema della privacy. Potrebbe essere uno spunto suggestivo notare che negli Stati Uniti solo il 50% delle imprese effettueranno degli investimenti simili a quelli delle companies europee. Uno dei principali motivi di tutto ciò potrebbe derivare dalla mancanza di necessità ad un tale adattamento, di fatti non è da escludere che molte di queste società siano "avanti nel percorso" rispetto alle concorrenti europee.
- Su 30 mila aziende seguite dai seicento studiosi coinvolti in questa analisi solo il 60% sarebbero state *"fully compliant"* (pienamente conforme) entro il Maggio 2018. Molte società si sono rese conto a pochi mesi dall'entrata in vigore del regolamento che non sarebbero riuscite ad adattarsi in tempo, fortunatamente la normativa sarà pienamente operativa solamente dopo i primi mesi del 2019.
- Il valore medio di investimento effettuato nel 2016 dalle aziende per l'adeguamento al GDPR era pari alla somma di 349 mila euro, mentre nel 2017 la quota era salita a 480 mila euro. L'importo in questione è rappresentato dai costi HR derivanti dalla figura del DPO, dai costi per i consulenti e dagli investimenti in infrastrutture IT per risultare conformi alla normativa. Complessivamente nel 2017 sono stati spesi 6,5 miliardi di euro da 30 mila aziende per questo adeguamento.

Inoltre, bisogna tener conto che le aziende multinazionali ritengono che i dati dei clienti siano fondamentali per il perseguimento di un vantaggio competitivo. Tuttavia è necessario considerare che compagnie di una certa grandezza ed importanza operano anche fuori i confini dell'Unione Europea e, nonostante uno degli aspetti innovativi del GDPR abbia a che fare proprio con la territorialità, potrebbero eludere i vincoli posti dall'Europa. A tal riguardo è necessario affermare che il legislatore è "corso ai ripari" per evitare una tale eventualità con gli articoli 44 e successivi.

Secondo il GDPR, infatti, il trasferimento dei dati è concesso solamente se il Paese, o l'organizzazione, terzo disponga di misure di sicurezza per le informazioni personali simile (o comunque approvata) a quella dell'UE: sebbene solitamente sia necessaria l'autorizzazione della Commissione Europea per il trasferimento dei dati in determinati casi essa può non essere richiesta, questo qualora la Commissione stessa abbia già ritenuto il Paese in questione adeguato nelle procedure di protezione dei dati. Ciò è scritto nel primo comma dell'articolo 45 della normativa in cui si recita letteralmente: *"Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio*

o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche.". Perciò in determinati Paesi "sicuri" non è nemmeno richiesta l'autorizzazione della Commissione europea per il trasferimento dei dati: cosa, però, porta un Paese ad essere considerato sicuro? Uno Stato è ritenuto tale qualora gli "standard di civiltà" siano simili o uguali a quelli che vigono nei confini europei, ci si riferisce perciò alle norme in tema di diritti umani, a quelle che vengono ritenute le libertà fondamentali in quel determinato Paese, la legislazione generale e settoriale riguardante la sicurezza pubblica, la difesa nazionale, il diritto penale e l'ordine pubblico. È inoltre opportuno che, ad intervalli periodici, la Commissione verifichi il livello di protezione nei Paesi terzi ritenuti "sicuri". (GVC consulenti di direzione associati, 2018)

Seguendo, invece, quanto scritto nell'articolo 46 in caso di assenza di adeguatezza (perciò di mancanza di autorizzazione da parte dell'Unione Europea per trasferire i dati) è il Titolare del trattamento a dover fornire alla Commissione europea delle adeguate garanzie a tutela degli interessati per compensare la carenza di protezione. Le garanzie che dovranno essere fornite possono, per esempio, consistere nell'applicazione di norme vincolanti d'impresa, clausole contrattuali autorizzate dall'autorità di controllo o, alternativamente, clausole-tipo di protezione dei dati adottate dalla Commissione.

L'articolo 47 si riferisce in maniera esplicita alle imprese e prevede che un gruppo di imprese che svolge un'attività economica comune può applicare le norme vincolanti d'impresa approvate per i trasferimenti internazionali dall'Unione Europea agli organismi del gruppo stesso, a condizione che queste norme contemplino tutti i principi fondamentali ed i diritti azionabili che costituiscono adeguate garanzie per il trasferimento dei dati personali.

Le norme vincolanti d'impresa dovrebbero indicare e specificare:

- Le procedure per il reclamo;
- I diritti dell'interessato ed i mezzi per esercitarli;
- I trasferimenti delle informazioni (i tipi di dati, come vengono trattati e la finalità per la quale vengono studiati);
- I compiti che hanno i responsabili della protezione dei dati;
- Le modalità con la quale sono state fornite le informazioni dell'interessato;
- La natura giuridicamente vincolante delle norme, sia a livello interno che a livello esterno;
- I meccanismi inerenti le modifiche delle norme;
- I meccanismi volti a garantire la conformità delle norme vincolanti d'impresa;
- I meccanismi di cooperazione con l'autorità di controllo e l'appropriata formazione del personale in materia di protezione dei dati al personale che ha regolarmente accesso alle informazioni dei consumatori;

- La struttura e le coordinate di contatto del gruppo imprenditoriale e di ognuno dei suoi membri.

Infine è di rilevante importanza anche l'articolo 49 che introduce i casi di deroga agli articoli 45 (in mancanza di decisione di adeguatezza) e 46 (mancanza delle garanzie richieste dal GDPR affinché un Paese risulti adeguato).

Vi è infatti la possibilità di trasferimento dei dati personali di un utente qualora questo abbia esplicitamente acconsentito, se il trasferimento delle informazioni è occasionale e necessario per la stipulazione di un contratto o per mettere in atto un'azione legale, in alternativa se ci sono motivi di rilevante interesse pubblico previsti dal diritto dell'Unione oppure se i dati sono trasferiti in un registro stabilito per legge e sarà destinato ad essere consultato da persone aventi legittimo diritto (solo in questo caso però il trasferimento non dovrebbe riguardare la totalità dei dati a disposizione).

Qualora la Commissione non avesse adottato alcuna decisione circa il livello di adeguatezza inerente la protezione dei dati di un Paese terzo il Titolare dovrebbe ricorrere a delle soluzioni che diano dei diritti effettivi all'interessato e la possibilità di esercitarli, dopo il trasferimento, così da continuare a godere di alcune garanzie e diritti fondamentali.

Questi articoli, sebbene sembrino complessi, hanno il ruolo di proteggere i dati nel momento più delicato ed in cui essi sono più vulnerabili: quando questo transita verso un Paese che non possiede una cultura del *"data protection"* simile a quella europea. (GVC consulenti di direzione associati, 2018)

Una seconda questione che ha assunto una notevole importanza con l'introduzione del GDPR riguarda gli impatti che esso può avere sui servizi *cloud*.

I motivi di questa rilevanza sono essenzialmente due: il primo riguarda il fatto che il *cloud* è ad oggi uno dei sistemi di archiviazione dei dati più utilizzati, complice il fatto che non comporta molte spese; la seconda ragione risiede proprio nel nuovo regolamento per la privacy dato che alcuni articoli regolano i rapporti tra i Titolari del trattamento dei dati e coloro che forniscono i servizi *cloud.*

Secondo quanto dichiarato da Vittorio Bitteleri, country manager di *CommVault* per l'Italia, è innanzitutto necessario che le aziende verifichino cinque fondamentali aspetti inerenti i servizi "SaaS" (*"Software as a Service"*) (Bitteleri, 2018):

1. Se il paese in cui sono localizzati i Saas o i *cloud* risponde ai requisiti di protezione dell'UE.
2. Se sarà possibile controllare dove saranno i dati dopo che il fornitore del SaaS o del *cloud* è stato scelto.
3. Quale è il processo di notifica e risoluzione dopo una eventuale violazione.
4. Quali sono le credenziali fornite dal servizio *cloud* per il GDPR.

5. Coloro che forniscono i servizi *cloud* si inseriscono nell'area dei *Data Processor* e le aziende, coloro che acquistano il servizio, saranno i *Data Controller*. Bisogna verificare che i dati siano trattati in maniera conforme al GDPR da entrambi i soggetti.

Quanto alla normativa è possibile affermare che il legislatore europeo sta facendo tutto il possibile affinché il mercato sia indirizzato verso l'esternalizzazione dei servizi inerenti la protezione dei dati: da un lato per avere una maggiore sicurezza e dall'altro per esternalizzare i trattamenti delle informazioni da parte delle imprese.

Tutto ciò ha ovviamente un senso. Negli ultimi anni abbiamo assistito ad attacchi informatici sempre più frequenti che hanno messo a repentaglio la sicurezza dei dati di migliaia di persone. Così facendo i legislatori europei tentano non solo di accentrare la gestione della sicurezza ma anche di innalzare i livelli generali di protezione contro le minacce in modo tale che diventi quasi impossibile riuscire ad ottenere (in maniera illecita) i dati degli utenti.

Le novità che sono contenute dalla normativa si riferiscono all'aggravamento della posizione del *Data Processor* (quindi il *cloud provider* che solitamente agisce in qualità di responsabile del trattamento), all'aumentata attenzione ai profili relativi alla sicurezza od ai maggiori oneri di formalizzazione degli obblighi correlati al trattamento dei dati che renderanno gli accordi di servizio più trasparenti e dettagliati.

Così facendo le aziende si ritroveranno a potere accedere a servizi (*cloud*) che avranno non solo un costo molto contenuto ma anche un livello di sicurezza che, verosimilmente, nessuna azienda italiana media riuscirebbe ad avere e mantenere in maniera autonoma al proprio interno.

È l'articolo 82 della normativa a sancire una maggiore responsabilizzazione dei *cloud providers* e costituisce una delle novità assolute introdotte dalla nuova normativa: nei fatti, a differenza del passato, il *cloud provider* insieme all'azienda titolare del trattamento potrà rispondere in maniera diretta e pari all'intero ammontare del danno cagionato all'utente. Ciò può accadere in due casi differenti: qualora non abbia adempiuto in maniera corretta agli obblighi che il GDPR pone in capo ai responsabili o, in alternativa, qualora essa abbia agito in maniera difforme rispetto alle istruzioni ricevute dal Titolare.

Inoltre è possibile affermare che il legislatore ha ritenuto opportuno introdurre un approccio *"risk based"* in cui non solo l'azienda in questione dovrà "misurare" i rischi che corre valutando l'adeguatezza dei livelli di sicurezza garantiti dal provider di volta in volta e se questi siano sufficientemente adeguati per i rischi insiti al trattamento dei dati, ma anche il provider stesso dovrà mettere in atto misure tecniche ed organizzative adeguate rispetto ai servizi che offre. La pena a cui si rischia di andare incontro qualora

ci siano dei trattamenti illeciti o delle violazioni delle prescrizioni di legge è l'esposizione sanzionatoria e risarcitoria.

L'introduzione di questa normativa impone ai *cloud providers* nuovi oneri di formalizzazione che impongono a questi soggetti una maggiore trasparenza ed una maggiore chiarezza nella redazione degli accordi di servizio; alle aziende, d'altro canto, viene richiesta una maggiore attenzione ai contenuti contrattuali. La norma di riferimento per tutto ciò è l'articolo 28 la quale contiene un elenco di contenuti puntuali e specifici che dovranno forzatamente corredare l'accordo con il *cloud* provider. Nel regolamento viene stabilito che il ricorso al subappalto è trasparente: il provider dovrà, oltretutto, garantire il ribaltamento sui subappaltatori degli stessi obblighi a cui esso stesso è vincolato (in particolare quelli inerenti la sicurezza) rispondendo in maniera diretta nei confronti del consumatore in caso di eventuali inadempimenti della propria catena di subfornitura. Nell'eventualità in cui il contratto autorizzasse il provider a ricorrere al subappalto le possibili sostituzioni dei subappaltatori debbono essere comunicate al cliente al quale spetterà la facoltà di opporsi, qualora manifesti del dissenso riguardante la modifica, esercitando il diritto di recesso dal contratto senza alcun tipo di costo od onere.

Vi sono ulteriori obblighi in capo al provider di dati:

- L'obbligo o la restituzione dei dati personali dei clienti dell'azienda una volta concluso il contratto di servizio con quest'ultima.
- Obbligo di comunicazione qualora vi sia un cosiddetto "*data breach"*. Questo comporta la perdita, la distruzione, la modifica, la divulgazione non autorizzata oppure l'accesso ai dati provocato in maniera accidentale o illecita.
- Obbligo da parte del provider di assistere e cooperare con l'azienda cliente (Titolare del trattamento dei dati) per notificare gli eventuali *data breaches* all'Autorità garante e, in secondo luogo, comunicarli ai consumatori.
- Dovere di assistenza all'azienda nell'effettuare la DPIA (valutazione d'impatto della protezione dei dati) e l'eventuale consultazione preventiva se previsto per legge.

È, quindi, possibile affermare che il GDPR rappresenta per il servizio *cloud* un'opportunità per maturare, favorendo anche la loro espansione sul mercato: la responsabilità che pende sui providers di servizi li "costringe" ad accrescere la fiducia che i clienti possono riporre in loro, l'affidabilità del servizio e la loro competitività nel panorama economico. Inoltre anche le imprese saranno incoraggiate nell'investire sui servizi *cloud*. Oltre ai motivi accennati in precedenza (costi minori e sicurezza maggiore) è fondamentale ricordare che l'Unione Europea, con questo nuovo regolamento, tenta di indirizzare i providers di dati ad effettuare pratiche contrattuali più eque, trasparenti e bilanciate, differentemente da quanto poteva accadere in passato, incoraggiando le imprese ad affidarsi sempre di più a questi servizi. (Italiano, 2018)

Per concludere, secondo quanto riportato anche dal *Sole 24 Ore,* alcuni colossi del web come Facebook e Google hanno avuto non pochi problemi con l'entrata in vigore di questo nuovo regolamento inerente la privacy ed i dati personali.

Le complicazioni per i due giganti derivano da un'associazione no-profit chiamata *"None of your business"*, letteralmente "non sono affari tuoi", che è stata fondata da un avvocato austriaco chiamato Max Schrems: quest'ultimo, a trent'anni, ha alle spalle già una bella e fortunata carriera. Nei fatti il legale ha iniziato una battaglia già da qualche anno utilizzando tutti gli strumenti a sua disposizione per ridimensionare le ingerenze delle imprese ICT nella vita dei loro clienti.

La sua associazione ha già presentato quattro reclami distinti verso: Android, il sistema operativo mobile di Google; Facebook; due delle sussidiarie di quest'ultima società, Instagram e WhatsApp.

L'accusa che è stata rivolta da "*None of your business*" alle aziende citate in precedenza è quella di aver richiesto una sorta di "consenso forzato" ai propri utenti, inondando gli smartphone ed i computer dei clienti con messaggi *pop-up* che pongono, anche se il termine "impongono" sarebbe più adatto, il via libera all'utilizzo delle loro informazioni personali.

Schrems precisa che, secondo il GDPR, il consenso debba essere rilasciato in un clima di profonda ed assoluta libertà senza subire dei pressing esterni, contrariamente a quanto è accaduto. Nei giorni successivi all'entrata in vigore di questa nuova normativa alcuni utenti sono stati tempestati di email e banner che avevano il chiaro intento di "mettere alle corde" gli individui: se non si accettano i *terms of use,* o condizioni d'uso, il servizio non sarebbe stato disponibile.

"Sono comparse tonnellate di "box di consenso" spinte online o sulle app. Spesso combinate con la minaccia che il servizio non sarebbe più stato accessibile senza un assenso esplicito" ha affermato l'avvocato durante un'intervista.

I quattro reclami, che sono stati presentati tra fine Maggio ed inizio Giugno, saranno gestiti a loro volta da quattro Autorità Garanti differenti per altrettanti Paesi dell'Unione Europea. Di fatti: delle accuse rivolte ad Android se ne occuperà l'Autorità francese, la *Commission Nationale de l'Informatique et des Libertés*, che potrà punire l'imputato con una multa massima di 3,7 miliardi di euro; la belga *Data Protection Authority* gestirà il caso che vede dal lato dell'accusa il social di sole immagini, Instagram, a cui verrà richiesto un importo pari ad 1,3 miliardi di euro; la tedesca *Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit* esaminerà il caso che ha come protagonista il principale sistema di messaggistica al mondo, WhatsApp, e le eventuali infrazioni commesse da tale impresa con una possibile sanzione di 1,3 miliardi di euro; la DBA, conosciuta anche come *Datenschutz behörden,* Autorità austriaca cercherà di

fare chiarezza sul comportamento tenuto da Facebook, il quale rischia una multa di 1,3 miliardi di euro.

Il punto saliente dell'accusa, anche come accennato prima, risiede nel fatto che seguendo quanto scritto nel GDPR è vietato alle aziende far dipendere l'accesso ad un servizio da un consenso che può essere dato o meno, seguendo la logica del *"prendere o lasciare"*. È vietato, quindi, negare un servizio da parte di un'impresa ad un cliente che non si adegua e non concede il servizio.

Secondo l'associazione la fine di questa era del "consenso forzato" non danneggerebbe in alcun modo le aziende dato che il trattamento dei dati sarà comunque possibile qualora si dimostrasse la necessità di alcune informazioni; tuttavia con la fine di questo "assedio" dei *pop-up* la qualità della navigazione sarebbe maggiore e la competitività delle PMI aumenterebbe, riequilibrando leggermente il mercato, dato che queste ultime non possono permettersi gli stessi toni e gli stessi investimenti di una *big company* per incalzare gli utenti sulla propria disponibilità ad accettare le condizioni d'uso di un servizio.

Dal canto loro Facebook e Google hanno immediatamente dichiarato, una volta pubblicate le accuse di Max Schrems, di essere a lavoro già da mesi per garantire il massimo dell'osservanza della normativa e che continueranno a lavorare su tale fronte, respingendo tutte le accuse.

Tuttavia Facebook e Google non sono state le uniche due imprese a pressare gli utenti per assicurarsi di continuare ad avere un contatto con l'azienda: molti utenti l'indomani dell'introduzione del GDPR si sono resi conto che molte compagnie hanno inviato loro numerose mail anche se fra queste ultime e gli individui non erano mai intercorsi rapporti di alcun genere. Ciò nonostante ci sono anche alcune aziende, statunitensi per lo più, che contrariamente a quelle nominate in precedenza hanno preferito mettere in *stand-by* la loro attività in Europa per adattarsi quanto meglio a questa nuova normativa. La mattina del 25 Maggio 2018, infatti, molti dei lettori europei di alcune importanti testate USA come il *Los Angeles Times* hanno trovato nel sito web del loro giornale una pagina in cui vi era scritto: *"Sfortunatamente il nostro sito al momento non è raggiungibile nella maggior parte dei Paesi europei. Ci stiamo occupando del problema e ci impegniamo a esaminare le opzioni che supportano la gamma completa della nostra offerta digitale per il mercato europeo".* Anche se non specificato è chiaro che l'editore abbia voluto "prendere tempo" per adattarsi nella maniera migliore alle nuove regole senza correre il rischio di essere sanzionato. (Magnani, 2018)

Probabilmente tra i due approcci è preferito il secondo dai cittadini europei. Infatti, sebbene interrompere (anche se per un breve periodo) l'attività in Europa per una qualsiasi azienda possa risultare sconveniente è comunque meglio del rischio di incorrere in sanzioni o battaglie legali: ciò che potrebbe accadere a chi viola il GDPR e cerca di avere un consenso forzato da parte del cliente.

CAPITOLO 4: "FOCUS GDPR: LA FIGURA DEL DPO".

4.1 Il DPO una figura nuova (ma non nuovissima) ed i suoi compiti.

L'articolo 37 della nuova normativa sulla privacy europea introduce una figura da molti definita innovativa: il "Responsabile della protezione dei dati", meglio noto come DPO acronimo di *"Data Protection Officer"*.

Per molti l'introduzione di questo nuovo ruolo all'interno delle aziende europee ha rappresentato una novità significativa ma è opportuno sottolineare il fatto che tale personalità era già parzialmente nota alle imprese europee: nei fatti il DPO è una evoluzione della figura del *"privacy officer",* prevista dall'articolo 18 della direttiva 95/46/CE la quale stabiliva agli Stati membri di applicare delle semplificazioni o esoneri per le imprese che avessero nominato un soggetto indipendente al quale demandare l'applicazione delle normative statali di attuazione della direttiva stessa.

Già nel 2014 le norme interne di ben diciotto Stati membri dell'Unione Europea prevedevano la figura del *privacy officer*: essa poteva essere obbligatoria, in alcuni casi, o facoltativa in altri. In paesi come la Germania, ad esempio vi era una legge che imponeva la nomina di un PO qualora l'impresa in questione avesse avuto più di dieci dipendenti che trattavano i dati personali dei clienti in maniera automatizzata o, in alternativa, più di venti dipendenti che si occupano del trattamento delle informazioni personali dei consumatori qualora questo non sia automatizzato. Nemmeno in Italia la figura è totalmente nuova: è stata introdotta, infatti, pochi anni fa a seguito di alcune linee guida pubblicate sulla Gazzetta Ufficiale del luglio 2015. Il Garante della Privacy si auspicava, ragionevolmente data la delicatezza delle informazioni trattate, che: *"i titolari del trattamento individuino al loro interno una figura responsabile della protezione dei dati che svolga il ruolo di referente con il Garante"*.[7]

Negli Stati Uniti d'America la figura è ben più conosciuta e presente da più tempo. Il ruolo, la posizione aziendale ed i compiti sono uguali al DPO sebbene il nome della carica sia differente. Negli USA infatti chi ricopre questa funzione è chiamato CPO, *"Chief Privacy Officer"* ed è una delle figure maggiormente di spicco nelle gerarchie aziendali nonché uno dei dipendenti più pagati all'interno dell'impresa. La prima CPO della storia è stata Jennifer Barret Glasgow nel 1991 e lavorava per la Acxiom Corporation. (Comellini & Graziano, 2018)

[7] Testo tratto da Linee Guida, adottate il 4 Giugno 2015 e pubblicate sulla Gazzetta Ufficiale numero 164 del 17 Luglio 2015, in materia di Dossier Sanitario.

È bene analizzare quali siano i tre casi specifici che rendono obbligatorio per un'impresa assumere un DPO secondo quanto scritto nel primo paragrafo dell'articolo 37 del GDPR (Comellini & Graziano, 2018):

1. Qualora il trattamento fosse effettuato da un' "autorità pubblica" o, in alternativa, da un "organismo pubblico" sarebbe necessario assumere un Responsabile della protezione dei dati.[8] Secondo quanto stabilito dal Garante della Privacy devono ritenersi obbligate a designare un DPO tutti i soggetti che ricadono nell'ambito degli articoli 18-22 del Codice della Privacy. Gli esempi fatti sono le amministrazioni dello Stato (anche con ordinamento autonomo), gli enti pubblici non economici nazionali, regionali e locali, le università, le Regioni e le Camere di commercio, industria, agricoltura ed artigianato.
2. Se le "attività principali" del Titolare del trattamento o del Responsabile del trattamento consistono in operazioni che, per loro natura, ambito di applicazione e/o finalità, richiedono di monitorare su larga scala, in maniera regolare e sistematica, gli utenti. Per "regolare" viene inteso che questo avvenga in maniera continua e costante con alcuni intervalli periodici; quanto a "sistematico" si prevede che questo controllo venga svolto in maniera metodica, predeterminata e nell'ambito di una strategia. Seguendo quanto scritto sulle Linee Guida si possono intendere le attività principali come *"le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal Titolare o dal Responsabile del trattamento dei dati, comprese tutte quelle attività per le quali il trattamento dei dati è inscindibile connesso all'attività del Titolare o del Responsabile"*. L'esempio che viene riportato è quello dell'ospedale. Il trattamento dei dati relativi alla salute del paziente è ritenuta una delle attività principali di qualsiasi struttura ospedaliera. Da qui consegue l'obbligo di nomina di un DPO.
3. Nell'eventualità in cui le attività principali del Titolare o del Responsabile del trattamento comportino dei trattamenti su "larga scala" di dati giudiziari o dati ritenuti sensibili. Il regolamento in questo caso non fornisce un'adeguata spiegazione del concetto di "larga scala". Fortunatamente le Linee Guida, anche in questo caso, vengono in soccorso fornendo delle utili considerazioni. I fattori che possono influenzare il concetto di "larga scala" o meno sono: il numero di soggetti interessati al trattamento (espressi anche in percentuale rispetto alla popolazione presa a riferimento); la durata del trattamento; la portata geografica dell'attività di trattamento; il volume e le diverse tipologie dei dati che sono argomento di studio.

[8] Sono esentate da questo obbligo le autorità giurisdizionali nell'esercizio delle loro funzioni (Art. 32 direttiva UE 2016/68).

È bene sottolineare anche il fatto che la richiesta di nomina obbligatoria di un DPO può essere prevista dal diritto nazionale di uno dei Paesi membri.

Secondo quanto scritto nel paragrafo primo dell'articolo 39 del Regolamento al DPO vengono assegnati almeno i seguenti quattro compiti:

- Deve effettuare un'attività di informazione e consulenza al Titolare o al Responsabile del trattamento dei dati (inclusi i dipendenti che svolgono tale mansione) su gli obblighi che derivano dal regolamento e dalle altre disposizioni dell'Unione Europea o degli Stati membri riguardo la protezione dei dati. Inoltre questa figura ha un ruolo di supervisione dato che dovrà individuare i trattamenti svolti, analizzarli e vedere se sono in conformità con quanto stabilito dalle normative. È necessario prestare attenzione, infatti spetta al Titolare il compito di adottare tutte le misure tecniche e organizzative adeguate per garantire la conformità del trattamento con il Regolamento, non al DPO. Quest'ultimo è solamente un consulente e supervisore del trattamento.
- Sorveglianza sull'osservanza, da parte del Titolare o del Responsabile del trattamento dei dati, del regolamento e delle altre disposizioni provenienti dall'Unione Europea o dagli Stati membri riguardanti la protezione dei dati. Spetta al DPO anche la sensibilizzazione e formazione del personale che partecipa ai trattamenti e alle attività di controllo a loro connesse.
- Se richiesto si deve fornire un parere sulla "valutazione d'impatto" delle protezione dei dati e sorvegliarne l'adempimento, seguendo quanto scritto nell'articolo 35. Bisogna prestare molta attenzione anche in questo caso. Nei fatti non è il DPO che effettua una valutazione d'impatto (DPIA nell'acronimo inglese) ma il Titolare il quale non fa altro che seguire quanto scritto nell'articolo 35 del GDPR. Costui potrà decidere di consultarsi con il DPO durante la stesura della DPIA e, qualora volesse, potrebbe chiedere un suo parere in merito alla valutazione. Nella maggioranza dei casi i consulti tra DPO e Titolare del trattamento dei dati avvengono sulla decisione di effettuare una DPIA o meno; quali metodologie utilizzare per la stesura della DPIA; se quest'ultima è stata condotta correttamente o meno e se le conclusioni a cui si è arrivati siano conformi al Regolamento o meno[9]. È bene specificare come il Titolare possa benissimo rifiutarsi di seguire le indicazioni date dal DPO. In quest'ultimo caso nella documentazione devono essere evidenziati i motivi che hanno condotto il Titolare a non seguire i consigli che gli sono stati concessi dal Responsabile della protezione dei dati.

[9] Sono le Linee Guida (punto 4.2) a raccomandare quali siano i casi in cui è necessario per il titolare consultare il DPO riguardo la DPIA.

- Cooperare con l'autorità di controllo e fare da "punto di contatto" con quest'ultima per questioni legate al trattamento dei dati; inoltre è previsto il dovere da parte del DPO di effettuare delle consultazioni con l'autorità di controllo, qualora questa lo richiedesse, che hanno per oggetto anche altre questioni. Questo compito è fondamentale dato che il DPO facilita l'accesso dell'autorità ai documenti e alle informazioni che permettono a quest'ultima di esercitare al meglio i suoi poteri di indagine e correzione. Inoltre, nonostante il DPO sia tenuto a rispettare delle norme in materia di segretezza non è escluso che sia proprio questo a contattare l'autorità di controllo e chiedere "luce" su alcune vicende (articolo 39).

In precedenza è stato sottolineato come il Responsabile della protezione dei dati svolga *almeno* le funzioni appena elencate: ciò vale a dire che questa figura può svolgere anche altre mansioni. È opportuno, però, che in una grande compagnia il DPO si limiti a svolgere i compiti scritti sopra.

Al Titolare od al Responsabile del trattamento dei dati spetta l'obbligo di tenere, rispettivamente, un "registro delle attività di trattamento svolte sotto la propria responsabilità" o un "registro di tutte le categorie di trattamento svolte per conto di un Titolare del trattamento". Tuttavia in alcuni Paesi europei (come la Francia) è nata la prassi di far redigere il registro dei trattamenti dei dati direttamente ai DPO sulla base delle informazioni a loro disponibili.

Per concludere la panoramica dei compiti legati a questo ruolo il Garante chiede di verificare se l'individuo che ricopre tale posizione è condiviso con un'autorità pubblica: ciò potrebbe comportare un problema dato che esso potrebbe svolgere ulteriori compiti che presentino dei conflitti di interesse con quelli svolti da DPO; in alternativa, le sue prestazioni sul posto di lavoro come Responsabile della protezione dei dati potrebbero essere compromesse da questo doppio incarico. In questi casi nell'atto di designazione o nel contratto di servizio il DPO dovrà fornire opportune garanzie per assicurare la massima efficienza e correttezza nonché prevenire eventuali conflitti d'interesse. (Comellini & Graziano, 2018)

4.2 La nomina del DPO: a chi spetta ed i requisiti richiesti.

Per quanto concerne la nomina del DPO l'articolo 37 specifica come questa appartenga sia al Titolare del trattamento dei dati che al Responsabile del trattamento dei dati. La designazione, ovviamente, non spetta ad entrambi i soggetti in contemporanea e non sarà nemmeno necessaria una consultazione tra queste due figure per nominare un DPO di comune accordo. La nomina spetta solo a chi soddisfi i criteri relativi alla obbligatorietà della nomina.

Vi sono, inoltre, dei casi di particolare interesse che meritano una menzione: un'azienda potrebbe infatti non essere obbligata a nominare un DPO ma il Responsabile del trattamento, invece, si.

I due esempi forniti dalle Linee Guida sono i seguenti:

- Un'impresa di medie dimensioni incarica un responsabile esterno nella gestione di alcuni dati di notevole importanza. Può sicuramente capitare che il responsabile in questione abbia clienti molto simili all'azienda in questione e, quindi, si ritrovi a gestire numerosi dati simili fra loro di differenti aziende. In tale caso seguendo quanto scritto ai sensi dell'articolo 37 paragrafo 1 lettera b) [10], poiché lo svolgimento dei trattamenti avviene su larga scala il Responsabile sarà tenuto a nominare un DPO. Tuttavia l'azienda non è tenuta necessariamente a compiere lo stesso adempimento.
- Un caso analogo può essere fatto per una piccola impresa che assume un Responsabile del trattamento dei dati che ha, ad esempio, il compito di tracciare gli utenti del sito web nonché quello di fornire consulenza per attività di pubblicità e marketing mirato. Anche in questo caso, data la limitata grandezza dell'azienda, le attività svolte dall'imprese riguardanti il trattamento dei dati non sono di larga scala. Tuttavia quelle del Responsabile al quale ci si è rivolti possono esserlo, il che obbliga quest'ultimo a dover designare un DPO ai sensi dell'articolo 37 paragrafo 1 lettera b). Nonostante ciò l'azienda non è obbligata a nominare un Responsabile della protezione dei dati.

È opportuno chiedersi anche se vi può essere un unico DPO per un gruppo imprenditoriale. Quest'ultimo deve essere necessariamente inteso come un gruppo costituito da un'impresa controllante e dalle controllate[11]. In tal caso la risposta è si, purché il DPO sia raggiungibile da ogni stabilimento.

La "raggiungibilità" è un requisito fortemente legato ai compiti che sono assegnati a questa figura dalla normativa in quanto essa deve fungere da "punto di contatto" sia per i soggetti interessati dal trattamento dei dati, sia per le autorità di controllo ma anche per i soggetti che sono all'interno dell'ente o dell'organismo, ci si riferisce quindi al Titolare del trattamento dei dati, al Responsabile del trattamento dei dati oppure ai dipendenti che eseguono il trattamento. (Comellini & Graziano, 2018)

Da qui deriva la conseguenza che il DPO, con l'eventuale supporto di un gruppo di collaboratori, deve essere in grado di comunicare in maniera efficiente con gli

[10] *"e attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala"* (Commissione Europea, 2018).

[11] Ai sensi della definizione fornita dall'articolo 4, numero 19, del regolamento.

interessati e collaborare con le autorità di controllo: ciò comporta una facilità nell'essere raggiunto con adeguati mezzi di trasporto e mezzi di comunicazione sicuri.

Ugualmente è consentita la designazione di un unico DPO per molteplici autorità pubbliche od organismi pubblici. Ovviamente bisognerà tener conto della loro dimensione nonché della struttura organizzativa[12].

Le Linee Guida specificano che il titolare della nomina del Responsabile della protezione dei dati ha il compito di assicurarsi che questo sia in grado di adempiere alle sue funzioni in maniera efficiente, anche con il supporto di un gruppo di collaboratori eventualmente. Ancora, raccomandano che il DPO sia localizzato in uno dei Paesi membri dell'Unione Europea.

Una volta che l'ente o l'organizzazione hanno nominato il loro DPO debbono obbligatoriamente, seguendo quanto scritto nel paragrafo 7 dell'articolo 37, pubblicare i suoi dati di contatto nonché comunicarli alle autorità di controllo. Questi contatti devono permettere agli interessati di poter comunicare in maniera diretta con il DPO senza doversi rivolgere ad un'altra struttura operante presso il Titolare od il Responsabile del trattamento. Seguendo quanto scritto nelle Linee Guida (punto 2.6) fra i contatti debbono rientrare:

1) Il recapito postale;
2) Recapito telefonico;
3) Indirizzo e-mail.

Sarebbe un'ottima prassi che i dati di contatto del DPO siano forniti dal Titolare del trattamento anche ai dipendenti pubblicandoli, ad esempio, sull'intranet dell'azienda oppure inserendolo nell'organigramma della struttura.

È inoltre necessario precisare che la norma non richiede la pubblicazione del "nominativo" del DPO: tuttavia, qualora sia necessario notificare un *data breach* all'Autorità Garante, l'articolo 33 paragrafo 3 lettera b) richiede il nominativo del Responsabile della protezione dei dati tra le informazioni che debbono essere comunicate[13].

Secondo quanto viene affermato nel sesto paragrafo dell'articolo 37 il DPO può essere un dipendente del Titolare del trattamento dei dati, quindi un soggetto interno

[12] Articolo 37, paragrafo 3: *"Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione".*

[13] Articolo 33, paragrafo 3, lettera b): *"3. La notifica di cui al paragrafo 1 deve almeno: b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni".*

all'impresa che gestisce le informazioni, legato da un contratto di servizi oppure un soggetto esterno all'organismo.

Le Linee Guida chiariscono, ulteriormente, che il DPO può sia essere una persona fisica che una persona giuridica. In questo ultimo caso è indispensabile che ciascun soggetto che vi appartiene (nell'eventualità operi come DPO) abbia i requisiti fondamentali per essere un Responsabile della protezione dei dati elencati nella sezione quattro del Regolamento. Oltre ciò viene anche specificato che qualora la funzione del DPO sia ricoperta da un intero team, dato che ciò è ammissibile nel caso della persona giuridica, ogni componente dovrà avere le abilità e le competenze per fornire alla clientela il servizio più efficiente possibile. I ruoli dovranno, ovviamente, essere ripartiti: solo uno dei membri avrà il ruolo di "contatto principale" con il cliente in questione. Nessuno di tali soggetti dovrà versare in una situazione di "conflitto di interessi" e dovranno tutti godere delle protezioni previste dal Regolamento, come l'inammissibilità della risoluzione ingiustificata del contratto di servizi a causa dell'attività come DPO o alternativamente l'inammissibilità della rimozione di un singolo appartenente alla persona giuridica che svolga la funzione di DPO.

Nella normativa non è presente nulla inerente alla durata dell'incarico: tuttavia, in linea con quanto scritto sul GDPR, le Linee Guida evidenziano quanto sia importante la stabilità del contratto stipulato. Nei fatti più questo è lungo (e maggiori sono le tutele previste contro eventuali ingiusti licenziamenti) maggiore sarà la probabilità che il DPO possa adempiere al suo compito in maniera indipendente e valida.

Vanno, chiaramente, evidenziate quali sono le differenze che intercorrono fra un soggetto interno ed uno esterno nel ricoprire la posizione di DPO. Il Garante della Privacy ha puntualizzato che qualora la scelta del Responsabile della Protezione dei dati ricadesse su una figura interna all'impresa sarebbe necessario formalizzare tramite un apposito atto di designazione il dipendente come DPO. Nel caso in cui il soggetto fosse esterno all'impresa la designazione costituirà parte integrante del contratto di servizio. È doveroso che nell'atto in questione, a prescindere dalla forma e dalla natura utilizzata, sia possibile individuare in maniera inequivocabile il titolare del ruolo riportandone anche le generalità, i compiti (eventualmente anche ulteriori a quelli previsti dall'articolo 39) e le funzioni che questo sarà tenuto a svolgere in ausilio al Titolare o al Responsabile del trattamento dei dati. Se al DPO chiesto di svolgere ulteriori compiti rispetto a quelli originariamente previsti dall'atto di designazione sarà necessaria la modifica di quest'ultimo. Il Garante raccomanda, ancora, che nell'atto di designazione dovranno essere presenti i motivi che hanno spinto l'organismo o l'ente a nominare la persona fisica selezionata come DPO al fine di consentire la verifica del rispetto dei requisiti disciplinati dall'articolo 37 (paragrafo 7). Secondo quanto scritto dall'avvocato Comellini: *"La specificazione dei criteri utilizzati nella valutazione compiuta dall'ente nella scelta di tale figura, oltre a essere indice di trasparenza e di buona*

amministrazione, costituisce anche elemento di valutazione del rispetto del principio di "responsabilizzazione" (c.d. "accountability")". (Comellini & Graziano, 2018).

Per quanto riguarda la nomina del DPO è bene specificare per il Garante della Privacy l'unicità di questa figura è una condizione di fondamentale importanza affinché vengano evitate incertezze nonché sovrapposizioni sulle responsabilità. Vi è, invece, l'autorizzazione nell'individuazione di più figure di supporto al Responsabile della protezione dei dati: queste possono essere dislocate con riferimento a settori differenti oppure presso diverse articolazioni organizzative dell'amministrazione. Queste, però, dovranno far riferimento ad un unico soggetto responsabile prescindendo dal fatto che il DPO sia interno oppure esterno. (Comellini & Graziano, 2018)

Per concludere è bene analizzare in maniera dettagliati i requisiti che vengono chiesti ad un individuo affinché esso possa ricoprire il ruolo di DPO.

Seguendo quanto scritto nel paragrafo 5 dell'articolo 37 il DPO è designato *"in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39"*. (Commissione Europea, 2018)

Il livello di conoscenza necessario dovrebbe essere stabilito in base ai trattamenti dei dati effettuati e sulla protezione delle informazioni richiesta dal Titolare o dal Responsabile del trattamento.

Quindi è possibile affermare che la normativa non stabilisce né il tipo di qualità professionali che devono essere prese in considerazione, né il livello di conoscenza specialistica della legge e delle pratiche in materia.

Tuttavia le Linee Guida hanno cercato di fare chiarezza in merito a ciò: come detto in precedenza il livello di conoscenza specialistica deve essere determinato in base ai trattamenti effettuati e sulla protezione dei dati richiesta dal Titolare o dal Responsabile; quindi per i trattamenti che hanno una natura particolarmente complessa verranno richiesti al DPO dei livelli di conoscenza specialistica particolarmente notevoli.

Secondo le Linee Guida rientrano nelle conoscenze e competenze specialistiche:

- Conoscenza da parte del DPO della normativa e delle prassi, sia nazionali che europee, in merito alla protezione dei dati con particolare e approfondita conoscenza del GDPR. Secondo il Garante della Privacy tale conoscenza può essere dimostrata attraverso una documentata esperienza professionale o, alternativamente, grazie alla partecipazione ad attività formative;
- Confidenza con le operazioni di trattamento che sono state svolte;
- Familiarità con le tecnologiche informatiche e con le misure di sicurezza dei dati;

- Capacità di promuovere all'interno dell'azienda del Titolare una cultura della protezione delle informazioni sensibili;
- Conoscenza del settore specifico di attività dell'organizzazione del Titolare del trattamento dei dati;
- Nel caso di un organismo pubblico il DPO dovrebbe possedere un'ottima conoscenza delle norme e delle procedure amministrative applicabili.

Secondo quanto stabilito nel regolamento dall'articolo 38 nel terzo paragrafo vi sono delle garanzie essenziali che permettono al DPO di avere una certa autonomia all'interno dell'organizzazione. Questo è fondamentale affinché tale figura abbia un impatto positivo nell'azienda: occorre assicurare che esso non riceva alcuna istruzione per quanto riguarda l'esecuzione dei suoi principali compiti. Ciò vale a prescindere dalla provenienza del titolare del ruolo, esterna o interna. Il Responsabile della protezione dei dati riferisce direttamente con i vertici gerarchici dell'azienda per cui lavora, in particolar modo con il Titolare o con il Responsabile del trattamento dei dati. Un tale rapporto diretto garantisce che il vertice amministrativo venga a conoscenza quanto prima delle indicazioni e delle raccomandazioni date dal DPO durante l'esercizio delle sue funzioni di informazione e consulenza. Esso inoltre avrà modo di capire in che modo verranno elaborati i dati, se in maniera conforme al GDPR o meno. Il Garante della Privacy raccomanda, qualora la scelta del Responsabile della protezione dei dati ricada su un individuo che è all'interno dell'azienda, che esso sia un dirigente o in alternativa un funzionario di alta professionalità a cui sarà consentito di svolgere le mansioni proprie di questa figura, abbiano queste una rilevanza interna (consulenza, pareri, sorveglianza sul rispetto delle disposizioni) o esterna (cooperazione con l'autorità di controllo e contatto con gli interessati in relazione all'esercizio dei propri diritti), nella maniera più autonoma ed indipendente possibile nonché in collaborazione con il vertice dell'organizzazione. (Comellini & Graziano, 2018)

Secondo quanto scritto sulle Linee Guida è, inoltre, importante che il DPO disponga di alcune qualità personali come l'integrità e l'etica professionale piuttosto che elevati standard deontologici e l'osservanza delle disposizioni del Regolamento. Svolgendo un ruolo di primo piano nella promozione di una cultura improntata sulla protezione dei dati all'interno dell'azienda il Responsabile della protezione dei dati aiuta ad attuare elementi essenziali della normativa: il rispetto dei principi generali e dei diritti degli interessati, i registri delle attività di trattamento, la sicurezza dei trattamenti dei dati e la notificazione di eventuali *data breaches*.

Per ricoprire il ruolo di DPO la nuova normativa europea sulla privacy non richiede alcuna abilitazione, certificazione od iscrizione ad ordini professionali. Il Garante della Privacy ha ribadito che, allo stato attuale delle cose, non vi è alcuna disposizione che preveda una sorta di "albo" per i Responsabili della protezione dei dati in cui vengono attestati i requisiti e le caratteristiche di conoscenza, competenza ed abilità previste dal GDPR; inoltre, non vengono richieste certificazioni riguardanti i requisiti richiesti.

Anzi, è doveroso sottolineare che come altre professioni "non regolamentate" si stanno diffondendo appositi enti che rilasciano delle certificazioni su competenze professionali ai soggetti che, di propria volontà, decidono di partecipare ai corsi da loro organizzati, sostenendo e passando un esame. (Comellini & Graziano, 2018)

Tuttavia il Garante tiene a precisare che: *"Tali certificazioni […] possono rappresentare, al pari di altri titoli, uno strumento per valutare il possesso di un livello minimo di conoscenza della disciplina, tuttavia non equivalgono, di per sé, a una abilitazione allo svolgimento del ruolo di DPO […]"*.[14] (Comellini & Graziano, 2018)

È quindi possibile concludere che la nomina del DPO in una qualsiasi azienda, grande o piccola che sia, è una scelta di fondamentale importanza che non deve essere assolutamente sottovalutata per una serie di motivi che sono stati indicati in precedenza. Questa figura, sebbene sia nuova, ricoprirà un ruolo di primo rilievo nell'immediato futuro delle imprese europee.

4.3 La posizione del DPO.

Nel primo paragrafo dell'articolo 38 si prescrive che il Titolare ed il Responsabile del trattamento dei dati assicurano che il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni inerenti la protezione dei dati personali.

La posizione strategica che tale figura andrà a ricoprire all'interno dell'impresa è di notevole importanza dato che costui (od il team che ricopre tali funzioni) dovrà essere consultato in tutte le questioni inerenti la gestione delle informazioni degli utenti. Si prenda come riferimento quanto affermato nell'articolo 35: per scrivere la "valutazione d'impatto" è necessario secondo il GDPR che il DPO sia coinvolto non solo nella fase iniziale della composizione di tale documento ma è fondamentale che il Titolare lo consulti qualora dovessero sorgere dei dubbi oppure vi sia bisogno di alcuni pareri.

È consigliabile, secondo le Linee Guida, che il Responsabile della protezione dei dati partecipi ai gruppi di lavoro che si occupano delle attività di trattamento delle informazioni.

In sostanza occorre garantire che:

- Il DPO sia invitato a presenziare, su base regolare, a tutte le riunioni del management di alto e medio livello;
- Il DPO sia consultato in maniera tempestiva nel caso in cui si verificasse una violazione dei dati o un qualsiasi altro incidente;

[14] Il testo citato è preso da *"Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico"*.

- I pareri dati da questa figura siano sempre presi in seria considerazione, qualora questo non accada bisognerà motivare le motivazioni che hanno spinto il management a seguire un'altra strada;
- Il DPO sia presente ogni qualvolta debbano essere prese delle decisioni che avranno un seguente impatto sulla protezione dei dati, inoltre chi ricopre questo ruolo dovrà tempestivamente disporre di tutte le informazioni che sono necessarie per poter effettuare un'idonea consulenza.

Seguendo quanto scritto nel paragrafo 2 dell'articolo 38 il Titolare o il Responsabile del trattamento dei dati devono favorire l'accesso alle informazioni al DPO, in modo tale da permettere a quest'ultimo di assolvere nella maniera più corretta possibile i propri compiti[15].

Stando alle Linee Guida (punto 3.2) l'attività di "supporto" che caratterizza il Titolare ed il Responsabile del trattamento si traduce nelle seguenti sette indicazioni:

1. Supporto attivo delle funzioni del DPO da parte del senior management (a livello del CDA, per esempio).
2. Supporto adeguato in termini di risorse finanziare, strutture e personale se richiesto (alcuni esempi possono essere le attrezzature, la strumentazione o la sede).
3. Accesso garantito per il DPO ad altri servizi, come l'ufficio delle risorse umane, l'ufficio giuridico o la sicurezza, così da avere informazioni, supporto e input essenziali.
4. Comunicare in maniera ufficiale e tempestiva a tutto il personale il soggetto che è stato nominato come Responsabile della protezione dei dati, in modo tale da garantire che la sua presenza e le sue funzioni siano note all'interno dell'organismo.
5. Deve essere garantito un aggiornamento continuo a chi ricopre una tale mansione. Nei fatti il DPO deve essere a conoscenza di tutti gli sviluppi inerenti i sistemi di protezione dei dati. Ciò, inoltre, consente un continuo incremento delle competenze del Responsabile alla protezione dei dati, i quali sono, quindi, incoraggiati a partecipare a vari corsi di formazione, forum in materia, workshop, *etc*.
6. È necessario che sia dato il tempo sufficiente alla realizzazione dei compiti affidati al DPO. Infatti, qualora venisse designato un DPO interno con un contratto part-time o, ancora, un DPO esterno che però ha il dovere di svolgere

[15] Articolo 39, paragrafo 2: *"Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica".*

anche altre mansioni non è impensabile che essi non abbiano il tempo materiale per svolgere al meglio il proprio ruolo da Responsabile della protezione dei dati e che quindi trascurino questa loro attività. È fondamentale disporre del tempo sufficiente da dedicare alla funzione di DPO. Sarebbe una buona prassi stabilire la percentuale di lavoro destinata all'attività di Responsabile alla protezione dei dati qualora il soggetto svolgesse anche altre funzioni. In alternativa un'altra buona prassi consisterebbe nello stabilire il tempo necessario per adempiere alle relative incombenze, definire il livello di priorità di quest'ultime e far redigere al DPO stesso un piano di lavoro da lui ritenuto adeguato.

7. Qualora l'azienda che necessita di un DPO risulti di grandi dimensioni potrebbe apparire opportuno costituire un ufficio o un gruppo lavoro DPO, in cui vi è un personale adibito ad aiutare il DPO nello svolgimento delle sue funzioni. In casi di questo genere è meglio stabilire con estrema chiarezza e precisione la struttura interna del gruppo nonché i compiti appartenenti ad ogni componente di esso. Inoltre, come già accennato in precedenza, non è da escludere che la funzione di DPO sia svolta da un soggetto esterno all'impresa. In questa circostanza il gruppo di lavoro sarà costituito da soggetti che sono, ovviamente, esterni all'impresa tutti guidati da un responsabile, il quale avrà anche il ruolo di fungere da contatto con il cliente.

Partendo proprio da quest'ultimo punto le Linee Guida consigliano una particolare attenzione nella scelta riguardante l'affidamento del ruolo di Responsabile della protezione dei dati ad una singola persona o, in alternativa, ad un ufficio. Quanto riportato da queste afferma, in linea di principio, che più aumentano la complessità e la sensibilità del trattamento delle informazioni più risorse dovranno essere a disposizione del DPO. La "protezione dei dati" deve essere svolta con efficienza ed i mezzi messi a disposizione del DPO devono essere proporzionali al trattamento svolto: proprio per tale motivo, dopo un'attenta analisi, un'azienda potrà valutare l'opportunità o la necessità di istituire un apposito ufficio verso il quale destinare le risorse necessarie al corretto svolgimento dei compiti stabiliti. (Comellini & Graziano, 2018)

Inoltre: l'articolo 38 nel terzo paragrafo[16] stabilisce che il DPO debba essere in grado di operare con un sufficiente grado di autonomia all'interno dell'azienda e vengono, inoltre, fissate alcune garanzie. Una di queste riguarda, sicuramente, il fatto che né il Titolare né tanto meno il Responsabile del trattamento dei dati possano esercitare delle

[16] Articolo 38, paragrafo 3: *"Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento".*

pressioni sul DPO dando lui delle "indicazioni" su come effettuare il proprio lavoro. Ciò significa non solo non ricevere istruzioni sull'approccio da seguire nei casi specifici ma nemmeno ricevere istruzioni su come interpretare gli articoli facenti parte del GDPR. Ovviamente il concetto di "autonomia" non significa che il DPO abbia poteri decisionali che si estendono oltre i compiti stabiliti dall'articolo 39.

A questo punto è lecito chiedersi chi sia il responsabile del rispetto della normativa sulla protezione dei dati. Bene: il DPO non è personalmente responsabile in caso di inosservanza degli obblighi inerenti la protezione dei dati elencati nel GDPR. Spetterà, infatti, al Titolare od al Responsabile del trattamento delle informazioni garantire ed essere in grado di dimostrare di essere conforme alla nuova normativa europea. Dunque ricade su questi ultimi due soggetti la piena responsabilità per l'osservanza ed il rispetto delle norme sulla protezione dei dati. Nell'articolo 38, al paragrafo 3, è scritto: *"[...] Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento"* (Commissione Europea, 2018). Sarà quindi lecito per il DPO manifestare tutto il suo dissenso ai più alti livelli del management: qualora questi non reputino opportuno seguire gli avvertimenti di tale figura dovranno essere pronti ad andare in contro a eventuali sanzioni per mancanza di conformità con il GDPR.

Inoltre, sempre con l'intento di potenziarne l'autonomia e l'indipendenza, sempre l'articolo 38 nel terzo paragrafo impedisce al Titolare o al Responsabile del trattamento dei dati di rimuovere o penalizzare il DPO per l'adempimento ai propri compiti. Nel punto 3.4 delle Linee Guida viene esemplificato il caso in cui un DPO venga rimosso dal suo ruolo dopo aver suggerito una "valutazione d'impatto" dovuta ad un elevato rischio del trattamento di determinate informazioni. Tale rimozione risulterebbe inammissibile così come altre penalizzazioni indirette (mancate promozioni, blocco nello sviluppo della carriera e mancate concessioni di incentivi rispetto ad altri dipendenti). (Comellini & Graziano, 2018)

Per concludere è necessario analizzare gli eventuali conflitti di interessi che possono, eventualmente, investire il DPO.

Seguendo quanto scritto nel paragrafo 6 dell'articolo 38 il DPO può, all'interno di un'impresa, svolgere altre funzioni e compiti ma è necessario che il Titolare od il Responsabile del trattamento dei dati si assicurino che tale mansioni non portino ad conflitto d'interesse. Pertanto il DPO non può ricoprire in un'azienda un ruolo che comporta la finalità o modalità del trattamento delle informazioni personali.

Secondo quanto scritto nelle Linee Guida (punto 3.5) può nascere un conflitto di interessi anche quando ad un DPO, in questa situazione esterno (che di norma difficilmente dovrebbe essere soggetto a questo conflitto), venga richiesto di rappresentare il Titolare od il Responsabile del trattamento in un giudizio che tocchi problematiche di protezione dei dati. (Comellini & Graziano, 2018)

Tuttavia le Linee Guida indicano alcune buone prassi da seguire per evitare tali inconvenienti:

- Debbono essere individuate qualifiche, funzioni e ruoli che possano risultare incompatibili con quanto richiede la figura del DPO.
- Dovranno essere redatte regolo interne in modo tale da prevenire eventuali conflitti di interesse.
- Prevedere un'illustrazione più articolata dei casi di conflitti di interessi;
- Sarà opportuno dichiarare che il DPO non versi in nessuna situazione di conflitto di interessi con riguardo ai compiti caratteristici di tale figura, al fine di sensibilizzare rispetto al requisito in questione;
- È consigliabile prevedere specifiche misure di garanzia nelle regole interne e fare in modo che segnalare la disponibilità di una posizione lavorativa, come quella del DPO, o nel redigere contratti di servizi (per DPO esterni) siano utilizzare formulazioni chiare, precise e dettagliate che permettano di prevenire questi conflitti di interessi.

Più e più volte nelle Linee Guida viene ricordato che i conflitti d'interessi sono molteplici e non si limitano ad i pochi casi presi a riferimento in precedenza: un tale contrasto può assumere svariate configurazioni a seconda della provenienza del DPO, sia questo interno od esterno. (Comellini & Graziano, 2018)

Concludendo: il DPO è una figura che, come detto alla fine del precedente paragrafo, assumerà un'importanza sempre maggiore con il passare del tempo in aziende di ogni dimensione. Tale ruolo avrà un peso non indifferente sia da un punto di vista strategico, nei fatti non è difficile pensare che il modo in cui i dati degli utenti saranno studiati siano influenzati dal Responsabile della protezione dei dati, sia da un punto di vista inerente la sorveglianza, dato che il DPO nonostante i suoi lavori all'interno di una qualsiasi impresa avrà anche il compito di interagire con l'autorità di controllo.

CONCLUSIONI.

Giunti alla fine di questo elaborato è doveroso trarre qualche conclusione.

L'intento di questo scritto era quello, innanzitutto, di mostrare come l'introduzione del digitale abbia cambiato il modo di fare impresa. Alle aziende moderne viene chiesta: una enorme flessibilità, un maggior contatto con i clienti (che a volte può risultare anche negativo), una maggiore velocità e di improntare il loro operato fondamentalmente sull'analisi dei dati.

Nei fatti questi si sono tramutati in quello che da molti viene definito l' "oro moderno": se per un servizio, come l'iscrizione ad un social, un individuo non è disposto a pagare, le aziende allora chiederanno i suoi dati e guadagneranno tramite essi. Nelle grandi compagnie ormai servono sempre di più figure che analizzino (e non solo) queste enormi masse di informazioni. Tuttavia il "domani" per i Big Data è rappresentato dal *machine learning*: questo consentirà di analizzare i dati, proprio come un uomo, ad un computer ma in maniera più veloce e maggiore da un punto di vista quantitativo.

Ovviamente per le grandi companies l'analisi dei dati, nonché la digitalizzazione, non rappresenta più il futuro ma il presente. Le imprese che oggi hanno il compito di evolversi in continuazione per essere al passo con i tempi sono le PMI: tuttavia la situazione in Italia non è delle più semplici. Ciò non è positivo se si considera che circa il 99% delle aziende sul nostro suolo sono piccole o medie. Solo il 35% delle piccole e medie imprese del Bel Paese sono in cammino verso la digitalizzazione; un terzo delle aziende in Italia resterà fermo fino al 2021 (circa) per quanto riguarda l'uso dei dati nell'analisi del business.

È impossibile, giunti a questo punto, non affermare che l'Italia necessiti in questo momento non tanto di un cambiamento, già solo la parola ha un significato eccessivamente radicale, quanto più di un movimento. Un movimento verso un Paese più connesso; un movimento verso dei sostegni per chi cerca di promuovere business digitali, adattando la sua azienda alle trasformazioni che stanno avvenendo negli ultimi anni, o chi cerca di creare un business da zero, come le numerose *Startup*. Tutto ciò vorrebbe significare fare dei passi in avanti, muoversi per l'appunto, verso un paese più competitivo.

Questo è evidente, altrimenti non sarebbe stata costituita un'Agenda Digitale sia dall'Unione Europea che dallo Stato italiano. In effetti la maggiore competitività è da sempre stata l'obiettivo dell'Agenda "Europa 2020", di cui queste iniziative a favore del digitale fanno parte; inutile affermare che questa finalità è ben lontana dall'essere raggiunta.

In molti nel corso degli anni si sono chiesti il perché di una tale difficoltà. La risposta che ha soddisfatto i più è la seguente: le persone ancora non si fidano di internet, temono che i loro dati siano utilizzati in maniera impropria.

Il caso "Cambridge Analytica" non ha fatto altro che aumentare queste preoccupazioni; tuttavia è necessario sottolineare come è stato più e più volte fatto all'interno dell'elaborato che nella vicenda appena citata non vi è mai stato un "ratto dei dati".

È necessario che le persone siano informate su questi accadimenti ed anche su come verranno trattati i loro dati.

Proprio per questo dal 2016 l'Unione Europea ha iniziato a scrivere un Regolamento preciso inerente la protezione dei dati. Il testo conosciuto come GDPR è entrato in vigore dal 25 Maggio 2018.

L'introduzione di tale norma comporterà effettivamente dei cambiamenti sia nel modo di operare delle aziende che nel modo delle persone di approcciarsi con le nuove tecnologie digitali?

Trovare una risposta univoca e certa in questo momento è impossibile dato che la legge è stata da poco introdotta ed entrerà a funzionare in pieno regime una volta che sarà iniziato il 2019. Fatto sta che il GDPR obbliga le imprese ad operare in maniera differente: l'UE chiede loro una maggiore chiarezza ed una maggiore trasparenza.

Queste richieste possono avere molteplici fini: innanzitutto questo nuovo Regolamento potrebbe, finalmente, aumentare la fiducia che la gente ripone nel digitale permettendo a molti mercati di decollare.

In secondo luogo, ricordando che il GDPR regola anche i sistemi *cloud* (od i SaaS più in generale), è possibile affermare che c'è una sorta di insistenza da parte dell'Europa affinché le aziende spostino i loro dati in alcuni dei sistemi citati poco più sopra. Ciò, effettivamente, può rappresentare un cambiamento estremamente positivo sia per le aziende che per i clienti: le prime si troverebbero a sostenere dei costi di immagazzinamento e mantenimento dei dati decisamente inferiori dato che affiderebbero le informazioni ad un *cloud* prodotto e gestito da un terzo soggetto, un'impresa specializzata in SaaS, la quale ha delle competenze maggiori nella gestione di questi sistemi; questo soggetto terzo possiederà anche delle risorse che permetterebbero alle informazioni sensibili degli utenti di essere più sicure di quanto non sarebbero nei sistemi di archiviazione di un'impresa.

Quanto questo sia effettivamente realizzabile, però, ancora non ci è dato saperlo. Dei dubbi, nemmeno piccoli, persistono: una compagnia avrebbe veramente il coraggio di affidare una enorme mole di dati ad un'altra azienda che, fondamentalmente, avrebbe solo il compito di custodirglieli? La risposta può sembrare scontata ma, dal punto di vista del sottoscritto, non lo è affatto. Sebbene prima ci sia scritto che l'UE insista

affinché ciò accada questo non significa che la stessa obblighi le aziende a far ciò. Se un'imprese si presentasse conforme a quanto scritto nel regolamento, in tutto e per tutto, e con un sistema di archiviazione delle informazioni differente dal *cloud* (ma pur sempre conforme al GDPR) l'Unione non potrebbe, giustamente, far nulla.

Il lato certamente negativo delle intenzioni dell'UE, anche se "catastrofico" è il termine che potrebbe adattarsi meglio a ciò, potrebbe emergere qualora una delle imprese che gestisce i *cloud* subisse un *data breach*: a quel punto sarebbero messi a repentaglio di dati di molteplici imprese.

Due delle innovazioni proposte dal nuovo Regolamento sulla protezione dei dati riguardano il diritto all'oblio ed il diritto alla portabilità dei dati: il primo, che permette ad un utente di richiedere la cancellazione di tutti i suoi dati ad un'impresa, alimenterà sicuramente la fiducia degli utenti che potranno quindi richiedere l'eliminazione delle proprie informazioni qualora lo ritenessero opportuno; il secondo agevola in particolar modo le imprese nei rapporti B2B (business-to-business), poiché sarà possibile richiedere da parte dell'utente (che può essere un'impresa ma anche una persona fisica) che i suoi dati siano passati ad un altro soggetto Titolare del trattamento. In quest'ultimo caso saranno agevolate, come detto, non poche aziende le quali non dovranno più fornire le loro informazioni ma le faranno passare direttamente da Titolare a Titolare. Ovvio, non si tratta di un cambiamento epocale ma di una semplificazione la quale, da molti, era ritenuta necessaria. L'introduzione di questi diritti evidenzia, dal mio punto di vista, come sia un obiettivo dell'Europa puntare sul digitale dato che fino a pochi mesi fa i diritti appartenenti al vecchio codice della privacy erano tutti di origine giurisprudenziale, fondamentalmente, mentre ora sono stati introdotti dei diritti *"ad-hoc"* che meglio si adattano al nostro contesto storico, dominato dal digitale.

Infine è necessario chiudere evidenziando quanto sarà importante la figura del DPO per le imprese nell'immediato futuro e nel lungo periodo.

Tale posizione, introdotta con il GDPR, avrà un ruolo importantissimo sia in sede di scelte strategiche sia da un punto di vista prettamente ispettivo dato che colui che ricoprirà questo compito sarà il punto di contatto tra l'azienda che tratterà i dati e l'Autorità di controllo.

Fondamentalmente, secondo la mia visione delle cose, almeno nel breve periodo sarà complicato per molte imprese stabilire chi dovrà ricoprire tale ufficio. Molte aziende faticheranno a capire se affidare una tale posizione ad un soggetto interno all'impresa oppure ad un soggetto esterno a quest'ultima. La decisione della persona fisica o giuridica, invece, dovrebbe risultare più semplice dato che questa dovrebbe, in linea teorica, dipendere dalla mole dei dati con la quale l'impresa opera.

Inoltre sarà difficile, per i primi periodi, capire quale posizione effettiva questa personalità dovrà ricoprire e come "inserirlo" nella maniera adatta all'interno del CDA aziendale.

In aggiunta, per concludere, sebbene secondo il sottoscritto il DPO non potrà che essere considerato fondamentale per ogni impresa una volta che il GDPR entrerà in piena funzione, sarà complicato per un'azienda non solo inserire a livello di struttura aziendale questa figura ma, rappresentando un "dipendente" in più, risulterà sgradevole, più che difficile, ad un'azienda sostenere questo (insieme a tanti altri) costo di adattamento alla nuova normativa seppur necessario.

Bibliografia.

- *Colombo C.,"LE AZIENDE TRASFORMABILI: LA SFIDA DELLA DIGITAL TRANSFORMATION ECONOMY", Comunicazione d'azienda nella network society, Corso di Alta Formazione UPA IV edizione, 176-181, 2016.*
- *Colombo F.,"SELF AND SOCIETY IN THE NETWORKED ERA", Comunicazione d'azienda nella network society, Corso di Alta Formazione UPA IV edizione, 10-14, 2016.*
- *Comellini S., "Il Responsabile della Protezione dei Dati (Data Protection Officer-DPO)", Maggioli editore, 22-44, 2018.*
- *Commissione Europea, "General Data Protection Regulation. Gazzetta ufficiale dell'Unione europea", Disponibile su PrivacyItaly.eu: https://www.privacyitalia.eu/wp-content/uploads/2017/10/GDPR_Italiano_PDF.pdf , Bruxelles, 2018.*
- *Commissione Europea, "Le norme si applicano alle PMI?", Disponibile su ec.europa.eu: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-rules-apply-smes_it, 2018.*
- *ConfCommercio, "Le piccole e medie imprese in Italia", Disponibile su Confcommercio.it: https://www.confcommercio.it/-/le-piccole-e-medie-imprese-in-italia , 2009.*
- *Crunchbase, "Cosa è Crunchbase", Disponibile su techcrunch.com: https://techcrunch.com/about/ , 2018.*
- *Di Fraia G., "CREARE VALORE CON IL CONTENT MARKETING: PROCESSI ORGANIZZATIVI E STRUMENTI OPERATIVI", Comunicazione d'azienda nella network society, Corso di Alta Formazione UPA IV edizione, 96-101, 2016.*
- *Forum dell'Economia Digitale "Manifesto FED", Disponibile su splashthat.com: https://splashthat.com/sites/view/fed2018.splashthat.com , 2018.*
- *Genco P. "Il management d'impresa fra old e new economy: nuovi principi o nuove soluzioni?", ECONOMIA E DIRITTO DEL TERZIARIO,781-789, 2002.*
- *Ministero dello Sviluppo Economico, "Piano Nazionale Industria 4.0", Disponibile su sviluppoeconomico.gov: http://www.sviluppoeconomico.gov.it/images/stories/documenti/PIANO-NAZIONALE-INDUSTRIA-40_ITA.pdf , 2017.*
- *Monti L. "Politiche dell'Unione Europea: la programmazione 2014-2020", LUISS University Press, 143-151 , 2016.*
- *Monti, L., Pepe, E., & Rizzuti, G., "E-Government and open data boosting economic growth: a new index", Journal of Business and Economics, 2015.*
- *Rapetto U., "Quella miniera d'oro dei dati personali", Il Sole 24 Ore, 2012.*

- *Rifkin J., "The Age of Access", Penguin Putnam, 2000.*
- *Spampinato G., "La domanda da 20 milioni di euro. I tuoi dati sono al sicuro?", NETAPP CIO READINGS, 2018.*
- *D. Tapscott, A. D. Williams, "How Mass Collaboration Changes Everything", Wikinomics, 9-10, 2006.*
- *Vitali G., "La politica per l'innovazione dell'unione europea", Consiglio Nazionale delle Ricerche, CERIS – Istituto di ricerca sull'Impresa e lo Sviluppo, 3-13, 2010.*

Sitografia.

- *Bacchetti A. & Zanardini M., "Aziende industry 4.0 italiane, ecco quali e come sono", Tratto da AgendaDigitale.eu: https://www.agendadigitale.eu/industry-4-0/aziende-industry-4-0-italiane-quali/ , 2018.*
- *Barberio R., "Facebook e il valore dei dati: la compravendita delle nostre vite", Tratto da The Huffington post: https://www.huffingtonpost.it/presidenteatprivacyitalia-eu/facebook-e-il-valore-dei-dati-la-compravendita-delle-nostre-vite_a_23389642/ , 2018.*
- *Bitteleri V. "GDPR e dati su cloud, le cose da ricordare.", Tratto da 01net.it: https://www.01net.it/gdpr-dati-cloud-cose-ricordare/ , 2018.*
- *D'adda A., "Le quattro caratteristiche chiave di un'azienda digitale", Tratto da IlSole24Ore.it: http://www.ilsole24ore.com/art/management/2017-03-09/le-quattro-caratteristiche-chiave-un-azienda-digitale--121603.shtml?uuid=AEEacpk , 2017.*
- *D'Andrea A. M. ,"Privacy, approvato il decreto di adeguamento al GDPR: periodo transitorio per le imprese.", Tratto da informazionefiscale.it: https://www.informazionefiscale.it/privacy-testo-decreto-adeguamento-gdpr-periodo-transitorio-imprese-ispezioni , 2018.*
- *Dell'Olio L., "Rivoluzione 'digital disruption' cambia il modo di fare impresa", Tratto da Repubblica: http://temi.repubblica.it/economiaefinanza-focus/2016/07/21/rivoluzione-%E2%80%98digital-disruption%E2%80%99-cambia-il-modo-di-fare-impresa/?refresh_ce , 2016.*
- *Della Mura M., "Data Monetization: la sfida sui big data si gioca qui.", Tratto da Big Data 4 Innovation: https://www.bigdata4innovation.it/big-data/data-monetization-la-sfida-sui-big-data-si-gioca/ , 2018.*
- *Fabbri P., "Gli Analytics in Italia: composizione e trend di mercato.", Tratto da ZeroUnoWeb.it: https://www.zerounoweb.it/analytics/gli-analytics-in-italia-composizione-e-trend-di-mercato/ , 2017.*

- *GVC consulenti di direzione associati, "Multinazionali e GDPR: attenzione a gestire il trasferimento dei dati all'estero.", Tratto da GVCassociati.it: http://www.gvcassociati.it/newsletter/documenti/multinazionali-e-gdpr-attenzione-a-gestire-il-trasferimento-dei-dati-all-estero.pdf , 2018.*
- *Italiano A., "GDPR e servizi cloud: gli impatti più rilevanti della nuova normativa.", Tratto da Digital4.biz: https://www.digital4.biz/legal/gdpr/gdpr-e-servizi-cloud-gli-impatti-piu-rilevanti-della-nuova-normativa/ , 2018.*
- *Krogerus M. & Grassegger H., "The Data That Turned the World Upside Down", Tratto da Vice https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win , 2017*
- *Magnani A., "Gdpr al via: denunciate Google e Facebook per «consenso forzato»." Tratto da IlSole24Ore.it: http://www.ilsole24ore.com/art/tecnologie/2018-05-25/gdpr-via-gia-denunciate-google-e-facebook-consenso-forzato-155204.shtml?uuid=AEdzcpuE , 2018.*
- *Mangia V., "Big Data: quanto sono importanti", Tratto da Awhy.it: http://www.awhy.it/awhy-blog/big-data-quanto-sono-importanti/ , 2016.*
- *Menietti E., "Il caso Cambridge Analytica, spiegato bene", Tratto da Il Post: https://www.ilpost.it/2018/03/19/facebook-cambridge-analytica/ , 2018.*
- *Natale R., & Longo A., "GDPR, tutto ciò che c'è da sapere per essere in regola.", Tratto da AgendaDigitale.eu: https://www.agendadigitale.eu/cittadinanza-digitale/gdpr-tutto-cio-che-ce-da-sapere-per-essere-preparati/ , 2018.*
- *Netti E., "Tecnologie digitali: le imprese spingono sugli investimenti", Tratto da IlSole24Ore: http://www.ilsole24ore.com/art/impresa-e-territori/2016-07-01/tecnologie-digitali-imprese-spingono-investimenti-150324.shtml?uuid=ADTmbdm , 2016.*
- *Pepe D., "Digital innovation hub, cosa sono e che ruolo hanno in Industria 4.0", Tratto da AgendaDigitale.eu: https://www.agendadigitale.eu/industry-4-0/innovazione-4-0-italia-competence-center-digital-innovation-hub/ , 2018.*
- *Pizzetti F., "Diritto all'oblio nel Gdpr, ecco tutte le novità." Tratto da AgendaDigitale.eu: https://www.agendadigitale.eu/sicurezza/diritto-alloblio-nel-gdpr-tutte-le-novita/ , 2018.*
- *Pizzetti F., "Portabilità dei dati nel GDPR: cosa significa e cosa implica questo nuovo diritto.", Tratto da AgendaDigitale.eu: https://www.agendadigitale.eu/sicurezza/portabilita-dei-dati-nel-gdpr-cosa-significa-e-cosa-implica-questo-nuovo-diritto/ , 2018.*
- *Redazione QuiFinanza, "Industria 4.0, ecco a che punto è la trasformazione digitale in Italia", Tratto da Quifinanza.it: https://quifinanza.it/pmi/industria-pmi-trasformazione-digitale-in-italia/179974/ , 2018.*
- *Redazione TechEconomy, "Come cambiano le imprese con Machine learning e Analytics", Tratto da TechEconomy.it:*

https://www.techeconomy.it/2018/07/24/cambiano-le-imprese-machine-learning-analytics/ , 2018.

- Redazione ZeroUno, "Come fare Big Data analysis e ottenere valore per le aziende", Tratto da ZeroUnoWeb.it: https://www.zerounoweb.it/analytics/big-data/come-fare-big-data-analysis-e-ottenere-valore-per-le-aziende/ , 2017.
- Rusconi G., "Il business dei dati personali: ecco il nostro prezzo per il marketing", Tratto da Il Sole 24 Ore: http://www.ilsole24ore.com/art/tecnologie/2013-06-13/business-dati-personali-ecco-183457.shtml?uuid=AbUwxl4H , 2013.
- Salerno A., "Banda larga, Facebook: "Decisiva per Pmi, il Governo acceleri"", Tratto da CorriereComunicazioni.it: https://www.corrierecomunicazioni.it/telco/banda-ultralarga/banda-larga-facebook-decisiva-per-pmi-il-governo-acceleri/ , 2017.
- Salerno A., "Pmi italiane sempre più digitali. Ma il 40% "resiste" all'innovazione", Tratto da CorriereComunicazioni.it: https://www.corrierecomunicazioni.it/over-the-top/pmi-italiane-sempre-piu-digitali-ma-il-40-resiste-all-innovazione/ , 2017.
- Schindhelm, "Tabella di confronto tra Codice della Privacy e regolamento europeo per la privacy GDPR." , Tratto da it.schindhelm.com: http://it.schindhelm.com/content/avvocato/italy/news_e_jusful/news/tabella_di_confronto_tra_codice_della_privacy_d_lgs_196_2003_e_regolamento_europeo_della_privacy_gdpr_2016_679_/index_ita.html , 2018.
- Spidalieri F., "Impatto del GDPR sulle piccole e medie imprese: il buono, brutto e il cattivo.", Tratto da AgendaDigitale.eu: https://www.agendadigitale.eu/sicurezza/impatto-del-gdpr-sulle-piccole-e-medie-imprese-il-buono-brutto-e-il-cattivo/ , 2018.
- Steel E., "Companies scramble for consumer data", Tratto da The Financial Times: http://ig-legacy.ft.com/content/f0b6edc0-d342-11e2-b3ff-00144feab7de#axzz5OdQZ4D88 , 2013.
- Troiano G., "Quanti dubbi minacciano la nuova privacy europea.", Tratto da AgendaDigitale.eu: https://www.agendadigitale.eu/sicurezza/quanti-dubbi-minacciano-la-nuova-privacy-europea/ , 2017.
- Vaciago G., "GDPR, quanto costa ad una PMI adeguarsi (e come ottimizzare la spesa).", Tratto da AgendaDigitale.eu: https://www.agendadigitale.eu/infrastrutture/gdpr-quanto-costera-a-una-pmi-adeguarsi-e-come-ottimizzare-la-spesa/ , 2018.
- Zanotti L., "Biga Data: cosa sono e come le aziende fatturano con la Big Data analytics", Tratto da Digital4Biz: https://www.digital4.biz/marketing/big-data-e-analytics/big-data-cosa-sono-e-perche-grazie-alle-analitiche-il-business-continua-a-crescere/ , 2017.

Video.

- *Marco Montemagno, "Facebook e Cambridge Analytica: cosa è davvero successo", Disponibile su YouTube.com: https://www.youtube.com/watch?v=tWPMUSfDbMY , 2018.*