CORSO DI LAUREA TRIENNALE

in

ECONOMIA E MANAGEMENT

INNOVAZIONE E DIGITALIZZAZIONE: VANTAGGI ORGANIZZATIVI E RISCHI PER LE ORGANIZZAZIONI

Laureanda:

Silvia Panico

Matricola: 213111

Relatore:

Ch.mo Prof. Nunzio Casalino

Anno Accademico 2018-2019

INDICE

INTRODUZIONE

Il presente elaborato si propone di analizzare gli effetti della Trasformazione Digitale e l'impatto che questa sta avendo sulle organizzazioni, dimostrando come l'adozione dell'Industria 4.0 permetterà alle imprese di raggiungere un vantaggio competitivo. In particolare si individueranno le pratiche e i modelli organizzativi che distinguono le imprese *digital oriented* dalle altre.

Il primo capitolo fornisce uno sguardo generale, *in primis*, su quella che è stata l'evoluzione del sistema industriale, fino ad arrivare ai giorni nostri, in cui si è affermato il concetto di Industria 4.0. Si è riflettuto su quelli che sono i vantaggi di intraprendere un processo di trasformazione digitale e dei rischi che le organizzazioni possono incontrare.

Il secondo capitolo propone una prospettiva di osservazione interna alle organizzazioni, finalizzata a comprendere i motivi che spingono le imprese a scegliere la digitalizzazione; dopo aver spiegato l'importanza dell'informazione, viene presentato il percorso necessario per intraprendere un processo di trasformazione digitale, i passi da compiere e i soggetti responsabili del cambiamento. Vengono, infine, descritti i nuovi modelli organizzativi come la *Flatter organization*, le *flatarchies* e le *holacracies*, e gli strumenti indispensabili che serviranno per organizzare i dati, ci si soffermerà in particolare sull'importanza dei *Big Data*, che distinguono un'impresa digitalizzata rispetto a quelle tradizionali.

Gli ultimi due capitoli, infine, si concentrano sui rischi digitali che le organizzazioni possono incontrare e sulla loro determinazione, su ciò che riguarda la *cybersecurity* e sull'importanza di proteggere i dati personali. Saranno elencati i principali strumenti attraverso i quali le imprese possono difendersi da attacchi cyber esterni e verrà illustrato il caso di Yahoo, che descrive un esempio rappresentativo di *data breach* che l'azienda ha subito, illustrando infine le misure che sono state adottate.

CAPITOLO 1
LA TRASFORMAZIONE DIGITALE

1.1.L'evoluzione del sistema industriale

Le origini della rivoluzione industriale affondano sia nella rivoluzione politica che nella rivoluzione scientifica e culturale degli ultimi anni del Seicento.

La rivoluzione politica ebbe luogo in Gran Bretagna, nel 1688-89, con le comunità locali che misero in discussione la figura del re, fino ad allora nominato per grazia di Dio, trasformandolo in sovrano voluto dal popolo, per volontà della nazione. In tal modo, la legittimazione del titolo, mutò radicalmente, ponendo le basi per la realizzazione di una monarchia non più di carattere assolutistico.

La rivoluzione scientifica ebbe inizio con Nicolò Copernico, che pubblicò il "*De revolutionibus orbium coelestium*", testo in cui si descrivono i moti celesti e la loro regolarità. Copernico sosteneva che la Terra, come gli altri corpi celesti ruota intorno al sole; ciò contraddiceva quanto si era ritenuto fino a quel momento, cioè che sia la Terra il centro dell'universo. Tale cambiamento rivoluzionario di prospettiva, che consentiva alla scienza di sottrarre alla religione il monopolio sul concetto di verità, venne, poi, definito da Thomas Kuhn: rivoluzione copernicana[1].

Nel 1689, John Locke pubblicava "*A Letter Concerning Toleration*" ed avviava una Rivoluzione culturale, diffondendo la nuova fisica Newtoniana, per la quale, non esisteva più un centro ordinatore, legittimato dall'esterno; essa rappresentava la società come un sistema di forze interagenti, le quali, insieme, con la loro azione comune, sono in grado di determinare il movimento e la trasformazione sociale.

Secondo Locke, in una società liberata dai vincoli feudali può dispiegarsi, appunto, in modo libero, la competizione economica fra gli individui, imparando dall'esperienza e sperimentando nuove soluzioni, quella che Locke definì: *human understanding*.

Le tre rivoluzioni che si realizzarono alla fine del Seicento, quella politica, quella culturale, quella scientifica, rappresentarono la base per sperimentare, innovare, creare nuove tecnologie, che consentissero di realizzare nuove iniziative in campo economico.

[1] La concezione tolemaica, per secoli dominante, sostenuta anche dalle Sacre Scritture, aveva teorizzato, in modo metaforico, l'esistenza di un imperatore, al centro del sistema politico, in un universo finito, in cui vassalli e valvassini giravano intorno.

Le innovazioni tecnologiche, alla fine del Seicento ed agli inizi del Settecento diventarono un mezzo per acquisire potere in un nuovo sistema di relazioni[2], in cui la conoscenza e le competenze rappresentavano un'occasione per riposizionarsi sul piano sociale ed economico. Numerosi furono gli "uomini meccanici" presentati alle corti settecentesche, espressione di un dinamismo del pensiero e dell'applicazione scientifica, di carattere rivoluzionario, capace di esprimere istanze di cambiamento sociale ed economico.

Fino alla metà del secolo XVIII, l'agricoltura era alla base dei sistemi economici dell'Occidente. Essa si caratterizzava per uno scarso livello di produttività, che precludeva alla maggioranza dei contadini di commercializzare i loro prodotti, a causa della difficoltà di produrre eccedenze rispetto al fabbisogno familiare. Soltanto, i grandi proprietari terrieri potevano permettersi di vendere il *surplus* della produzione agricola e ottenere ricavi. I mezzi di produzione agricola erano l'aratro a ruote e gli animali da tiro, che non consentivano un efficiente sfruttamento del terreno. Le campagne erano isolate e distanti dai centri abitati; i sistemi di trasporto erano arretrati, mancavano le infrastrutture e quindi i costi del trasporto delle merci agricole non erano sostenibili per i singoli contadini. A livello demografico, questo contesto produttivo determinava una stagnazione della popolazione, in quanto si realizzava un sostanziale equilibrio tra la capacità produttiva di un territorio e il numero di abitanti. Eventuali fasi di crescita demografica non erano sostenute da una produzione di derrate alimentari sufficiente a sfamare i nuovi nati; di conseguenza, la popolazione che non riusciva ad assicurarsi cibo a sufficienza per sopravvivere andava incontro a malnutrizione, che sovente favoriva la diffusione di epidemie. Queste epidemie provocavano una elevata mortalità della popolazione che, di conseguenza, si riduceva a livelli compatibili con la limitata produzione alimentare.

In questo contesto, la Prima Rivoluzione Industriale[3] segnò una profonda trasformazione non solo in ambito economico e produttivo, ma anche dell'intero sistema sociale. Essa si sviluppò, nel Regno Unito, alla fine del XVIII secolo e si caratterizzò per una radicale trasformazione del sistema economico, che divenne Economia industriale, con l'invenzione della macchina a vapore, da parte di Watt[4]. L'utilizzazione del vapore come forza motrice determinò la produzione di massa nei grandi

[2] P. Bianchi, *4.0 La nuova rivoluzione industriale*, Il Mulino, 2018, pagg. 20-21.

[3] La locuzione Rivoluzione Industriale venne adoperata, per la prima volta, già negli Anni Venti del XIX secolo, utilizzata in analogia con il termine Rivoluzione francese. In precedenza, era stata utilizzata da Friedrich Engels ne "La situazione della classe operaia in Inghilterra" (1845), da Karl Marx, ne "Il Capitale" (1867), da John Stuart Mill nei suoi "Principi" (1848).

[4] Le invenzioni più rilevanti si concentrarono nella seconda metà del Settecento: la giannetta (1764) era un sistema che si basava sull'utilizzazione di una ruota, la quale innescava la mobilitazione di un complesso di fusi; la water frame (1769), che era un filatoio idraulico, la mule Jenny (1779) che era una macchina più articolata, che permetteva di ottenere una qualità dei filati, di livello superiore a quella di tessuti di altri paesi; infine il telaio meccanico a vapore. Lo sviluppo del settore tessile, come rileva il De Simone (E. De Simone, Storia economica. Dalla rivoluzione industriale alla rivoluzione informatica, Franco Angeli, 2014), fu facilitato, dal lavoro a domicilio e dal lavoro intensivo, sfruttando la grande quantità di manodopera ed investimenti economici limitati, a fronte di una domanda interna ed estera assai elevata.

stabilimenti. L'energia offerta dalla macchina a vapore venne utilizzata, innanzitutto, nelle lavorazioni tessili (consentendo di realizzare una più efficiente organizzazione della produzione grazie alla divisione del lavoro e allo spostamento delle lavorazioni all'interno di fabbriche appositamente costruite) nonché nelle miniere e nei trasporti.

La rivoluzione industriale comportò un radicale mutamento della struttura della società, con una trasformazione delle abitudini di vita e dei rapporti fra le classi sociali. Sotto il profilo demografico, l'incremento della produzione agricola e, più in generale, della disponibilità delle risorse naturali, comportò un notevole aumento della popolazione, che si concentrò in grandi sobborghi a ridosso dei principali centri urbani, nei quali si ammassava il sottoproletariato che dalle campagne cercava lavoro nelle fabbriche cittadine.

Tra il 1870 ed il 1970 in Europa e negli Stati Uniti si verificarono dei processi di trasformazione tecnologica, definiti dagli storici: "seconda rivoluzione industriale". L'epoca della seconda rivoluzione industriale fu contraddistinta dall' invenzione del motore a scoppio e dalla sostituzione del petrolio al carbone, come principale fonte di energia.

Queste invenzioni furono in grado di rivoluzionare l'organizzazione dei processi produttivi. L'organizzazione della produzione fu interessata da innovazioni volte a facilitare il flusso della produzione (nastri trasportatori) e ad incrementare la produttività del lavoro (utilizzo di macchine utensili di elevata precisione).

Il più importante processo di riorganizzazione produttiva fu costituito dall'applicazione, in campo industriale, dei principi di Taylor (Taylorismo), che intendevano abbattere i costi del lavoro ed accrescere la produttività, come espresso in *The Principles of scientific Management.*

L'applicazione di tali principi di riorganizzazione del lavoro, in campo industriale, fu posta in essere, nella propria fabbrica, da Henry Ford, a partire dal 1913. L'imprenditore americano divise, in modo razionale, il lavoro dei suoi operai, i quali, pur restando nella propria postazione, potevano eseguire il proprio intervento, sulla catena di montaggio, realizzando, in modo efficiente, l'assemblaggio delle varie componenti dell'automobile. Tale divisione del lavoro determinò un abbattimento dei costi unitari di produzione, conseguendo un aumento della produttività dei lavoratori al fine di implementare le economie di scala. Sfruttando i benefici in termini di costi offerti dalla catena di montaggio, si riuscì a produrre un modello di automobile (la Ford T) che, grazie al suo prezzo relativamente contenuto, vide una notevole diffusione.

Fra la metà dell'Ottocento e la metà del Novecento si realizzò uno sviluppo più intenso delle epoche precedenti. La crescita demografica costituì un fattore determinante. Il miglioramento delle condizioni igienico sanitarie e le scoperte della medicina consentirono un aumento della natalità ed un abbassamento del tasso di mortalità, nonché, un aumento della vita media.

La seconda rivoluzione industriale si può considerare l'epoca della produzione standardizzata, caratterizzata da un'estensione del mercato e dai consumi di massa. In tale mercato, si possono individuare due tipi di attori: i produttori, che sono in posizione dominante ed i consumatori, che subiscono le scelte dei produttori.

I trasporti subiscono grandi trasformazioni, con un importante ampliamento della rete stradale e l'invenzione dell'automobile. La rete ferroviaria viene caratterizzata da una rilevante espansione, soprattutto, a fini commerciali. Sul piano dei mezzi navali, si ammodernano le flotte commerciali; a partire dagli Anni Venti, si avviano i primi esperimenti, sul piano dell'aviazione commerciale.

Nel 1840 viene inventato il telegrafo; nel 1871 nasce il telefono e nel 1896, la radio. Queste invenzioni determinano delle innovazioni nel campo dei trasporti e delle comunicazioni, producendo dei benefici nelle attività economiche, come il commercio, con riguardo alla riduzione dei costi e dei tempi di movimentazione delle merci.

Vengono create nuove istituzioni finanziarie come le banche cooperative, le casse di risparmio, che facilitano la raccolta e l'impiego dei fondi, consentendo la diffusione dei servizi e crediti bancari ai piccoli artigiani, contadini ed imprenditori.

Tra la fine della seconda Guerra Mondiale e la fine del XX secolo, si avviano dei cambiamenti profondi nei sistemi economici e nello stile di vita dei popoli. A questo periodo, ci si riferisce, comunemente, con la definizione di Terza Rivoluzione Industriale[5].

La Terza Rivoluzione Industriale è caratterizzata da un processo di evoluzione tecnologica che incide, in modo particolare, sull'elettronica e sull'informatica, con la nascita del computer, che modifica radicalmente, lo stile di vita delle popolazioni. Gli effetti di queste trasformazioni hanno, anche, un impatto sulle preferenze dei consumatori, i quali cominciano a premiare la qualità del prodotto, a fronte della standardizzazione dello stesso.

In conseguenza di ciò, le grandi imprese devono sostituire la rigidità della produzione standardizzata di massa, con sistemi di produzione flessibili ed automatizzati, capaci di adattare i volumi e le caratteristiche delle modalità produttive, alla mutevolezza della domanda, consentendo alle imprese stesse di abbattere i costi e di conseguire economie di scala, non sui volumi, bensì nella raccolta, elaborazione e trasmissione dei dati.

[5] Cfr.: J. Rifkin, *La terza rivoluzione industriale*, Mondadori, 2011; R. Ippolito, *La terza rivoluzione industriale*, Pacini Editore, 2016; A. Günther, *Sulla distruzione della vita nell'epoca della terza rivoluzione industriale*, in Id. (a cura di), *L'uomo è antiquato*, Torino, Bollati Boringhieri, 2007; G. Di Taranto, *Dalle infrastrutture materiali di comunicazione alle reti immateriali di connessione*, in C.B. Lopez et al. (a cura di), *Vie e mezzi di comunicazione in Italia e Spagna in età contemporanea*, Rubbettino, 2013.

La trasformazione profonda dei metodi di produzione e del mercato determina la fine del modello fordista e l'affermazione del modello giapponese di *lean production*, basato sui principi di qualità totale, flusso di informazioni *bottom-up* e *just in time*.
L'industria chimica diventa protagonista con la produzione delle fibre sintetiche e della plastica, che trovano numerose applicazioni. La diffusione della corrente elettrica favorisce lo sviluppo del settore petrolifero. L'industria metallurgica si sviluppa, in modo importante.
A seguito di tale rivoluzione industriale, si configura un'Economia post-industriale, con una ampia gamma di servizi, nella quale, si realizza un cambiamento della condizione dei consumatori (che diventano dominanti), rispetto a quella dei produttori (che diventano dominati), all'inverso del periodo precedente.
In tal modo, si affaccia sul mercato la scelta del consumatore, che diviene la priorità. Prima di ogni cosa, si afferma l'esigenza del consumatore, che rappresenta l'*input* per le scelte dei produttori, i quali devono seguire i gusti, le preferenze dei consumatori, che dominano il mercato.
Il differente uso delle tecnologie permette, a taluni competitori, di emergere rispetto ad altri e determina un riposizionamento degli individui nella scala sociale della società, trasformando, quindi, i rapporti di forza interni alla società stessa[6].
Il riferimento alle grandi trasformazioni tecnologiche viene enfatizzato con il termine dirompente, di rivoluzione. La rivoluzione tecnologica, applicata all'industria, ha prodotto cambiamenti di rilievo nelle dinamiche sociali. Infatti, l'industria ha rappresentato il luogo essenziale del mutamento sociale, poiché nell'ambito della produzione si sono determinate le applicazioni delle innovazioni tecnologiche.

1.2. L'industria 4.0

Le riflessioni esposte nel paragrafo precedente consentono di comprendere come le rivoluzioni industriali che hanno caratterizzato la fine del XIX e l'intero XX secolo, abbiano permesso, attraverso innovazioni "distruttive", che la produzione non sia più condizionata dalla limitata forza fisica dell'uomo e degli animali; ciò grazie all'utilizzo di "macchine intelligenti" che hanno reso possibile la produzione di massa.
I radicali cambiamenti nello stile di vita quotidiano e nei paradigmi di sviluppo economico che si sono realizzati a partire dal nuovo millennio sono conseguenza dei processi di evoluzione tecnologica; tali processi hanno contribuito a determinare la realizzazione della cosiddetta "Industria 4.0", o "Manifattura 4.0", o "Fabbrica 4.0", espressioni terminologiche di un unico fenomeno globale, che,

[6] P. Bianchi, op cit., pag. 27.

nei singoli paesi, assume una connotazione peculiare e differente, rappresentando, sostanzialmente, una vera e propria Quarta Rivoluzione Industriale. In realtà, tale terminologia più che possedere una valenza scientifica è riconducibile alle definizioni delle politiche dei governi nazionali e delle istituzioni internazionali, ispirandosi ai processi di automatizzazione e di interconnessione della produzione industriale.

La locuzione "Industria 4.0"[7] indica l'inserimento nei processi manifatturieri, sinora svolti dagli esseri umani, di macchine intelligenti e connesse a Internet. La manifattura rimane centrale nella produzione industriale, ma non va più considerata come una sequenza di fasi separate, bensì come un flusso integrato, sul piano immateriale, grazie alle tecnologie digitali.

Il termine "Industria 4.0" venne usato, per la prima volta, nel 2011 dalla Accademia Tedesca di Scienze e Ingegneria (Acatech20), per una specifica iniziativa adottata dal Governo Tedesco a novembre 2011 all'interno del più ampio "High-Tech Strategy 2020 Action Plan"21."*Quarta rivoluzione industriale*", o anche "*Fabbrica 4.0*" o "*Industria 4.0*" è una definizione che nasce, quindi, in Germania e prende il nome da una iniziativa promossa da Centri di Ricerca e Imprese finalizzata ad aumentare la competitività delle industrie manifatturiere tramite l'integrazione nei processi produttivi di "*cyber-physical systems*" (CPS). CPS è, cioè, l'acronimo con cui viene indicata l'integrazione fra sistemi "*fisici*" (*physical*) e le "*macchine intelligenti*" (*cyber*), che comunicano fra loro tramite la rete Internet. Con tale definizione terminologica, in sostanza, si indica l'integrazione tecnica del *cyber-physical system* (CPS) nella produzione e nella logistica, così come l'applicazione di Internet delle Cose (IOT) e dei Servizi nei processi industriali – incluse le conseguenze che ne derivano per la creazione di valore, i modelli di business e a valle, per la fornitura dei servizi e l'organizzazione del lavoro (H. Kagermann, 2013).

Industria 4.0 risulta essere un approccio nuovo ed efficiente rispetto alla produzione di beni e servizi, attraverso il quale, si produce di più e con minor numero di errori, potendosi modificare schemi di produzione, a seconda degli *input* esterni. Si tratta di una rivoluzione che ha inciso, in modo sostanziale, sull'economia, modificando non soltanto le modalità produttive dell'attività manifatturiera, ma riconvertendo l'intero tessuto economico, in tutti i suoi settori. Pertanto, definire tale fenomeno una mera rivoluzione industriale, appare riduttivo, poiché le conseguenze interessano non solo il sistema economico, ma anche tutti gli ambiti della società.

In questo sistema di comunicazione e produzione interconnesso, la dimensione spaziale diviene pressoché irrilevante e l'accesso alla informazione diventa unico e al contempo, diffuso. L'elemento

[7] Su questo tema, cfr. K. Schwab, *La quarta rivoluzione industriale*, FrancoAngeli, 2016; A.Gilchrist, *Industry 4.0: The Industrial Internet of Things*, Apress, 2016; G. Cristoforetti - G. Lodi, *Human Revolution: Quarta rivoluzione industriale e innovazione sociale*, Imprimatur editore, 2017.

ordinatore della nuova industria è rappresentato dall'interconnessione dell'individuo, dell'impresa, di ogni singolo soggetto, con le reti di relazione, di carattere planetario. Si tratta di un sistema industriale in connessione ed interazione globale, che rende ciascun soggetto, allo stesso tempo, attore delle sue azioni e dipendente dalle interazioni altrui[8].

Questa integrazione si realizza attraverso "un sistema nervoso", composto, fra l'altro, di sensori installati sulle macchine, i quali permettono la connessione in rete continua delle stesse, realizzando la possibilità di una produzione auto-controllata sulla base di opportuni input provenienti dal sistema medesimo e dal mondo esterno. Le innovazioni che sono alla base della manifattura 4.0 derivano da una integrazione, sempre maggiore, nella produzione industriale, di nuove logiche e servizi, sfruttando varie tecnologie, tra cui: macchine e tecniche innovative come la stampa 3D e 4D, *big-data* e *Open System*, *Internet of Things* (IoT - Internet delle cose), *Cloud Manufacturing CBS* (*Computer Business System*), utilizzo di "*robot*" e "*cobot*" (*collaborative robot*), *Wearable Devices*. Queste sono alcune delle cosiddette "*tecnologie abilitanti*", che rendono possibile una digitalizzazione ed una interconnessione globale dei processi industriali, determinando una maggiore produttività e competitività del sistema economico, incidendo, anche, sui servizi e non soltanto, sulla manifattura. Non è stata ancora individuata, o forse, non esiste, "*l'innovazione simbolo*" della Quarta rivoluzione industriale, ma di certo, la sua caratterizzazione, universalmente, riconosciuta, è la "*interconnessione*".

La nuova manifattura digitale rappresenta, oggi, una delle realtà a più alto potenziale di sviluppo, con dinamiche di crescita esponenziale. La nuova "*digital manufacturing*", derivante dall'applicazione delle tecnologie abilitanti di industria 4.0, nasce e si forma in un sistema produttivo industriale, ma da quest'ultimo, ne prende profondamente, le distanze, in termini di: attori, processi e luoghi produttivi, tipologia di prodotto, che si ottiene alla fine del processo e chi ne diventa il consumatore e destinatario.

La *digital manufacturing*, è entrata in scena dopo il primo decennio degli anni duemila, rappresentando, oggi, il quarto paradigma produttivo dei nostri giorni. Esso esprime il rinnovamento del sistema della manifattura attraverso l'uso delle tecnologie digitali, che sono utilizzate in modo integrato per l'innovazione di prodotto, la sperimentazione, la prototipizzazione e la produzione di beni; consentono, inoltre, l'ottimizzazione dei processi di fabbricazione, innovazione, commercializzazione e distribuzione in un ambiente agile, flessibile, integrato ed interconnesso.

Ridurre questo grande cambiamento, semplicemente, ad un mero processo di robotizzazione spinta, rappresenta una semplificazione fuorviante. Infatti, l'applicazione delle tecnologie abilitanti e gli annessi effetti sui processi industriali, determineranno profondi mutamenti nei vecchi modelli di

[8] P. Bianchi, 4.0, op. cit., pag. 57.

business, favorendo la nascita di nuovi modelli, nei quali, la competitività delle aziende non sarà più basata sui costi, ma sulla capacità di innovare, di personalizzare i prodotti e la qualità.

Si va verso un concetto di "*on-demand manufacturing*", dove a prodotti e servizi personalizzati, corrisponde un rafforzamento del ruolo del consumatore, che non si limita più ad essere un semplice consumatore attivo, ma sarà considerato un *prosumer,* ovvero un consumatore più che attivo, quasi dominante, nel processo che coinvolge le fasi di creazione, produzione, distribuzione e consumo del prodotto.

Dal punto di vista del luogo della produzione, invece, si stanno diffondendo processi di *reshoring*, in quanto le fabbriche digitali e automatizzate non hanno più bisogno di delocalizzare in paesi con un costo del lavoro minore, riuscendo a raggiungere in loco sia economie interne che esterne conseguendo determinanti vantaggi di costo. Le imprese europee potranno, di conseguenza, ritrasferire in Europa gli stabilimenti e localizzare molte operazioni manifatturiere più vicino al consumatore.

Le strategie di sviluppo dell'Industria 4.0 si susseguono: in Germania: *Industrie 4.0*; in Francia: *Industrie du Futur*; in Spagna: l'*Industria connectada*; in Gran Bretagna: *High Value Factoring*; in Italia: la *Fabbrica Intelligente*; in Svezia: *Production 2030*;. In realtà, appare evidente, come il livello dimensionale europeo, sia la scala minima per poter affrontare il cambiamento strutturale in atto, su base globale[9].

D'altra parte, i programmi di sviluppo, di livello nazionale, senza una regia sovraordinata, rappresentano uno strumento debole e non competitivo, non capace di risolvere le problematiche economiche mondiali. Nel lungo periodo, si verifica un effetto compensativo[10], con la sostituzione dei lavoratori "generici" usciti dal ciclo produttivo, a seguito dell'incidenza dei processi di automazione, con l'inserimento di nuovi occupati, che sono formati in funzione di questi nuovi processi.

1.3. Opportunità e rischi della trasformazione digitale

Numerose sono le opportunità che vengono a determinarsi, in tutti i campi, a seguito di questi processi evolutivi. La rivoluzione digitale sta realizzando mutamenti importanti, nell'ambito della comunicazione e della mobilità, poiché determina l'interazione dell'ambito fisico, con quello biologico e con quello digitale, causando la caduta delle barriere spazio-temporali e favorendo la

[9] P. Bianchi, 4.0, op. cit., pag. 95.
[10] Ivi, pag. 96.

circolazione degli individui. I progressi conseguiti in uno dei predetti ambiti hanno conseguenze, anche, negli altri[11].

Nell'ambito della sfera fisica, i *megatrend* tecnologici, con le loro quattro applicazioni pratiche sono: veicoli autonomi, stampa 3D, robotica avanzata e nuovi materiali[12].

L'interazione fra il modo fisico degli esseri umani e quello digitale produce un sistema *cyber* fisico, che si compone di una rete complessa di macchine, oggetti virtuali, strutture di calcolo, *device* di comunicazione.

Una indagine di Federmeccanica del 2016 individua, in modo non esaustivo, un pacchetto di tecnologie abilitanti: meccatronica, robotica, robotica collaborativa, *IoT*, *Big Data*, *Cloud Computing*, Sicurezza Informatica, Stampa 3D, Simulazione, Nanotecnologie, Materiali Intelligenti[13].

In particolare, alcune di queste tecnologie, poiché generano e trattano dati sensibili, saranno oggetto - di seguito - di un approfondimento *ad hoc*: *Internet of Things*, *Big Data* e *Cloud computing*.

Definire, precisamente, il significato del termine *Internet of Things*, non è semplice, poiché, con tale locuzione, ci si riferisce alle connessioni realizzabili con una ampia offerta di componenti *software* ed *hardware* commercializzate da varie aziende del settore tecnologico. Comunemente, con la locuzione "*Internet of Things*", si indica l'interconnessione di oggetti fisici tramite Internet.

La rete Internet è nata per mettere in comunicazione gli esseri umani, attraverso dei computer, capaci di trasformare il testo in segnali elettrici, trasferendolo su rete elettrica e trasmettendolo su rete telefonica. Con il progredire della tecnologia e il miglioramento dei *software*, si è giunti alla capacità delle macchine di potersi connettere, autonomamente e dialogare fra loro, grazie ad algoritmi sempre più complessi ed intelligenti. Ad esempio, oggi, uno *smartphone* è capace di verificare l'accesso del padrone di casa ed attivare, automaticamente, l'accensione delle luci o di altri meccanismi domestici. Sul mercato, le imprese competono sulla base della differenziazione della qualità delle loro tecnologie, che si adattano, di più o di meno, alle esigenze dei consumatori[14].

In tale prospettiva, un importante settore di sviluppo grazie alla diffusione del fenomeno IoT è rappresentato da un "design orientato ai servizi" e fortemente personalizzato. In sostanza, i consumatori potranno incidere direttamente sulle attività in fabbrica per acquisire oggetti non più selezionati semplicemente da un catalogo, ma scegliendo fra una serie di opzioni che andranno a incidere realmente sui processi di produzione; tale impostazione apre certamente enormi opportunità per i nuovi modelli di *business*.

---

[11] K. Schwab, op cit., Franco Angeli, 2016, pag. 30.
[12] *Ibidem*.
[13] *Industria 4.0*, Indagine di Federmeccanica, pagg. 155-160.
[14] Beltrametti - Intini – Guarnacci - La Forgia, *La Fabbrica Connessa,* Guerini e Associati, pag. 54.

Un altro fattore con rilevanti prospettive di sviluppo è rappresentato dalle applicazioni, *web* e *mobile*, le quali consentono l'acquisizione di informazioni necessarie a prendere decisioni. Tali applicazioni, vengono, oggi, adoperate, anche, da un'utenza "*business oriented*", sebbene, meno tecnologica, oltre che da un target di consumatori con una più spiccata competenza tecnico-informatica.
Altro elemento di innovazione dell'Industria 4.0 sono i c.d. *Big data*.
Prima di definire esattamente di cosa si tratta, è opportuno premettere che qualsiasi oggetto connesso alla rete e qualsiasi servizio (online e non) producono dati. Il flusso di informazioni è tale che, i dati accumulati negli ultimi anni hanno raggiunto ormai l'ordine di *zettabyte*.
Con il termine *Big Data* non ci si riferisce, in realtà, unicamente all'effettiva quantità di dati generati, bensì alla sua analisi. La vera rivoluzione offerta dai *Big Data* deriva proprio dalla capacità di raccogliere, condividere, selezionare, aggregare tutte le informazioni utili per elaborare, analizzare e individuare soluzioni nuove tramite algoritmi capaci di moltiplicare la capacità di analisi delle macchine elettroniche.
In proposito, è stata elaborata una classificazione ed una distinzione della tipologia dei dati, definibile come "analisi delle 4 V". Volume, *Velocity*, *Variety*, *Veracity*:

- il Volume dei dati, in primo luogo, è enorme, perché si genera e si trasferisce, in modo esponenziale, una massa enorme di dati.
- *Variety*. Coesistono fonti e tipi di dati molto differenti fra loro: strutturati, non strutturati, foto, email, video, file pdf, audio, ecc…
- *Velocity*. Risulta determinante la rapidità con la quale si trasferiscono dei dati, anche, in numero rilevante, sui *social network*, ma, soprattutto, per formulare decisioni da parte di imprenditori, manager e ricercatori.
- Veracity. Di fondamentale importanza è la veridicità e l'affidabilità dei dati. Pertanto, sono insite nel concetto di *big data veracity* delle tecniche di pulizia e bilanciamento dei dati.

Il processo di estrazione di 'conoscenza' da banche dati di grandi dimensioni è definito *data mining*. Tale processo sfrutta specifici algoritmi e particolari tecniche come *grid computing*, *in-database processing* e *in-memory analytics* che individuano associazioni e sequenze rendendo le informazioni disponibili e immediatamente utilizzabili nell'ambito del *decision making*.
Un ultimo approfondimento merita il *Cloud computing.* Esso indica l'insieme delle tecnologie che consentono di memorizzare, archiviare ed elaborare dati per mezzo dell'utilizzo di risorse *hardware* e *software* distribuite in rete, fornendo così una risposta alla crescente domanda di risorse informatiche ad elevata potenza di archiviazione e di calcolo.
I fornitori di tecnologia digitale hanno evoluto la loro competizione dalla mera realizzazione del software più innovativo, dal punto di vista tecnologico, alla offerta sul mercato di servizi integrati,

comprensivi dell'infrastruttura fisica, il supporto, la manutenzione ed il modello di business integrato. L'offerta del servizio può essere usufruita sulla base di una modalità temporale o del numero di utilizzatori, i cosiddetti *Cloud Services*. Il concetto del servizio *Cloud* è rivoluzionario, poiché l'oggetto del business si trasforma da strumento legato ad un'opera prestata dietro retribuzione, ad un accesso al servizio pagabile sulla base del consumo, effettivamente, fruito.

Pertanto, diventa necessario, per le aziende, avviare e terminare la loro trasformazione organizzativa e tecnologica interna, attraverso i processi di ammodernamento, determinati da queste innovazioni straordinarie. Per cogliere le nuove opportunità offerte dall'evoluzione tecnologica è necessario che il mondo imprenditoriale divenga protagonista di processi di aggregazione delle imprese, di formazione specialistica manageriale, di investimenti in ricerca e sviluppo. In questo senso, i modelli organizzativi si stanno già evolvendo[15].

Mentre il modello di produzione fordista si caratterizzava per un elevatissimo livello di standardizzazione e necessitava di una organizzazione del lavoro di tipo taylorista, che si basava su una estrema differenziazione delle mansioni dei lavoratori, con limitata autonomia intellettuale e scarso interesse per la componente intellettuale, le innovazioni che si accompagnano a Industria 4.0 richiedono l'utilizzo di nuovi paradigmi organizzativi.

Una ricerca di Eurofound 2017[16] indica come l'impiego di lavoratori con accesso a percorsi di formazione, strumenti di retribuzione variabile e utilizzo della flessibilità nella gestione dei tempi di lavoro determini una crescita dei livelli di innovazione pari al 9%. Inoltre, la presenza di modalità di organizzazione del lavoro basate sulla consultazione dei lavoratori e su strumenti paritetici di miglioramento dei processi può accrescere tali livelli dell'8%.

La "questione organizzativa" dell'Industria 4.0 può essere osservata in una duplice prospettiva:

a. una MICRO, legata alle c.d. HR ovvero alla disponibilità di risorse umane adeguate;
b. una MACRO, legata alla trasformazione delle organizzazioni, a seguito dell'impatto rivoluzionario e pervasivo delle tecnologie dell'Industria 4.0.

Nella prospettiva MICRO, si impongono: una maggiore interdisciplinarietà nella formazione, che consenta ai dipendenti, anche quelli altamente specializzati, di interagire tra loro; maggiori responsabilità gestionali dei lavoratori; mentalità aperta ai cambiamenti, approccio proattivo, e capacità di operare per progetti.

Sotto il profilo MACRO, occorre un'organizzazione *lean* (snella), che si declina con i seguenti corollari: organizzazione per processi (finalizzazione di tutte le attività in una logica globale di

[15] Ivi, pagg.178-180.
[16] Cfr. *Eurofound, Innovative changes* in *European companies: Evidence from the European Company* Survey, Publications Office of the European Union, 2017.

processo); organizzazione per progetti (il miglioramento è realizzato attraverso progetti che si prefiggono obiettivi); organizzazione che apprende (nel senso che si alimenta attraverso la sperimentazione e l'integrazione); organizzazione cellulare e a rete (nel senso che è costituita da Team autonomi, diretti dall'alto solo per l'indicazione delle linee guida e degli obiettivi).

Le riflessioni di cui innanzi fanno comprendere come il vantaggio competitivo derivante dal basso costo della manodopera poco qualificata stia perdendo rilievo. Ciò contribuisce, nei Paesi più avanzati, ad alimentare flussi di *re-shoring*, ovvero il rientro in patria di segmenti di produzione, in precedenza delocalizzati in paesi a basso costo di manodopera. D'altra parte, risultando sempre meno importante la vicinanza fisica tra le aziende nella definizione del ciclo produttivo, i costi della logistica incideranno sempre meno e vi sarà una distribuzione delle unità produttive sul territorio radicalmente diversa[17].

La digitalizzazione del settore manifatturiero sta creando un nuovo paradigma produttivo nel quale la concorrenza nei mercati non riguarda più solamente il prodotto o il processo produttivo ed interessa sempre meno anche il marchio. La competizione, adesso, si gioca su fattori vincenti quali l'artigianalità, il design, la personalizzazione, l'autenticità e la qualità dei servizi. D'altra parte, bisogna, poi, fare i conti con le trasformazioni della figura del consumatore, che apprezza ed acquista il prodotto sulla base della differenziazione e della varietà del prodotto stesso.

Specifiche tecnologie consentono di incrementare la capacità di realizzare produzioni customizzate (*on demand manufacturing*) dove il prodotto può essere persino noleggiato perché il vero valore aggiunto diventa il servizio e la remunerazione si basa sulla prestazione.

Certamente, con le innovazioni tecnologiche, nel manifatturiero, vi sarà l'opportunità di aumentare la produttività, attraverso minori tempi di *set-up*, si potranno ridurre gli errori ed i fermi macchina e al contempo, si potrà aumentare la qualità e si potranno ridurre gli scarti, mediante l'utilizzo di sensori che monitorano la produzione in tempo reale. Questo implicherà maggiore competitività del prodotto e maggior flessibilità per le nostre imprese che, nella nuova manifattura, assai, customizzata, a "misura di cliente", consentirà di coniugare, da una parte, la produzione in piccoli lotti e dall'altra, la rapida capacità di rispondere ai bisogni del consumatore di nicchia, con i vantaggi di costo derivanti dalla produzione su larga scala.

Le innovazioni tecnologiche consentiranno di creare una più stretta integrazione della filiera e di consolidare la catena del valore fra fornitori e subfornitori, fra imprese intermedie e imprese a capo della filiera, fra imprese mature e start-up innovative, in tal modo, permettendo di restituire al sistema produttivo una maggiore razionalità e proporzionalità organizzativa e logistica. Il vantaggio

[17] Beltrametti - Intini – Guarnacci - La Forgia, op. cit., pag. 76.

competitivo, di conseguenza, diventerà, meno legato alla dimensione dell'impresa ed invece, sarà determinato dal suo posizionamento strategico e dalle sue interconnessioni lungo la catena del valore.
Con questi cambiamenti radicali la quarta rivoluzione industriale determinerà la modifica dei ruoli del personale che lavora nelle imprese. Infatti, alle persone sarà richiesto di lavorare come parte di un sistema socio-tecnico integrato, all'interno del quale, si passerà da una lavorazione, prettamente, manuale, all'attività di supervisione, in tempo reale, dei processi produttivi automatizzati.
Quindi, con l'introduzione dell'IoT, nella catena di montaggio non necessiterà più l'attività dell'operaio allo scopo di compiere azioni, puramente, meccaniche, bensì, la finalità dell'azione umana sarà, piuttosto, di svolgere attività di settaggio dei macchinari e di *problem-solving*. Tutto questo, come si può immaginare, avrà importanti conseguenze, in primo luogo, sul piano occupazionale, poiché si creeranno nuove opportunità di lavoro, ma vi sarà incidenza, anche, sulla specializzazione professionale dei lavoratori e diventerà necessario un adeguamento della formazione digitale degli occupati.
Alle acquisizioni evolutive di Industria 4.0 si accompagnano, però, alcuni rischi significativi.
Tra questi, particolare rilevanza assumono: la tutela della *privacy*, il Digital Divide e la sicurezza informatica.
Sotto il primo profilo, si evidenzia che l'interconnessione dei dispositivi e la condivisione delle informazioni rese possibili dagli strumenti di Industria 4.0, con l'enorme mole di dati personali che vengono trattati, conservati e trasmessi, rappresenta un serio pericolo per la *privacy* del cittadino.
In proposito, si evidenzia che il diritto deve continuamente adeguare i propri strumenti per adattarsi alle continue evoluzioni che si realizzano in ambito tecnologico. In particolare, il Regolamento Europeo 679/2016 (GDPR) ha toccato alcuni problemi tipici del mercato IoT, facendo perno sui principi di trasparenza, *privacy by design*, e *privacy by default*.
Il principio di trasparenza stabilisce che le informazioni destinate all'interessato al trattamento siano complete, facilmente accessibili e di facile comprensione. Le imprese devono specificare, con la massima chiarezza, quali siano le conseguenze della raccolta dei dati connessa al prodotto IoT. I dati devono essere adeguati e pertinenti e i trattamenti vanno limitati a quanto necessario per le finalità del trattamento. I dati personali, inoltre, devono essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi.
Altro rischio connesso con Industria 4.0 riguarda la sicurezza informatica.
Il problema sicurezza non si riferisce, banalmente, alla diffusone di virus che possano attaccare i pc aziendali, ma, soprattutto, al pericolo che soggetti ostili possano realizzare attacchi informatici ai sistemi digitali aziendali finalizzati ad assumere il controllo di impianti, rubare informazioni riservate

o provocare danni. I c.d. cyber attacchi possono diventare particolarmente critici proprio per il fatto che i dispositivi di Industria 4.0 sono altamente interconnessi e digitalizzati.

Infine, altra questione, che si accompagna a implicazioni anche di natura etica, riguarda il c.d. *Digital Divide* o divario digitale[18].

I nuovi paradigmi di Industria 4.0 comportano trasformazioni tali da incidere non solo sul piano economico, ma anche sul piano sociale. Il pericolo è che alle disuguaglianze nella distribuzione dei redditi e della ricchezza già preesistenti si sommino quelle nell'accesso e nell'utilizzo delle nuove tecnologie. Si è osservato che in molti settori tecnologici si siano verificati fenomeni del tipo *winner takes all,* cioè situazioni nelle quali emerga un'unica impresa vincente nella competizione con le altre che si impossessi del monopolio dell'intero mercato (si pensi ai casi di Google e Facebook).

Questa tendenza si sta verificando anche in contesti manifatturieri e, probabilmente, singoli Paesi potranno conquistare un vantaggio competitivo incolmabile rispetto ad altri.

Dal punto di vista dei lavoratori, invece, il pericolo è che molti individui perderanno il proprio posto di lavoro e si troveranno nell'impossibilità di trovarne uno.

Di fronte a questi rischi, occorrerà, probabilmente, incentivare politiche pubbliche volte ad evitare che le disuguaglianze permangano o, addirittura, si accentuino.

1.4. Quarta rivoluzione industriale e trasformazioni delle attività lavorative

L'organizzazione del lavoro, nelle fabbriche, a seguito delle innovazioni tecnologiche, ha subito cambiamenti importanti. Se, da un lato, si assiste alla nascita di nuove professionalità, caratterizzate da elevate competenze tecniche, dall'altro lato, si constata la progressiva estinzione di alcuni mestieri e il depauperamento di altri[19].

Certamente, nel prossimo futuro, capacità decisionali ed *e-skills* rappresenteranno priorità non prescindibili. Si parlerà, sempre più spesso, di "idealtipi", piuttosto che di figure professionali specifiche. Ai "nuovi" lavoratori verrà richiesta la competenza di gestire le informazioni prodotte dalle macchine e quella di assumere decisioni conseguenti, in tempo reale, quindi, con capacità di *problem solving*.

Nelle fabbriche del prossimo futuro si modificherà la natura dell'interazione uomo-macchina. Infatti, i *CoBot* saranno in movimento nello spazio e non già fermi, in una postazione fissa, come è stato fino ad ora. Ad essi verranno affidate quelle funzioni di carattere alienante, ripetitive e fisicamente gravose per gli esseri umani. Le macchine addette alla produzione diventeranno flessibili e capaci di segnalare i guasti e consigliare gli operatori umani rispetto alle scelte da prendere. E' prevedibile che le

[18] Cfr. L. Sartori, *Il Divario digitale. Internet e le nuove disuguaglianze sociali*, Il Mulino, 2006.
[19] Beltrametti, Intini, Guarnacci, La Forgia, op. cit., pag.135.

fabbriche avranno un elevato grado di flessibilità e le postazioni di lavoro fisse, sul piano dello spazio e del tempo, non esisteranno più. I lavoratori assumeranno, progressivamente, una funzione di gestione delle informazioni fornite dalle macchine e saranno chiamati ad assumere decisioni, piuttosto che a svolgere, come è accaduto fino ad ora, attività, fisicamente, usuranti. La qualità della vita nelle fabbriche sarà certamente migliore. Le parti sociali dovranno preordinare dei modelli nuovi di organizzazione aziendale, più flessibili ed adeguati alle nuove esigenze. Nel futuro prossimo, in fabbrica, potrebbero essere operative macchine capaci di riconoscere l'operaio che si trova davanti a loro e fornirgli indicazioni nella sua "lingua tecnica", individualizzando l'erogazione delle informazioni in base al soggetto ed alla sua competenza.

Il *management* delle nuove imprese dovrà avere competenze adeguate e conoscere le nuove tecnologie per poter realizzare investimenti pertinenti in relazione alle stesse tecnologie e definire le strategie aziendali più opportune[20].

Autorevoli osservatori (ad esempio il World Economic Forum, 2016) ritengono che, nel prossimo futuro, nei luoghi di lavoro, diventeranno rilevanti non soltanto, le competenze tecnologiche verticali, ma, soprattutto, quelle relazionali, poiché si prevede che ai lavoratori sarà richiesta una mobilità elevata fra diversi ruoli e vari progetti, valorizzando, di conseguenza, *soft skills*, idonei a supportare la cooperazione e la negoziazione[21].

Nel saggio *La Nuova Rivoluzione delle macchine,* gli economisti del *MIT* Erik Brynjolfsson e Andrew McAfee*,* sostengono che, ad oggi, resterebbero al di fuori del "potere delle macchine" le professioni caratterizzate da *skills* emozionali, affettivi, relazionali, creativi; come pure, le professioni che elaborano diagnosi, difficilmente replicabili[22].

Molti studiosi sostengono che viviamo un'epoca di transizione verso assetti nuovi di mercato, sociali, tecnologici, che dovranno ricreare posti di lavoro più gratificanti. Ci troveremmo di fronte, quindi, ad una forma di *Shumpiteriana* "distruzione creativa". In tale prospettiva, gli strumenti per combattere la disoccupazione sarebbero già contenuti nelle forme stesse dei processi di innovazione; anche se risulterebbe necessario cogliere le opportunità attraverso la creazione di posti di lavoro che siano di *knowledge workers*. Occorrerebbe qualificare la manodopera, portandola a migliorare le performance, anche, sul piano qualitativo[23].

Esiste una contrapposizione di correnti di pensiero fra i cosiddetti catastrofisti, cioè fra coloro che sostengono la "degradazione del lavoro"[24], a causa della perdita di competenze, causata

[20] Ivi, pag. 137.
[21] Ivi pag. 140.
[22] Cfr. A. Magone - T. Mazali, *Industria 4.0, Uomini e Macchine nella Fabbrica Digitale*, Guerini e Associati, 2017, pag. 87.
[23] Ivi, pagg. 85-87.
[24] Cfr. H. Braverman, *Lavoro e capitale monopolistico: la degradazione del lavoro nel XX secolo*, Einaudi, 1978.

dall'espandersi dei profili scientifici del *management* e dalla proliferazione dell'automazione e dall'altro lato, gli innovatori, cioè, coloro che sostengono, al contrario, l'approccio e le conseguenze positive dell'introduzione, in fabbrica, delle nuove tecnologie, che viene giustificato dal diffondersi della professionalizzazione e dell'istruzione tecnica, nell'ambito dei profili collegati ai processi produttivi[25].

Catastrofisti ed innovatori non concordano sulle conclusioni, ma condividono una medesima riflessione: mentre, negli Anni Settanta le ristrutturazioni erano seguite da una nuova dislocazione dei posti di lavoro, ora non appare semplice prevedere l'avvicendabilità di tutti licenziati con un pari numero di nuovi assunti. I beni e i servizi sono oggetto di una combinazione produttiva sempre meno delimitata fra loro. Le nuove figure professionali che emergono dalle innovazioni tecnologiche nelle fabbriche mancano di una tipizzazione e di una configurazione idealtipica[26].

Nella fabbrica intelligente, a differenza che nel passato, si chiede all'operaio di assumere consapevolezza del processo produttivo tecnologico, del quale deve conoscere la logica di fondo.

Nello stabilimento Avio Aero a Rivalta, di Torino, campeggia la figura di *Blu collar* polivalente, o "esperto di flussi", che riporta di attualità dei profili che l'evoluzione della manifattura aveva proposto, precedentemente. Il profilo più evoluto nella fabbrica *smart*, controlla e monitora il ciclo produttivo. Si pone la necessità di una maggiore integrazione fra il settore produttivo e le funzioni che conferiscono intelligenza alle macchine. Pertanto, il *Blue collar* deve essere poliedrico, ma al contempo, maggiormente collaborativo e comunicativo rispetto ai livelli gerarchici superiori[27].

Nonostante ciò, il *Blue collar* non si può considerare già un maturo lavoratore della conoscenza, mancando, ancora, una strutturazione ed una standardizzazione delle sue competenze tecnologiche; si tratta, bensì, di un auspicio di crescita professionale generalizzata, da consolidarsi nelle fabbriche più *smart* ed evolute[28].

L'integrazione rappresenta un fattore caratterizzante della fabbrica intelligente, nella quale si realizza una vera e propria compenetrazione fra il lavoro dei tecnologi e quello degli addetti al *manufactoring*, sebbene questa accresciuta integrazione non produca una relazione fra pari, ma, al contrario, metta in evidenza la differenza gerarchica fra coloro i quali forniscono il processo tecnologico e gli operai che devono solo monitorare l'attuazione dei processi. Comunque, gli ingegneri di nuova concezione diventano anche loro polivalenti come gli operai, assumendo nelle loro attività funzioni prima distinte fra loro ed acquistando, anche, capacità di rapida attuazione operativa dei processi.

[25] A. Magone - T. Mazali, op. cit., pag.96
[26] Ivi, pag. 88.
[27] Ivi, pagg. 89-91.
[28] Ivi, pag. 99.

Un altro effetto determinato dall'integrazione nelle fabbriche *smart* è rappresentato dall'esigenza di condividere dei linguaggi comuni, come l'Inglese, che, deve essere conosciuto, in particolare, dall'ingegnere, il quale pur provenendo da diverse aree geografiche, può colloquiare e comprendersi con il collega e con l'operaio, il quale, anche lui, deve conoscere almeno i termini basilari della lingua.
È opportuno soffermarsi sulla ridefinizione del rapporto uomo-macchina. Infatti, pur essendo sempre più pervasivo e determinante il ruolo delle macchine nella *smart factory*, appare imprescindibile il ruolo dell'operaio che verifica il funzionamento del processo tecnologico, che ha bisogno comunque, del controllo, insostituibile, da parte dell'essere umano, con le sue conoscenze tecniche e sociali e la sua capacità di tradurre il linguaggio digitale.
D'altra parte, nella *smart factory* si stanno diffondendo formule di controllo a distanza sui processi produttivi delle macchine, ad opera di lavoratori, che, in remoto, a distanza, verificano l'esito del processo di produzione, attraverso lo *smartphone*, un computer, con l'installazione di webcam e sensori presenti sui punti strategici della catena di montaggio.
È chiaro, quindi, che l'operaio della fabbrica intelligente si interfaccerà, sempre di più, attraverso il proprio *tablet*, con la macchina addetta al processo produttivo.
Ad esempio, la General Electrics, già nel 2012 con un investimento di 1,5 miliardi, ha installato 10,000 sensori nel suo stabilimento di Schenectdaty, tutti connessi alla rete aziendale, rendendo, di conseguenza, possibile ai suoi operai, il monitoraggio dell'andamento produttivo grazie al *loro I-pad*.
Questo nuovo sistema di controllo inciderà, profondamente, nella vita quotidiana dei lavoratori. Infatti, la flessibilità della produzione, che sarà resa possibile dalla diffusione dell'utilizzo delle nuove tecnologie, insieme alla diversa natura della domanda da parte dei consumatori, potrà consentire orari di lavoro più flessibili e la possibilità, in alcuni casi, di necessità familiari o di salute, anche, di poter lavorare a distanza, senza particolari problemi.
Tutto ciò, come abbiamo anticipato, dovrebbe consentire un miglioramento della qualità del lavoro dell'uomo, ma alla fine, un giudizio completo sull'avvento dell'applicazione delle nuove tecnologie digitali all'interno delle fabbriche, lo si potrà dare, soltanto, fra qualche tempo, dopo aver verificato, in modo definitivo, le effettive conseguenze del nuovo modello aziendale della fabbrica intelligente e l'impatto dell'Industria 4.0 sull'occupazione e sulla qualità del lavoro degli operai.
Tuttavia, è verosimile che, come già accaduto in conseguenza di tutti i progressi tecnologici realizzatisi a partire dal XVIII secolo, la *disruption* provocata dalla rivoluzione digitale avrà effetti notevoli in ambito occupazionale nel breve periodo, che saranno riassorbiti dai nuovi equilibri che si ristabiliranno nel medio-lungo periodo. Il sistema economico conseguirà un livello di produttività

superiore e la domanda di lavoro muterà profilo, ma riuscirà a riassorbire coloro che erano stati eliminati dal mercato del lavoro[29].

[29] Cfr. P. Boccardelli – D. Iacovone (a cura di), *"L'impresa" di diventare digitale. Come la rivoluzione tecnologica sta influenzando la gestione di impresa*, Il Mulino, 2017, pagg. 10-11.

CAPITOLO 2
LE IMPRESE SCELGONO LA DIGITALIZZAZIONE

2.1. Il ruolo centrale delle informazioni nel nuovo paradigma economico

Quando si parla di "Informazione" ci si riferisce ad un insieme di dati, che, uniti tra loro, danno origine ad un'idea che viene divulgata.

La società moderna non può fare a meno della "Informazione" per il proprio funzionamento e per la riproduzione della comunicazione, tanto che l'informazione stessa è divenuta un paradigma per descrivere la società contemporanea come "Società dell'informazione"[30]. L'informazione assume una posizione centrale, ritagliandosi il ruolo di risorsa strategica che condiziona l'efficienza dei sistemi e divenendo fattore di sviluppo sociale ed economico, di crescita e di ricchezza culturale.

Nella società dell'informazione le nuove tecnologie informatiche e di telecomunicazione assumono un ruolo fondamentale nello sviluppo delle attività umane. Infatti, ciò che, in particolare, la caratterizza è il prevalere di un bene immateriale come l'informazione rispetto alla manifattura industriale di beni materiali; industria che era stata il settore trainante per tutto il XX secolo.

Chiunque detenga "Informazione", cerca di proteggerla e, per questo motivo, sono stati elaborati istituti giuridici come i diritti di proprietà intellettuale che tutelano il c.d. *copyright*, il diritto d'autore, il brevetto che hanno come obiettivo quello di offrire un incentivo economico ai beneficiari, garantendo loro una sorta di monopolio[31].

L'informazione può essere considerata un bene commerciale, e in quanto tale ha due proprietà principali che la distinguono da altri beni: in primo luogo è un bene non rivale, in quanto il consumo di essa da parte di un individuo non implica l'impossibilità per un altro individuo di usarla allo stesso tempo; in secondo luogo l'informazione può essere un bene non esclusivo essendo disponibile e facilmente rilevata e condivisa, anche se alcune informazioni spesso sono protette e possono richiedere uno sforzo ulteriore;

L'informazione si manifesta sotto più forme e possiede molti significati, tra questi rientra il valore economico, valore che fa rifermento al prezzo che un consumatore sarebbe disposto a spendere per acquistarla. Quando infatti l'informazione è considerata tempestiva, rilevante e aggiornata, un

[30] Il concetto di società dell'informazione fu elaborato da Daniel Bell, nel proprio libro "*L'avvento della società post – industriale*" che distingue il ruolo dell'economia che deriva dall'informazione dal ruolo che giocano ai nostri giorni le conoscenze e le scienze. Secondo Bell questa distinzione avrebbe favorito la creazione di infrastrutture e di servizi adatti alla distribuzione dei servizi stessi.

[31] Cfr. L. Floridi, *La Rivoluzione dell'informazione,* Codice, 2012, pag 109.

individuo sarà disposto a pagare un corrispettivo per la sua utilità attesa, consapevole infatti di ottenere un beneficio e un'assenza di danno dato dalla qualità di quest'ultima.[32]

L'insieme dei metodi e delle tecniche per garantire poi la trasmissione, la ricezione e l'elaborazione dei dati e delle informazioni prende il nome di TIC (Tecnologie dell'Informazione e della Comunicazione) in inglese ICT; essendo l'informazione un bene prezioso, l'uso della tecnologia nella gestione di quest'ultima assume oggi grande importanza strategica.

La disponibilità di informazioni tempestive e affidabili ha determinato la revisione e la semplificazione di molti processi interni alle organizzazioni, e tra le organizzazioni, con un incremento dell'efficienza e della produttività complessiva dei sistemi.

Lo strumento che maggiormente ha inciso nella costruzione dello scenario attuale, dando vita alla cosiddetta trasformazione digitale è Internet. Questo strumento ha consentito in maniera più rapida il reperimento di informazioni da parte delle imprese, le quali le utilizzano per migliorare l'offerta e soprattutto la *Customer Experience*.

La possibilità di reperire informazioni in maniera più rapida è dovuta al passaggio dall'*off line* all'*on line* e in particolare dalla disponibilità da parte dei consumatori, continuamente connessi ai loro dispositivi di farsi raggiungere in qualsiasi momento e in qualsiasi luogo grazie ai sistemi di geo-localizzazione, che forniscono alle aziende numerose indicazioni; se nel passato infatti, le informazioni derivanti dal comportamento del consumatore venivano classificate e raccolte unicamente dalle imprese attraverso l'esperienza di acquisto sui canali fisici, nello scenario attuale i consumatori posso effettuare acquisti direttamente *online* essendo Internet molto più che un semplice catalogo illustrato;

In questo modo, le imprese possono tracciare le abitudini dei consumatori, registrando non solo la fase di acquisto finale ma raccogliendo informazioni sulla fase precedente all'acquisto analizzando i giudizi espressi, le esperienze di acquisto passate, le abitudini di acquisto, la disponibilità a pagare dei clienti, e la ricerca di un determinato bene o servizio[33].

La consistente mole di informazioni disponibili sul mercato, se opportunamente utilizzata, permette di ottenere un vantaggio competitivo; per questo motivo i dati digitali non sono più un ostacolo, ma consentono di migliorare servizi, prodotti e processi[34].

La tecnologia, nello scenario attuale, è essenziale per gestire questa mole di informazione. È necessario, per questo motivo, che le figure professionali all'interno delle imprese, conoscano e si specializzino nella cosiddetta "Digital Literacy". Questa espressione fu usata per la prima volta da

[32] Ivi, pag 101.
[33] Cfr. P. Boccardelli – D. Iacovone (a cura di*) "L'impresa" di diventare digitale. Come la rivoluzione tecnologica sta influenzando la gestione di impresa*, Il Mulino, 2017, pag 57.
[34] Ivi, pag 61.

Paul Gilster, il quale nel suo libro la definisce come "*la capacità di comprendere e utilizzare le informazioni, in diversi formati, a partire da una vasta gamma di fonti accessibili tramite computer"*[35].

Le competenze digitali perciò non sono considerate più un fenomeno che interessa solo particolari imprese tecnologiche, ma si tratta di una realtà che interessa tutti i settori. Le nuove figure professionali, appunto, devono saper gestire con semplicità le "Digital Hard Skill", cioè le competenze digitali di base, specifiche che consentono alle imprese di raggiungere il vantaggio competitivo. Queste competenze possono essere acquisite con corsi di perfezionamento o direttamente sul posto di lavoro, con l'obiettivo di saper usare con spirito critico le tecnologie della società dell'informazione (TIS).

Le imprese perciò, avvertendo il deficit e la mancanza di personale in questo settore, cercano di assumere ai vari livelli dell'organizzazione, persone che sono in grado di rinforzare il patrimonio aziendale di *e-skill*.

Normalmente un'impresa per raccogliere informazioni prende in considerazione diverse fonti, in particolare un articolo pubblicato nel 2014, nella rivista Accademy of Management ne ha individuato cinque tipi:

- Dati pubblici, i quali possono essere sfruttati per un gran numero di applicazioni
- Dati scarichi, che, anche se non ritenuti primari sono essenziali in combinazione con altri per generare nuove informazioni
- Dati privati, considerati essenziali per raccogliere informazioni private possedute da imprese e individui
- Dati della comunità, i quali creano trend e preferenze della società
- Dati di auto-quantificazione, che fanno riferimento alla quantificazione di singole azioni e comportamenti[36].

Spesso succede che i dati raccolti possono presentarsi in un formato diverso da quello desiderato, ed è perciò necessario ricorrere ad un'analisi che consiste in un processo di estrazione degli stessi, in modo da organizzarli in modo più adeguato. Uno strumento proprio per analizzare e monitorare i click dei clienti è rappresentato da Google Analytics, un vero e proprio mezzo che illustra le statistiche e i dati relativi agli accessi degli utenti di un sito internet, per esempio in caso di invio di newsletter è possibile calcolare il numero di visualizzazioni dell'articolo o il tempo impiegato a leggerlo.

[35] Cfr. P. Gilster, *Digital Literacy,* John Wiley & Sons Inc, 1997.

[36] Ivi, pag 58.

La vastità di dati digitali disponibili permetterà di liberare nuove fonti di valore economico grazie ad una corretta gestione dei dati; i Big Data danno una spinta all'economica creando una trasformazione dei tradizionali modelli di business in nuove opportunità di utilizzo di *Business Intelligence.*

La raccolta di informazioni "*crea notevoli opportunità di miglioramento per la società moderna e accelera l'innovazione e lo scambio di idee*"[37].

2.2 Nuovi modelli organizzativi digitali e vantaggi competitivi

La trasformazione digitale ha radicalmente modificato il modo in cui le imprese operano all'interno dei loro processi organizzativi e come queste si rapportano con il mondo esterno. Questa rivoluzione sta avvenendo in una particolare fase del mercato, nella quale si dà molta importanza alle esigenze della clientela, la cosiddetta "*age of customer*", in cui si cerca di soddisfare ogni bisogno e aspettativa del consumatore per raggiungere un vantaggio competitivo. Per alcuni versi, si sono modificati quelli che sono gli equilibri tra domanda e offerta: se in passato, l'economista Say con la sua legge[38] affermava che "*è l'offerta che crea la sua domanda*" poiché l'offerta determina la nascita di un bisogno nel consumatore che prima non aveva, oggi invece si può affermare che è la domanda da parte dei clienti che manda segnali alle aziende, le quali si impegnano a produrre prodotti e servizi per soddisfare le loro aspettative. Le aziende perciò devono ascoltare la domanda, i consumatori.

Una vera e propria trasformazione digitale non può essere messa in atto da tutti i tipi di imprese, o meglio alcune di esse possono trovare degli ostacoli. Le imprese del XX secolo per esempio, hanno sempre adottato una struttura di tipo funzionale, caratterizzata da un'organizzazione interna di tipo verticale, nella quale i ruoli erano tipicamente articolati in maniera gerarchica, in cui non è presente spirito di iniziativa e collaborazione tra i dipendenti, un approccio cioè tipicamente definito *top-down,* che da una parte porta benefici per il mantenimento del cosiddetto *status quo*, ma non è adatto per un'impresa che attraversa una fase di rapida trasformazione.

Un esempio è dato dal fallimento di Blockbuster, che a causa della sua incapacità di innovarsi, non è riuscito a tenere il passo ed è stato superato dalla concorrenza come Netflix che, di contro ha saputo sfruttare i vantaggi della trasformazione digitale. Questo tipo di aziende, al contrario, sono aperte e accomodanti, si caratterizzano per modelli organizzativi "*sviluppati orizzontalmente, poco gerarchici*

[37] Ivi, pag 59.

[38] In economia la legge di Say fu enunciata dall'economista francese Jean-Baptiste Say (1767-1832) e fa riferimento al fenomeno delle crisi economiche. Egli sosteneva che in regime di libero scambio, non sono possibili crisi prolungate perché l'offerta crea la domanda. Se in un particolare momento si ha un eccesso di offerta, i prezzi tenderanno a scendere, e ciò renderà conveniente la domanda. È in questo senso che egli sostiene che l'offerta è sempre in grado di creare la propria domanda.

e non burocratizzati"[39], del tutto opposti a quello del caso precedente, con una struttura non più di tipo funzionale ma a matrice o divisionale, in cui non è presente un ambiente teso, in competizione in cui tutti pensano ai propri interessi, ma i colleghi collaborano tra di loro, scambiano le idee, sono aperti e pro innovazione. Le decisioni o le idee non sono più prese unicamente e ascoltate dai vertici dell'impresa, da poche persone inquadrate ma da tutti coloro che si sentono liberi di esprimere.

Tra i nuovi modelli organizzativi quelli che si stanno affermando in particolare rispetto agli altri, e che permettono di realizzare in maniera più semplice una *Digital Transformation*, sono: la *Flatter organisation*, le *flatarchies* e le *holacracies*[40].

Il primo modello è organizzato in maniera orizzontale, nel quale si promuove un "*un forte orientamento al coordinamento spontaneo e alla comunicazione tra tutte le risorse interne appartenenti ai diversi livelli gerarchici*". Per fare ciò le imprese che decidono di adottare questo modello, danno importanza sicuramente al ruolo della tecnologia ma anche ai leader aziendali, cioè a coloro che si trovano al vertice dell'organizzazione e prendono le decisioni. Il ruolo di questi è fondamentale in quanto non devono trasmettere una cultura organizzativa negativa facendo percepire ai colleghi che loro soltanto hanno il controllo, ma al contrario in questo modello chi si trova al vertice deve promuovere flessibilità interna e valorizzare le risorse umane, in modo che tutti possano essere liberi di decidere come e dove lavorare.

Anche il secondo modello è contraddistinto da una struttura orizzontale, caratterizzata da collaborazione interna e flessibilità, in cui sono presenti dei laboratori il cui obiettivo è quello di individuare e promuovere progetti. Questo modello infatti è caratterizzato da *flat term,* cioè da unità formate da un certo numero di persone le quali sono in continuo aggiornamento e in totale autonomia si concentrano sull'innovazione. Questa modalità cerca di sviluppare le doti di *leadership* e di valorizzare le capacità dei dipendenti.

L'ultimo modello organizzativo prende il nome di *Olacrazia*, nel quale tutte le figure che si trovano all'interno dell'impresa non solo hanno la possibilità di influenzare idee o decisioni aziendali, ma possono farsene carico. In questo modello non esiste gerarchia, in quanto non esiste nessuna figura che ha il potere assoluto e al contrario si promuove l'auto-organizzazione, la trasparenza, la libertà di accedere a tutte le informazioni. Tutto ciò però si realizza in realtà aziendali relativamente piccole, nelle quali risulta più semplice realizzare un'organizzazione totalmente orizzontale. Più grandi saranno le imprese, più difficile sarà il passaggio verso questo nuovo paradigma, e più complesso sarà raggiungere alti livelli di innovazione.

[39] Cfr. P. Boccardelli – D. Iacovone (a cura di*) "L'impresa" di diventare digitale. Come la rivoluzione tecnologica sta influenzando la gestione di impresa*, Il Mulino, 2017, pag 232

[40] Ivi, pag 232

Si può affermare che i modelli organizzativi sopra descritti sono caratterizzati da elementi altamente tecnologici, i quali però sono fondamentali ma non sufficienti per poter identificare un'azienda come pienamente *digital oriented.* La tecnologia infatti è indispensabile per iniziare un processo di trasformazione digitale, poiché permette di informatizzare processi rendendo le imprese più efficienti, esse per esempio sono in grado analizzare i dati e le informazioni raccolte attraverso i Big Data Analytics. La tecnologia inoltre permette di intensificare la capacità di comunicazione e collaborazione all'interno dell'impresa, di snellire l'organizzazione grazie a processi automatizzati che sono in grado di ridurre via via distanze, sia temporali che spaziali. È anche necessario però che le imprese adottino un nuovo *mindset,* cioè è necessario affiancare alla trasformazione del modello di business, l'evoluzione del modello organizzativo aziendale. Ciò significa che la nuova organizzazione deve diffondere una cultura diversa da quella fin ora adottata, che enfatizzi e promuovi l'importanza della collaborazione, della cooperazione tra le risorse interne ed esterne dell'impresa, bisogna garantire libertà e un ambiente in cui chi ci lavora possa poter prendere decisioni in totale autonomia; ciò che poi permette di accelerare il processo di innovazione è l'apertura dei confini aziendali a università e clienti di riferimento.

Spesso quando le imprese decidono di attuare un processo di rivoluzione digitale, decidano di introdurre nuove tecnologie solo in alcuni ambiti dell'azienda, ma se questo processo non arriva a termine e al contrario rimane circoscritto solo in alcuni settori, l'innovazione rischia di rimanere limitata solo in singole unità. Questo modo di operare è sbagliato perché le imprese in questo modo, decidono di sfruttare i vantaggi che può offrire la digitalizzazione solo attraverso il mero utilizzo delle tecnologie, senza quindi portare avanti una vera trasformazione organizzativa[41]. È anche vero però che esistono situazioni opposte, in cui prima si diffonde una nuova cultura digitale e l'orientamento all'innovazione. Solo in questo modo si può parlare di rivoluzione digitale, la quale non può essere solo tecnologica. "*L'attuazione di una trasformazione di successo è dunque fortemente guidata da un'efficace leadership, affiancata dalla condivisione di un chiaro purpose"*[42].

Per far sì che la trasformazione digitale all'interno dell'impresa si realizzi, è necessario che il *Chief Digital Officer,* responsabile della realizzazione di questo processo, riorganizzi in maniera sistematica tutta l'organizzazione: dalla struttura fino ai processi interni. Egli ha bisogno di essere orientato, di avere una guida da seguire che gli possa essere utile per il compimento di questo processo. Tra i tanti modelli di *framework* che vengono suggeriti per l'attuazione dei processi di trasformazione digitale, uno di questi prevede quattro fasi: definire la sfida digitale*,* mobilitare tutta l'organizzazione, focalizzare gli investimenti, rendere scalabile la trasformazione. Il primo passo è quello di prendere

[41] Ivi, pag 242.
[42] Ivi, pag 246.

consapevolezza del cambiamento che sta per avvenire, valutare poi lo stato attuale dell'organizzazione e definire gli obiettivi a cui si vuole arrivare. Una volta che è stata definita la prima fase, è necessario che il CDO coinvolga tutti i soggetti attivi nell'organizzazione che saranno interessati dal processo e stabilire in modo chiaro il modello di *governance*. Il terzo passo è quello di definire con chiarezza gli investimenti da fare per compire il processo di trasformazione digitale, definire un budget e le risorse. Infine è necessario monitorare facendo riferimento al medio lungo termine il processo, controllare in maniera continua le performance generate dai nuovi metodi *digital-oriented* e una volta che questi progetti si saranno consolidati, allora sarà possibile estenderli al resto dell'organizzazione[43].

Questo modello quindi è considerato fondamentale per orientare le principali azioni necessarie per condurre e attuare una *Digital Transformation*, e affinché si arrivi al compimento del processo, è necessario che ogni fase sia completata cosicché si possa passare a quella successiva per arrivare poi all'obiettivo finale.

Nella prima fase per esempio non bisogna sottovalutare il passaggio che riguarda il creare consapevolezza: molto spesso, infatti, nonostante il management sia consapevole degli effetti della trasformazione digitale, tende comunque a ritenere che quest'ultima non sia così necessaria e posticipa le azioni per motivi di budget e risorse. Per motivare e convincere gli imprenditori ad attuare questo processo è bene a volta ricordare loro il racconto del tramonto di Blockbuster e l'alba di Netflix. Come già accennato in precedenza, Blockbuster nel 2004 era la più grande azienda di noleggio film ma con il passare del tempo non sentì l'esigenza di innovare il proprio modello di business. Questo errore però favorì un'altra azienda, Netflix che, innovandosi, fece un passo avanti offrendo film *on demand* direttamente visibili online. Blockbuster reagì a questa mossa troppo tardi e il risultato fu il fallimento dichiarato nel 2010, con Netflix considerata leader di mercato[44].

Un cambiamento digitale richiede convinzione e coinvolgimento e molto spesso la paura è uno stimolo utile per motivare il management a muoversi.

Una volta convinto il management sulla necessità di muoversi, è necessario coinvolgere tutti i soggetti dell'organizzazione; per farlo è importante come già accennato in precedenza, promuovere e trasmettere una nuova cultura organizzativa. Questa fase è fondamentale in quanto, di fronte ogni cambiamento, ogni soggetto può reagire in maniera differente. Le reazioni al cambiamento possono manifestarsi in quattro possibili modi: un lavoratore può nel migliore dei casi accettare il cambiamento, con entusiasmo e cooperazione positiva, può manifestare indifferenza con apatia e

[43]Cfr. A. Prunesti – M. Bombardieri, *Chief Digital Officier Gestire la Digital Trasformation per persone e organizzazioni,* Franco Angeli, 2019, pag 58.
[44] Ivi, pag 60.

perdita di interesse verso il lavoro, resistenza passiva lavorando seguendo alla lettera le regole, e nel peggiore dei casi resistenza attiva cioè fare il meno possibile, assentarsi, non avere stimoli e fare errori. Questi quattro possibili modi di reagire al cambiamento sono propri di ulteriori quattro tipologie di lavoratori: i resistenti che temono il cambiamento e l'utilizzo dei nuovi metodi, conservatori che conoscono i vantaggi delle tecnologie digitali, ma rimandano l'adozione, coloro che sono affascinati da queste nuove tecnologie e le sperimentano in maniera personale e infine ci sono i leader che favoriscono l'innovazione e promuovono nuove soluzioni tecnologiche.

L'obiettivo di un processo di trasformazione digitale è quello di trasformare le persone in leader[45].

Una volta che l'organizzazione ha individuato l'entità del cambiamento, prima di far partire il processo di trasformazione digitale, occorre pensare a quali possibili fattori potrebbero far fallire il processo. Occorre considerare che le organizzazioni più efficienti per esempio trovano maggiori difficoltà nell'adottare il cambiamento, quando infatti il business va bene, il senso di urgenza non è pressante; i manager che si trovano al vertice dell'azienda sono più resistenti al cambiamento in quanto il loro ragionamento è: perché rischiare di perdere la posizione acquisita in azienda, per iniziare un progetto rischioso?

In un processo di trasformazione digitale occorre sempre partire dal proprio core business. È necessario indentificare quali potrebbero essere gli *asset* dell'azienda che possono essere trasferiti sul digitale tra il brand, i prodotti, e i principali *asset* sono:

- *Asset* fisici i quali comprendono punti vendita, i magazzini. Questa potrebbe essere un'efficace soluzione in quanto molto spesso avere diversi punti vendita sparsi nel territorio comporta solo ulteriori costi, soprattutto quando la clientela preferisce utilizzare i servizi online.
- Le competenze digitali che sono fondamentali e che devono essere consolidate e ampliate con percorsi di formazione
- *Asset* intangibili come la *brand equity*, i valori aziendali, i brevetti.

Una volta che gli *asset* sono stati identificati, il processo di trasformazione può avere inizio.

Per identificare il punto di partenza a partire dal quale l'organizzazione sarà coinvolta in questo processo di trasformazione, può essere utile effettuare un *assessment* delle competenze del personale. Ciò che risulterà, consentirà di definire un livello di partenza che può essere base, intermedio, avanzato o super avanzato, e permetterà di erogare specifiche percorsi di formazione per ciascuna risorsa all'interno dell'organizzazione[46].

Come detto in precedenza, una trasformazione digitale richiede organizzazioni con una struttura a matrice o divisionale, in cui è presente una gerarchia liquida e aperta al cambiamento. In questa nuova

[45] Ivi, pag 65.
[46] Ivi, pag 71.

ottica perciò è necessario pensare a una nuova figura professionale che abbia come qualità un approccio *open-minded* per il cambimento, abbia competenze avanzate di gestione e in ambito digitale e abbia un ruolo di leadership nei confronti del personale; questa nuova figura professionale prende il nome di Chief Digital Officer – CDO che svolge un ruolo chiave per divulgare la sua passione per il digitale all'intera organizzazione. È attento ai bisogni dei clienti, è considerato un innovatore di prodotti e di processi, un leader. Deve essere in grado di far collaborare tra loro tutti i dipendenti e creare team di lavoro, e in particolare deve saper sfruttare le sue capacità di networking online per scoprire nuovi talenti e valorizzare le competenze.

È necessario adesso concentrarsi su quelli che sono i benefici che porta il processo di trasformazione digitale. Se ci si sofferma sul fronte interno, la digitalizzazione può massimizzare l'utilizzo di asset produttivi, come impianti e attrezzature. Tutto ciò è possibile grazie alla possibilità di "*monitorare in tempo reale le condizioni di funzionamento di tali risorse, evidenziando eventuali stati di fermo che possono essere comunicati agli operatori e permettere un intervento immediato per ripristinare le condizioni operative"*[47]. È possibile sviluppare modelli che sono in grado di segnalare in anticipo possibili situazione di anomalia nel funzionamento degli impianti; questo permetterebbe di porre in essere una serie di azioni preventive tese ad evitare il fermo impianti. Sempre sul fronte interno è possibile prendere in considerazione il tema delle risorse umane che lavorano nella produzione. Un ulteriore vantaggio infatti è costituito dalla possibilità di monitorare con maggiore tempestività le attività degli operatori e di conseguenza creare situazioni per aumentare la loro produttività. Un esempio è costituito, come già accennato, grazie una migliore formazione degli operatori sui loro cicli di lavoro. Un altro beneficio che può essere ottenuto è una migliore sincronizzazione delle attività produttive e logistiche, a questo proposito si fa riferimento alla possibilità di compiere in un tempo più corto più attività. Riguardo le attività di logistica interna per esempio gli operatori ricevono istruzioni sui percorsi da compiere in modo da ottimizzare i tempi e il numero di viaggi. Infine un ulteriore vantaggio riguarda la riorganizzazione dei processi di sviluppo dei prodotti. Le aspettative dei clienti oggi costituiscono un elemento fondamentale su cui le imprese puntano, soprattutto le aspettative sui tempi di consegna, per questo motivo sono stati sviluppati alcuni approcci come *concurrent engineering* che permettono di organizzare e gestire il processo in logica simultanea. Questo prevede di progettare in maniera simultanea, cioè di porre in essere in parallelo delle fasi di progettazione mediante l'avvio anticipato delle fasi a valle. Tutto ciò ha contribuito a snellire e a velocizzare le fasi di attività di sviluppo di un prodotto[48].

[47] Cfr. R. Secchi – T. Rossi, *Fabbriche 4.0 percorsi di trasformazione digitale della manifattura italiana,* Guerini Next, 2018, pag 29.
[48] Ivi, pag 34.

2.3. Strumenti innovativi per organizzare dati e amministrare: *Big Data* e *analytics*, *Cloud manufactoring*; *augmented reality* e *simulation*.

La grande influenza della digitalizzazione e la possibilità da parte degli utenti di essere sempre in contatto tra di loro, in qualunque luogo e in qualsiasi momento, permettono oggi di tracciare qualsiasi tipo di interazione. Tutto ciò ha un forte impatto sulle abitudini comportamentali dei consumatori e aziende, in ciò favoriti soprattutto dal crescente utilizzo di piattaforme *social network* e dalla presenza di dispositivi come *smartphone* e *tablet*[49]. Questo ha portato ad un aumento della capacità di avere informazioni preziose e al bisogno di maggiore disponibilità di spazio per l'archiviazione di dati, maggiore capacità di calcolo e di ricavare dai dati le informazioni con maggiore valore.

Questa trasformazione, cioè la digitalizzazione di quasi tutto (documenti, immagini, video, mappe) unita alle nuove tecnologie sempre più avanzate, alla diffusione di internet e dei social media ha consentito l'affermazione di un trend che prende il nome di *Big Data*: con questo termine si indica un insieme di dati, così grande, che va al di là della capacità di un normale database di catturarli e analizzarli, per questo motivo per ricavare un "valore" sono necessarie tecnologie molto avanzate. Ogni consumatore che viene a contatto con un'azienda, fornisce un insieme di informazioni, ad esempio una ricerca su Google, la prenotazione di un viaggio, un "mi piace" su Facebook, un ordine online o presso uno store sono solo alcune delle interazioni attraverso le quali le organizzazioni raccolgono dati sui consumatori. A causa di questi fattori, come già detto in precedenza, le aziende hanno bisogno di maggiore esperienza nella gestione dei dati, aumento della capacità di memorizzazione e risorse aggiuntive. I Big data presentano quattro caratteristiche: volume, velocità, varietà e veridicità. *Volume* perché implicano un enorme volume di dati, che si generano grazie alla diffusione di informazioni prodotte dalle macchine e dalle molteplici interazioni umane. *Varietà* di fonti e tipi di dato, sia strutturati che non strutturati, completamente differenziati tra loro; oggi infatti i dati non sono più rappresentati solo da fogli di calcolo, ma le informazioni sono contenute anche da email, foto o video. *Velocità* è il terzo connotato dei big data rappresentato da un flusso di dati continuo, prodotto da processi aziendali e network sociali. Infine la caratteristica più significativa dei big data è l'affidabilità e la veridicità rappresentativa del dato.[50]

Tra i notevoli vantaggi che i *Big Data* possono offrire alle aziende, il principale è rappresentato da "*una reale e concreta opportunità di produrre infinite informazioni e di permettere un incredibile*

[49] Cfr. P. Boccardelli – D. Iacovone (a cura di*) "L'impresa" di diventare digitale. Come la rivoluzione tecnologica sta influenzando la gestione di impresa*, Il Mulino, 2017, pag 63.
[50] Cfr. L. Beltrametti – N. Guarnacci – N. Intini – C. La Forgia. *La fabbrica connessa la manifattura italiana (attra)verso industria 4.0,* Guerini e Associati, 2017, pag 64.

incremento delle conoscenze aziendali"[51] ; prendendo in considerazione l'azienda Amazon, essa sfruttando le potenzialità dei *Big Data*, che si basano sul riconoscimento del comportamento di un determinato cliente e sugli acquisti eseguiti in passato, svolge giorno dopo giorno analisi per proporre nuovi prodotti che si avvicinino al suo stile. Non a caso da una ricerca svolta, basata su un campione di quasi 300 senior executive, che aveva come finalità la comprensione delle logiche e delle finalità di utilizzo dei Big Data, emerge che le tre principali ragioni di utilizzo sono: 1 una migliore comprensione dei propri clienti, 2 il miglioramento dei prodotti, 3 nuove opportunità per generare ricavi[52].

I *Big Data* inoltre forniscono ulteriori vantaggi: la grande mole di dati e informazioni disponibili fornisce alle imprese un'opportunità di accesso ai nuovi mercati, di sviluppare nuovi prodotti e di creare rapporti più duraturi con i propri clienti. I *Big Data* poi consentono "*un crescente spostamento del focus dal prodotto al servizio, ideato e personalizzato per il consumatore*"[53], e ciò rappresenta per le imprese un ulteriore canale di crescita. La maggiore disponibilità dei dati inoltre, permetterà di svolgere maggiori e migliori analisi e di conseguenza il Management sarà in grado di prendere decisioni sempre più consapevoli. Tutto ciò si può riassumere in quattro vantaggi: aumento dell'efficienza, miglioramento dei processi decisionali, miglioramento della *Customer Experience*, risparmi. I Big Data offrono ulteriori vantaggi anche alle istituzioni e agli individui, contribuendo a migliorare il mondo in cui viviamo. I settori più interessati sono: *Prevenzione del crimine*, i big data consentono di adottare strategie più efficienti per prevenire il crimine; *Previsione dei disastri naturali,* grazie all'utilizzo di sensori che possono prevedere dove si verificheranno terremoti o inondazioni.

Stabiliti quali sono i vantaggi che i Big Data offrono, è opportuno fare un passo indietro per comprendere ciò che costituisce la benzina di questo motore. Le potenzialità dei big data derivano essenzialmente da tre fattori:

- *Internet of Things*: l'espressione Internet delle cose o degli oggetti è stata per la prima volta utilizzata nel 1999, dal direttore esecutivo di un centro di ricerca del Mit, Kevin Ashton, in occasione di una presentazione. Si tratta di una rete di oggetti fisici in grado di comunicare tra loro, che uniti all'elettronica, creano una rete multistrato di oggetti intelligenti che sono in grado di aumentare la loro intelligenza grazie alla condivisione di informazioni. Nell'uso comune IoT fa riferimento ad ogni oggetto che può essere collegato ad internet, e tutto ciò costituisce un elemento fondamentale che apre infinite opportunità.

[51] P. Boccardelli – D. Iacovone, op. cit., pag 65.
[52] Ivi, pag 66.
[53] Ivi, pag 69.

- Il *cloud computing* e i minori costi di archiviazione: i nuovi strumenti di reporting infatti rendono più rapido l'accesso alle informazioni; il *cloud computing* per esempio consente di usufruire di risorse hardware e software da remoto.

- *Real-time analytics*. Il minor tempo e la velocità con cui vengono prodotte le nuove informazioni e realizzate nuove tecnologie comporta sia un aumento della velocità nel tasso di innovazione aziendale, sia un'evoluzione delle richieste dei consumatori.

L'utilizzo dei *Big Data* non può che aumentare con il tempo e questo consentirà di elaborare volumi di dati sempre più grandi e utilizzando minor tempo, ma soprattutto consentirà di gestire una crescente eterogeneità dei formati. Nonostante gli indubbi vantaggi, essi però sollevano altrettanti dubbi in particolare su privacy e sicurezza dei dati, dei quali parleremo nel prossimo capitolo. Ciò che realmente da un valore ai dati è l'analisi su questi, che altrimenti avrebbero un uso fortemente limitato, le aziende quindi possono beneficiare di aumento delle vendite, miglioramento dei servizi ai clienti, maggiore efficienza tramite la riduzione dei costi ed un aumento generale di competitività.
La gestione dei *Big Data* è strettamente legata al *Cloud*, il quale è ritenuto attualmente uno dei servizi più richiesto ed utilizzato dagli utenti. Il termine, che fa riferimento letteralmente ad una nuvola, è considerato il modo più veloce per ottenere un'analisi dati senza perdere tempo e denaro.
Il *Cloud* perciò è uno spazio di archiviazione personale, di memorizzazione ed elaborazione di dati tramite hardware e software accessibili in qualsiasi momento mediante internet. Il termine fa riferimento sia al *Cloud Storage*, sia al *Cloud Computing*.
Il primo serve per sincronizzare i file in un unico posto, con la possibilità successivamente di riscaricarli e modificarli; in questo modo si può limitare l'utilizzo di hard disk, pen drive USB. È possibile poi fare delle copie di backup e di condividere i propri file con chi chiunque.
Con il termine *Cloud Computing* invece si fa riferimento ad un insieme di tecnologie che permettono di elaborare, memorizzare e archiviare dati solo grazie all'utilizzo di risorse hardware e software.
Il *Cloud Computing* si contraddistingue per cinque caratteristiche essenziali:

- È disponibile a scaffale: il cliente perciò può acquistare il servizio senza entrare in contatto con il fornitore;
- Le funzionalità del *Cloud* sono disponibili in rete e raggiungibili tramite piattaforme client eterogenee per mezzo di meccanismi standard;
- Condivisione delle risorse, capacità di memorizzazione e di elaborazione;
- Elasticità;

- Possibilità di controllo e di ottimizzazione automatici dell'utilizzo delle risorse a disposizione, che garantisce trasparenza sia per il fornitore sia per il cliente;[54]

I modelli del *Cloud Computing* offerti alle imprese che operano nello scenario dell'Industria 4.0 sono tre: coloro che decidono di affidarsi a questo servizio hanno la possibilità di scegliere tra Iaas, Paas, Saas.

Il primo modello, "Infrastruttura distribuita come servizio" (Iaas), si riferisce ai componenti fondamentali dell'informatica che possono essere affittati; il cliente ha il controllo sui sistemi operativi e sull'archiviazione dei dati in quanto noleggia solo il numero di CPU/hard disk che gli servono.

Con il secondo modello "piattaforma distribuita come servizio" (Paas), il cliente non controlla e non gestisce l'infrastruttura *Cloud*, ma ha il controllo sulle applicazioni. Per questo motivo non paga le spese legate al servizio, le complessità legate all'acquisto e alla gestione di licenze software.

Infine con il terzo modello "software come servizio" (Saas) i provider Saas ospitano un'applicazione e la rendono disponibile agli utenti tramite internet. I clienti utilizzano l'applicazione senza preoccuparsi di sviluppo e manutenzione.[55]

Scopo principale del *Cloud* è quello di rendere disponibile le funzionalità di un software a cui si è interessati, senza acquistarlo definitivamente, permettendo di utilizzarlo in una modalità <<secondo necessità>>[56]

I motivi infine che spingono le imprese a ricorrere ai servizi di *Cloud Computing* riguardano sicuramente il *minor costo* per ciò che concerne le spese di capitale per l'acquisto di hardware e software e alla gestione di data center che richiedono elettricità 24 ore su 24, la *velocità* in quanto la maggior parte di questi servizi viene fornita con la modalità self-service, per la *sicurezza* grazie alla protezione di dati e app e per *l'affidabilità* perché aumenta la semplicità, riducendo i costi di backup.

Nel corso degli ultimi anni, le tecnologie informatiche hanno amplificato la capacità dell'essere umano, rendendo accessibili in pochi click una quantità di informazioni inimmaginabili. La possibilità di accedere in modo semplice e veloce ad una mole così consistente di dati, ovviamente, ha avuto diversi impatti sulla nostra vita personale e lavorativa.

La grande mole di informazioni disponibili da parte delle imprese ha consentito la diffusione due tecnologie che prendono il nome di **Realtà Virtuale** (VR – *Virtual* Reality) e **Realtà Aumentata** (AR – *Augmented Realit*), che ci supportano nel processo di raccolta delle informazioni, cercando di

[54] Cfr. R. Secchi – T. Rossi, *Fabbriche 4.0 percorsi di trasformazione digitale della manifattura italiana,* Guerini Next, 2018, pag 59 e 60.
[55] Ivi, pag 60.
[56] L. Beltrametti – N. Guarnacci – N. Intini – C. La Forgia, op. cit., pag 75.

creare scorciatoie per facilitare l'interazione tra l'uomo e contesto che lo circonda.

Il primo concetto presuppone l'uso di tecnologie informatiche, le quali permettono all'utente di navigare in un mondo parallelo che simula l'ambiente che ci circonda nel quotidiano. Una realtà del tutto digitale. Grazie infatti a dispositivi informativi come caschi o semplici occhiali per la vista, gli utenti si isolano dall'ambiente circostante e sono in grado di interagire con mondi virtuali tridimensionali e dinamici in cui possono essere coinvolti tutti i sensi in maniera realistica. Il termine **Realtà Virtuale** può in realtà essere applicato a due diversi tipi di simulazione, che si suddividono in "immersiva" e "non immersiva": nel primo caso il soggetto è "staccato" dall'ambiente esterno e condotto in una realtà parallela nella quale viene completamente assorbito grazie all'uso di accessori come gli occhiali 3D. Nel secondo caso invece l'ambiente creato ha un minor impatto emotivo sull'utente in quanto non vengono utilizzati caschi o guanti, ma il soggetto è posto davanti ad un monitor che rappresenta una finestra sul mondo tridimensionale e con il quale può entrare in contatto attraverso specifici joystick.

Mentre la **Realtà Virtuale** è un ambiente esclusivamente digitale, creato da uno o più computer, la **Realtà Aumentata** (AR – *Augmented Reality*) rappresenta esattamene il mondo reale arricchito però con oggetti virtuali. In particolare si tratta di una tecnologia basata su **intelligenza artificiale** e machine learning, in grado di proiettare nel mondo reale, oggetti creati virtualmente mediante l'utilizzo di dispositivi intelligenti. La realtà aumentata è fondamentale per le aziende che desiderano realizzare un vantaggio competitivo, questa tecnica infatti può migliorare l'esperienza comunicativa non richiedendo la presenza fisica. La famosa azienda Ikea, per esempio, ha creato l'App Ikea Place, una soluzione per ottimizzare l'esperienza d'acquisto del consumatore: Ikea Place permette all'utente di selezionare qualsiasi prodotto dal catalogo e posizionarlo realmente all'interno della propria abitazione. Ikea Place è un perfetto esempio di utilizzo della realtà aumentata per aziende, perché grazie alla realizzazione di un catalogo virtuale e alla possibilità di visualizzare ciascun prodotto all'interno del proprio spazio disponibile, l'esperienza pre-acquisto del potenziale cliente viene curata nel minimo dettaglio.

Queste tecnologie vengono impiegate però non solo come supporto a distanza ma anche e soprattutto per realizzare delle attività di "simulazione". Con questo termine si intende un modello virtuale in grado di riprodurre la realtà grazie all'uso di dati in tempo reale, e che permette di valutare e prevedere eventi o processi futuri. Grazie all'adozione e all'interconnessione delle macchine, sarà possibile svolgere simulazioni sulle linee di produzione in modo da testare il lavoro svolto dai macchinari ed attuare eventuali correzioni. In questo modo le imprese riusciranno a contenere il sostenimento di

ingenti costi derivanti dal *learning-by-doing*, ottimizzando tempi ed errori all'interno dei processi produttivi ed incrementando, di conseguenza, la qualità dei prodotti realizzati[57].

[57] R. Secchi – T. Rossi, op. cit., pag 51-53.

CAPITOLO 3
IL RISCHIO DIGITALE NELLE ORGANIZZAZIONI 4.0

3.1 La determinazione del rischio *cyber* in azienda

I sistemi e le tecnologie *Big Data*, affrontate nel capitolo precedente, sono da una parte il risultato del crescente utilizzo di nuove tecnologie e del mutamento dei comportamenti dei consumatori, e dall'altra rappresentano un importante *input* nel processo di trasformazione aziendale.

Questo *input* però, oltre ad offrire molte opportunità, presenta anche notevoli rischi. Questi per esempio, riguardano i rischi di attacchi informatici dall'esterno, dovuti ad i maggiori punti di accesso, alla maggiore disponibilità di informazioni e infine perché la maggior parte di queste ultime è rilevante e fondamentale, e suscita grande interesse.

Con il passare del tempo infatti, la diffusione della digitalizzazione, fa sì che i dati, che prima non erano accessibili tramite piattaforme informatiche, siano adesso più fruibili tramite il *web*. I rischi di attacchi informatici rientrano in quella disciplina chiamata *Cyber Security*, che, per l'appunto, è quell'insieme di tecnologie e processi volti alla protezione dei dati, alla loro salvaguardia, alla difesa delle reti da attacchi esterni o da accessi non autorizzati. Per queste ragioni l'evoluzione del processo di *Digital Transformation* deve andare di pari passo con l'evoluzione dei meccanismi di difesa messi in atto per prevenire ad un *cyber* attacco. È necessario considerare perciò che l'economia digitale e la sicurezza sono le facce della stessa moneta e che ad oggi la superficie di attacco di cui possono disporre i cosiddetti hacker è aumentata[58].

La questione legata alla *cyber security* non deve essere più sottovalutata in quanto i "*cyber* criminali" possono ormai attaccare da qualunque luogo del pianeta, ed è opportuno che il ruolo delle istituzioni diventa cruciale. È necessario garantire adeguati livelli di sicurezza da minacce informatiche essendo queste in continua evoluzione e gli stati devono intervenire attivamente al fine di essere pronti e saper rispondere ai rischi e ai pericoli provenienti dal nuovo paradigma della rivoluzione digitale.

Per determinare il rischio *cyber* all'interno delle imprese è opportuno far riferimento al mondo analogico: questo è basato sulla materialità delle cose e prevede che un bene tangibile possa essere protetto da attacchi fisici. In più si basa sull'idea che un bene possa essere oggetto di diverse forme di attacco, ma mai contemporaneamente (si pensi per esempio all'attacco di due bande di ladri le quali non potranno mai realizzare lo stesso colpo nello stesso posto e nello stesso momento).

[58] Cfr. P. Boccardelli – D. Iacovone, *L'<<impresa>> di diventare digitale, come la rivoluzione tecnologica sta influenzando la gestione di impresa,* il Mulino, 2017, pag 394.

Il mondo digitale invece è diverso, in quanto consente di "smaterializzare" beni e documenti e di espandere il concetto di territorialità. Per fare ciò, i documenti utilizzati vengono qualificati come "dati". Il concetto di dato infatti esprime una valenza più estesa, che si distacca dal supporto fisico di ubicazione delle informazioni per identificarsi con l'informazione stessa[59]. In questo modo le informazioni possono essere oltre che smaterializzate, suddivise in sequenze di bit e delocalizzate in più posti contemporaneamente: una parte della sequenza dell'informazione potrebbe essere salvata in un server in una parte del mondo e l'altra in un altro. Tutto ciò si traduce nella possibilità di essere attaccato simultaneamente da diversi aggressori. Due criminali *cyber* infatti, potrebbero porre in essere due attacchi contemporaneamente allo stesso sistema nello stesso momento; la protezione e la sicurezza dei dati rappresenta una sfida imponente per aziende ed enti pubblici.

Ma, mentre nel mondo analogico un criminale è esposto ad una serie di rischi e conseguenze, dovute ad un insieme di variabili e circostanze che si possono determinare, nel mondo digitale, un crimine viene realizzato in un in un ambiente cosiddetto "chiuso" e protetto: in primo luogo per elementi emotivi, dal momento che si deve immaginare la differenza tra un ladro in passamontagna e un hacker che opera dalla sua postazione rappresentata dalla poltrona del suo ufficio, tranquillo, perché quasi consapevole del fatto che la sua identità potrà difficilmente essere scoperta; in secondo luogo per elementi identificativi, in quanto mentre nel mondo analogico un ladro può correre il rischio di essere identificato da qualche conoscente, che può segnalarlo e riconoscerlo da piccoli elementi, nel mondo digitale invece sarà complicato identificare un criminale *cyber* il quale come già detto può operare in totale anonimato; ancora, nel mondo analogico un criminale per commettere un crimine deve necessariamente sottrarre un bene fisico ad un'altra persona, tutto ciò però non è indispensabile nel mondo digitale, un *hacker* può far si che siano le stesse informazioni di un utente a raggiungere il criminale informatico.

Da ciò si evince che il mondo digitale e quello analogico sono molto diversi tra loro; basta immaginare che fino a poco tempo fa sembrava impensabile effettuare operazioni *online* come l'acquisto e la vendita direttamente dalla poltrona di casa propria. Come sappiamo tutto è cambiato con l'avvento di Internet, che è entrato nelle nostre vite cambiando radicalmente il modo di trascorrere il tempo libero e quello lavorativo. Ogni gesto e operazione che viene compiuta, viene salvata sul *web* e le informazioni navigano nelle reti aziendali e negli archivi *on-line*. Se da una parte tutto ciò rappresenta un vantaggio perché grazie ad una rete disponibile, un utente può essere connesso immediatamente e molto spesso i dati vengono salvati sul web, un attacco informatico però può avvenire in qualsiasi istante.

[59] Cfr. A. Contaldo – F. Peluso, *Cybersecurity, la nuova disciplina italiana ed europea alla luce della direttiva NIS,* Pacini Giuridica, 4 luglio 2018, pag 4.

Si basti pensare che i domini italiani rimasti vittima di un *data breach*, un furto di dati, sono circa l'1,6% del totale, e il numero di *account* italiani che sono stati "rubati" arriva al 2% di quelli esistenti. Se prendiamo in considerazione l'Italia, oltre in un'impresa su due, si parla del 51%, è in corso un progetto per adeguare la nuova regolamentazione UE in materia di trattamento dei dati personali.
Diversi studi su scala mondiale hanno confermato che quando ai *senior leader* viene chiesto quale sia il danno maggiore che un attacco *cyber* possa provocare in azienda, la loro risposta è sempre la stessa: la reputazione del cliente e la *customer experience* da loro percepita.
Il *brand* di un'azienda infatti è considerato l'*asset* più importante, e se compromesso può provocare effetti collaterali rilevanti. Questo perché la reputazione di un brand è un *asset* delicato: ci possono voler anni per costruirlo e pochi attimi per perderlo. La ragione per cui questi attacchi possono essere così pericolosi per la reputazione di un'organizzazione è che il danno non rimane confinato all'interno dell'impresa ma come detto si estende a tutte le parti esterne coinvolte.
I clienti dell'azienda poi sono del tutto consapevoli di questo e se dovesse realizzarsi, ciò provocherebbe un effetto negativo per tutti: in caso infatti di furto di dati aziendali, i clienti metteranno in discussione l'intero *brand*, la qualità dei prodotti, la serietà del personale, ecc.
L'attacco informatico quindi è solo l'inizio della fine per un'impresa, dal momento che un'impresa può anche incorrere in problemi legali; si pensi che negli ultimi cinque anni la maggior parte delle aziende affrontano cause legali da parte di coloro che sono le vittime dei furti aziendali, nonché dai clienti dell'azienda; le imprese perciò sono responsabili di un risarcimento significativo nei confronti dei clienti e dei fornitori, ed in più devono prepararsi ad affrontare un periodo non facile nel quale saranno sottoposte a controlli e sanzioni da parte dell'autorità di regolamentazione.
Queste notizie poi, vengono diffuse a macchia d'olio, pubblicizzate e colpiscono l'opinione pubblica. Secondo Forbes, il *retailer* americano Target, che nel 2015 ha rilevato una violazione di dati a più di cento milioni di clienti, ha registrato, subito dopo, una diminuzione delle vendite del 4% e il profitto è crollato. Questo ha provocato un effetto collaterale per tutta l'organizzazione, il prezzo delle azioni è precipitato e il CEO è stato costretto a dimettersi.
Le aziende poi, non sono solo preoccupate per le conseguenze che un attacco cyber può provocare, ma sono maggiormente preoccupate anche sulla possibilità che questo possa accadere nuovamente.
Per comprendere la gravità della situazione, basta pensare che tutto ciò riguarda anche le aziende governative e nazionali, le quali non sono considerate immuni dagli attacchi on-line; in media le organizzazioni impiegano quasi 230 giorni per rivelare un attacco, un tempo abbastanza lungo che può creare danni significativi.
Il vero problema è che i criminali informatici, ripongono un'attenzione particolare sui clienti tanto quanto fa l'azienda. Il mercato dei *cyber* criminali è un mercato altamente lucrativo che guadagna sui

dati dei clienti e sulle informazioni su quello che concerne carte di credito, numeri personali e tutto ciò ne incentiva il furto. I dati dei clienti restano una priorità non solo per le organizzazioni ma soprattutto per i *cyber* criminali. Come già detto, alla luce di ciò, in ambito di *cyber security* che s'intende un insieme di tecnologie, programmi processi e tecniche messi in atto per proteggere dispositivi, dati e reti informatiche, è necessario un continuo aggiornamento delle tecniche e delle metodologie di protezione[60].

3.2. IOT e vulnerabilità dei sistemi

Come già osservato precedentemente, *Internet Of Things* è un neologismo che si riferisce all'estensione della reta *Internet* agli oggetti: le cose infatti, acquistano intelligenza grazie alla connessione in rete, e trasmettono dati agli utenti. Per essere più concreti si può far riferimento a casi quali sveglie che suonano prima in caso di traffico o code sulla strada, medicinali che avvisano i soggetti se si dimenticano di prendere il farmaco. Grazie alla connessione in rete tutti gli oggetti possono acquisire un ruolo fondamentale e attivo nella realtà di oggi.

L'obiettivo è fare in modo che il mondo elettronico e connesso a *Internet* supporti e aiuti il mondo reale nella quotidianità[61].

Chi maggiormente dovrà sfruttare le tecnologie di *Internet of Things*, per ottenere un vantaggio competitivo e raggiungere una posizione sempre più importante sono le aziende; queste infatti hanno una vasta scelta in quanto i campi di applicabilità sono molteplici; in questo modo arrivano ad offrire un servizio più completo alla clientela, la quale godrà di maggiori benefici.

L'*Internet of Things* perciò, insieme alla *Digital Transformation*, stanno avendo un impatto reale, diventando parte integrante della vita dell'essere umano. Affinché la nuova tecnologia stravolga la realtà in cui viviamo, è necessario che le applicazioni siano sempre più innovative, sia da un punto di vista tecnologico, sia da un punto di vista dei modelli di business.

L'introduzione di questa tecnologia comporta l'innovazione di processi e prodotti con importanti conseguenze sulle infrastrutture, sulle informazioni e sulle persone, tutto realizzabile grazie alle tecnologie informatiche.

Alla base di tale tecnologia vi sono più funzionalità, come *self-awareness*, cioè la possibilità di conoscere la propria identità, la capacità di conoscere la propria posizione geografica; l'interazione con l'ambiente circostante è un'ulteriore funzionalità che è alla base dell'*IoT*, che riguarda la raccolta

[60] Cfr. I. Corradini, *Internet delle cose. Dati, sicurezza e reputazione,* Franco angeli, 2017, pag 64.
[61] Cfr. I. Corradini, *Internet delle cose. Dati, sicurezza e reputazione,* Franco angeli, 2017, pag 83.

di dati tramite la misura di variabili di stato come la temperatura, la pressione o il consumo di energia elettrica; elaborazione di dati; connessione per trasmettere informazioni[62].

Cisco[63] ci dice che ad oggi i dispositivi collegati nel mondo sono più di 15 miliardi, e che entro il 2020 il numero potrebbe salire a 50 miliardi. L'obiettivo d'altronde è quello di un mondo di sensori e pc connessi in rete che porterà maggiore efficienza e convenienza.

Il rischio che si corre però è quello di dimenticare i primi anni di Intenet, per la fretta di introdurre l'*IoT*. Agli inizi degli anni 80 infatti le grandi Microsoft e Apple sistemarono le cose solo dopo che i problemi si palesassero sotto forma di virus e così via. Pensare di risolvere i problemi però solo dopo che questi si sono verificati è molto costoso e difficile, e questo errore si sta ripetendo anche con l'*Internet of Things.* Come tutte le tecnologie, infatti, anche l'*IoT* comporta dei rischi di sicurezza e questo è dovuto alla grande vulnerabilità di questi sistemi: oggi le tecnologie create per la protezione degli oggetti connessi, stanno evolvendo ma non sono ancora sufficienti per affermare che una determinata azienda sia del tutto sicura di non ricevere attacchi. Per esempio molto spesso per minimizzare i costi dei sistemi, non è possibile modificare la password o la chiave di sicurezza; in questi casi i sistemi *IoT* potrebbero funzionare con chiavi compromesse. L'uso però di password deboli, è solo la prima delle principali vulnerabilità dei dispositivi *IoT*. Bisogna considerare anche le interfacce non sicure all'ecosistema, la carenza di meccanismi sicuri di aggiornamento, l'uso di componenti non sicuri o superati, per cui si intende non solo componenti hardware ma anche software, la protezione della privacy insufficiente, la conservazione e la trasmissione dei dati non sicura, le carenze nella gestione del dispositivo, la configurazione di default non sicura e la mancanza di protezione fisica. Tutto ciò permette di affermare che questi dispositivi sono al giorno d'oggi vulnerabili e questo viene sfruttato dagli hacker, che utilizzano questa vulnerabilità per porre in essere *cyber attacks*. In più questa tecnologia promuovendo lo status di *always-on,* essere cioè sempre connessi, ha già incrementato a dismisura le possibilità di attacchi *cyber.* Essere sempre connessi in effetti significa essere sempre a contatto con il mondo esterno, quindi essere esposti a maggiori rischi. Gli attacchi da parte dei *cyber* criminali possono essere di diversi tipi:

- *Denial of service:* un attacco in cui si fanno esaurire le risorse in un sistema informatico, fino a non essere più in grado di erogare un servizio.
- *Buffer overflow:* consiste nel sosvrascrivere sezioni di memoria, provocando un crash dei sistemi.

[62] Ivi, pag 88.

[63] Cisco è un'azienda multinazionale specializzata nella fornitura di apparati di networking per il funzionamento delle reti LAN, MAN, e il sistema operativo IOS che le pilota. Questa è entrata anche nel mercato della sicurezza, attraverso Firewall e VPN.

- *Malware:* che consiste in un insieme di virus quali *trojan, worm,* che sono software dannosi che vengono utilizzati per consentire il controllo delle funzioni dell'oggetto dell'attacco e l'accesso ai dati in esso custoditi.
- *Replay attack:* consiste nell'impossessarsi di una delle credenziale di autenticazione comunicata da un host e riproporla successivamente simulando l'identità dell'emittente.
- *Side channel attack:* un attacco *cyber* reso possibile quando si dispone di un canale supplementare di informazioni offerte da output involontari sul sistema, come ad esempio controllando il consumo di elettricicità, le variazioni del campo magnetico.
- *Attacco spoofing:* si attua quando un dispositivo tenta di impossessarsi di un altro per inviare informazioni false. Un esempio di questo attacco accade nell'industria automobilistica, si parla infatti di un attacco *spoofing* GPS quando vengono inviate false coordinate al ricevitore GPS di un veicolo[64].

Questi attacchi appena elencati sono solo delle macro categorie, ma potrebbero verificarsi degli attacchi *cyber* anche in ambiti più specifici, per questa ragione bisogna garantire sicurezza durante tutto il ciclo di vita del dispositivo: in particolare in una prima fase di avvio del dispositivo *IoT*, l'autenticità del software deve essere verificata tramite firme digitali crittografate. Tali verifiche *"assicurano che solo il software preventivamente autorizzato per l'esecuzione su quel dispositivo verrà caricato e potrà operare"*[65]. Questo non basta però per assicurare al dispositivo sicurezza da parte di attacchi *cyber*, il dispositivo infatti ha ancora bisogno di protezione. L'autenticazione è un passo necessario quando il dispositivo viene collegato, prima ancora di trasmettere dati. Proprio come accade nella fase di autenticazione di un utente, che tramite username e password ha la possibilità di accedere ad una rete aziendale, così l'autenticazione di un computer consente ad un dispositivo di accedere a una rete basata su un insieme di credenziali salvate in un dispositivo sicuro.

Il controllo degli accessi deve far sì che chi accede al dispositivo abbia privilegi rappresentati da ruoli incorporati nel sistema operativo, che sono limitati solo a componenti e applicazioni di cui si ha bisogno per svolgere il proprio lavoro. Se poi una o diverse componenti dovessero essere compromesse, il controllo di accesso assicura che l'intruso, con i privilegi limitati di cui dispone, non possa compromettere l'intero sistema. I *firewall* e IPS garantiscono poi al dispositivo la capacità di ispezione approfondita per controllare il traffico che terminerà sul dispositivo. Questo permetterà di scoprire *pay-load* dannosi nascosti nei protocolli. Una caratteristica dei dispositivi *IoT* è che questi hanno poca potenza di calcolo e sono progettati per consumare poco, tutto ciò rende quasi impossibile installare degli anti-virus sul sensore.

[64] I. Corradini, op. cit., pag 89.
[65] Ivi, pag 90.

Una volta che il dispositivo è in funzione ed è attivo, sono necessari aggiornamenti software in modo da non compromettere la connettività di un dispositivo *IoT.*

La sicurezza dei dispositivi *Internet of Things* è quindi un requisito fondamentale affinché questi possono essere utilizzati, quello che serve è un circolo virtuoso che spinga da una parte i produttori a creare migliori tecnologie e dall'altro le organizzazioni ad adottarle in massa.

C'è da dire infine che l'*Internet of Things* è oggi una grande innovazione tecnologica in grado di travolgere la vita di milioni di persone e trasformare interi settori industriali, favorendo un mondo sempre più connesso, che è in grado di gestire una consistente mole di dati e informazioni preziose. Ma oltre alle opportunità questa novità porta, anche rischi che richiedono una attenta valutazione.

Solo attraverso un approccio olistico che mette insieme da una parte l'analisi dell'ecosistema dell*'IoT* e considera dall'altra le implicazioni sociali e legali si potranno disegnare le necessarie misure di salvaguardia di sicurezza e privacy[66].

3.3 La protezione dei dati nell'era digitale

Come tutti i processi storici importanti, anche il processo di *Digital Trasformation,* comporta sicuramente delle grandi opportunità ma anche rischi e pericoli. Tra i più importanti emerge sicuramente il problema della *privacy* e della sicurezza informatica. Questo tema non fa riferimento solamente alla possibile presenza di qualche virus ma al rischio che qualche soggetto entri nei sistemi digitali per rubare informazioni o provocare danni. Ancora più importante è considerare che la connessione e la condivisione dei dati mette fortemente a rischio la nostra *privacy.* Bisogna considerare inoltre che la quantità di dati che vengono trattati da aziende ed organizzazioni raddoppia ogni due mesi e si stima che entro il 2020 toccherà i 44 trilioni di gigabyte. Questa enorme crescita di dati, va di pari passo con quella dei potenziali rischi legati al loro possesso. Per questo motivo in materia di protezione dei dati, dal 25 maggio 2018 è diventato applicabile anche in Italia, il Regolamento Generale sulla Protezione dei Dati, meglio noto come GDPR, ufficialmente regolamentato (UE) n. 2016/679. La ratio persegue un equilibrio tra la tutela della sicurezza e il rispetto della privacy. L'obiettivo perciò è quello di rafforzare la protezione dei dati personali dell'Unione Europea. Di notevole importanza sicuramente è anche il Regolamento ePrivacy, il quale è complementare al GDPR e che stabilisce norme per la tutela dei dati ai fini della fornitura e della fruizione di servizi di comunicazione elettronica, come email e messaggistica istantanea.

[66] Ivi, pag 104.

Se approvato il Regolamento, andrebbe a sostituire, la Direttiva ePrivacy che ora fissa le regole per garantire la riservatezza delle comunicazioni e la tutela dei dati personali nel settore delle comunicazioni elettroniche. Questo servirà ad aumentare la fiducia dei consumatori nei servizi digitali nonché per mettere la normativa del settore in questione al passo con gli sviluppi tecnologici[67].

Il regolamento GDPR infine attraverso l'espressione "*privacy by default and by design"* richiama all'attenzione due criteri fondamentali: l'attenzione dei titolari sull'importanza che la protezione dei dati personali venga garantita "fin dalla progettazione". Il Regolamento quindi stabilisce che il titolare del trattamento dei dati personali deve adottare delle misure tecniche e organizzative idonee, in particolare la predisposizione delle misure necessarie è prescritta sia nel momento in cui il titolare del trattamento deve determinare i mezzi del trattamento stesso, sia quando pone in essere le vere e proprie operazioni di trattamento.

L'adozione di misure di sicurezza adeguate è ormai indispensabile per tutelare i dati personali; tra le migliori pratiche emerge sicuramente l'uso di password: questo strumento esiste fin dagli inizi degli anni 60, quando nacque il primo ambiente condiviso. In quel periodo nacque il Compatible Time-Sharing System del MIT, che fu il primo computer multiutente. A quei tempi non esisteva nessuna sicurezza che si basasse sulle password. Le password del CTSS erano accessibili solo dagli amministratori, ma ad un certo punto accadde qualcosa di inaspettato; a causa di un errore infatti, le password di tutti gli utenti apparvero inaspettatamente sugli schermi. Sicuramente da allora le password hanno fatto molta strada, nonostante alcuni pensino che queste siano inutili. Queste possono garantire un'implementazione sicura e rappresentare le chiavi del regno ma alcune implementazioni possono rivelarsi incredibilmente insicure. Oggi si può dire che i furti di password da parte di hacker sono ormai all'ordine del giorno: nonostante infatti tutte le misure di sicurezza e gli accorgimenti da parte degli utenti, gli attacchi da parte dei *cyber* criminali sembrano essere sempre un passo avanti rispetto agli utenti. La tecnologia però ha fatto grandi passi avanti, soprattutto negli ultimi anni. Entra in gioco infatti una particolare tecnica cibernetica chiamata *password hashing*[68]. Questa tecnica fa si che in caso di furto, il criminale si trovi in mano un lungo elenco di caratteri casuali praticamente inutilizzabile. Ecco perciò che la crittografia è considerata ad oggi il metodo più sicuro per la protezione dei dati personali, che può resistere anche agli attacchi più elaborati. Questa tecnica quindi consiste nel rendere incomprensibili i dati, cosicché chiunque ne venga in possesso non possa riuscire a comprendere nulla del loro significato.

---

[67] Cfr. A. Contaldo – F. Peluso, *Cybersecurity, la nuova disciplina italiana ed europea alla luce della direttiva NIS,* Pacini Giuridica, 4 luglio 2018, pag 55.

[68] Cfr. L. Brotherston – A. Berlin, *La sicurezza dei dati e delle reti aziendali, tecniche e best practice per evitare intrusioni indesiderate,* Tecniche Nuove, 2017, pag 129.

Nel mondo informatico infatti, la crittografia permette di convertire i dati da un formato leggibile in un formato codificato che può essere letto o elaborato solo dopo essere stato decrittato. Cifrare i dati oggi è molto semplice. L'utente deve utilizzare un sistema di cifratura, cioè prende i dati "in chiaro" e li trasforma in cifrati, cioè li oscura.

La tecnica in questione si divide in Crittografia Simmetrica e Asimmetrica:

questa appena esaminata è quella simmetrica, che viene usata da secoli e fa si che il messaggio trasmesso non sia comprensibile senza una certa informazione (la chiave). Le caratteristiche di questa prima forma sono il fatto che sia molto scalabile, i processi di cifratura sono molti veloci e ed efficienti e la struttura algoritmica è semplice; i difetti però riguardano il fatto che lo scambio della chiave deve avvenire attraverso un canale sicuro alternativo.

Il secondo tipo di Crittografia, quella Asimmetrica, utilizza invece due coppie di chiavi, una pubblica e l'altra segreta. Queste sono estremamente correlate e ciò che è criptato con una chiave può essere decriptato con l'altra[69].

Riprendendo ciò che il GDPR dice sulle tecniche di protezione dei dati poi, questo raccomanda l'utilizzo di sistemi che permettono di anonimizzare o pseudonimizzare informazioni che identificano una persona. Per quanto riguarda la tecnica di pseudonimizzazione, questa consiste nel conservare i dati in una forma che impedisce l'identificazione della persona e senza che vengano aggiunte informazioni in più. Questa è ritenuta una tecnica fondamentale sia per proteggere i dati personali di persone fisiche per garantire la piena e totale riservatezza, sia per conservare le informazioni di profilazione dell'utente in modo che non venga identificato. A differenza della seconda tecnica, qui il dato, essendo una forma pseudo-anonima, può essere ancora letto e usato.

Differente è invece l'anonimizzazione. Il titolare in questo caso non è più in grado di risalire al dato specifico di un interessato perché non possiede le informazioni complete.

Entrambe possono essere considerate due facce della stessa medaglia; entrambe oscurano i dati, tuttavia mentre la prima tecnica permette di identificare in un secondo momento i dati, i dati anonimi non consentono la successiva identificazione. Gli effetti sono molto diversi, perchè l'anonimizzazione rimuove qualsiasi elemento riconoscibile che possa permettere a tali informazioni combinate di risalire al soggetto, la pseudonimizzazione invece non elemina tutti gli elementi identificativi dei dati, ma riduce semplicemente il collegamento di un set di dati con l'identità originale di un soggetto. Entrambe possono considerarsi tecniche efficaci per ridurre i rischi al minimo su dati personali. Adottare queste tecniche poi, rappresenta anche un supporto importante per

[69] Cfr. F. Garzia, *Sicurezza delle comunicazioni, telecomunicazioni, criptografia, steganografia, digital watermarking, reti cablate, reti wireless, comunicazioni vocali, protezione delle intercettazioni,* EPC, 2012.

garantire la *Security by Design*, che è considerata indispensabile per garantire un percorso efficace verso la trasformazione digitale.

Se pensiamo per esempio alla famosa azienda statunitense Apple, questa utilizza sistemi e tecniche come la "*privacy* differenziale" per proteggere i dati personali sui dispositivi.

Questa tecnica aggiunge informazione casuali ai dati prima che Apple li analizzi, in modo tale da non essere collegati al dispositivo. I dati vengono perciò combinati con quelli di molti altri utenti e le aggiunte casuali compensano a vicenda, lasciando emergere solo schermi generali che aiutano a conoscere meglio le abitudini degli utenti, senza dare informazioni sulle singole persone.

I dispositivi iOS includono funzioni per proteggere l'intero sistema, in modo da tener a sicuro tutte le app e garantire che i dati aziendali e personali siano criptati facilmente. IOS è progettato in modo che il software e l'hardware siano sempre sicuri e offre metodi efficaci per gestire i dati: questi dispositivi hanno un processore hardware dedicato e utilizzano la criptografia AES-256[70]; la protezione di dati a livello di file usa chiavi crittografiche forti, e usa tecnologie consolidate per garantire una connessione facile.

Ad oggi perciò è fondamentale che organizzazioni ed enti pubblici adottino tecniche per la riservatezza dei dati, affinché questi non vengano divulgati, per evitare di rovinare la reputazione dell'azienda e di impelagarsi in battaglie legati infinite.

3.4. *Best practice* in tema di *data protection* nelle organizzazioni

Come abbiamo già accennato nel paragrafo precedente, la protezione e la sicurezza dei dati personali, sono argomenti all'ordine del giorno per aziende e organizzazioni, le quali hanno molto su cui riflettere quando si parla di garantire la salute e il successo aziendale. La maggior parte delle aziende dovrebbero adottare, come precedentemente detto, un approccio olistico, quando valutano quale sia il modo migliore per acquisire le capacità necessarie per promuovere e garantire la sicurezza nel proprio ambiente, e per raggiungere questo obiettivo è necessario combinare tecnologie hardware e software intelligenti.

Sin dall'entrata in vigore del Regolamento UE, il Legislatore ha posto l'accento sul concetto di protezione, d'altronde GDPR significa *General Data Protection Regulation.* Ogni sistema *privacy* deve avere come fine ultimo quello di proteggere i dati oggetto di trattamento quotidiano. In tema di *data protection* il Regolamento ha introdotto una novità: la figura del responsabile per la protezione dei dati personali, conosciuto con il nome inglese di *Data Protection Officer (DPO).* Il Regolamento

[70] Advanced Encryption Standard (AES) è uno dei più usati e sicuri algoritmi di crittografia a blocchi disponibili ad oggi. È basato su sostituzioni, permutazioni e trasformazioni lineari. Si presume, data la sua sicurezza, che in un prossimo futuro venga utilizzato in tutto il mondo.

inoltre descrive in modo chiaro le qualità, il raggio d'azione e le dinamiche aziendali associate al Dpo. Egli è un supervisore indipendente, il quale sarà designato obbligatoriamente da soggetti di tutte le pubbliche amministrazioni, ha molteplici compiti, è indipendente e ha grande autonomia decisionale.

Per prima cosa egli fornisce consulenza al responsabile della conversazione e informa tutte le figure coinvolte, sia in merito alla normativa, sia riguardo alle soluzioni tecniche adottate per rispettare gli standard imposti. La sua prima azione è quella di analizzare quelli che sono i meccanismi di raccolta e conversazione dei dati in atto; dopo una verifica sulle probabilità di perdite e sui possibili rischi, egli produce un documento nel quale evidenzia anche l'eventuale necessità di un adeguamento tecnologico o di correttivi da apportare. Dopo aver fornito un quadro generale della situazione esistente, il DPO redige un piano di aggiornamento e manutenzione dei sistemi, per restare sempre al passo con l'evolversi delle normative; egli perciò è del tutto consapevole dei rischi che la sua organizzazione può incontrare nel caso in cui le informazioni critiche e sensibili non vengano adeguatamente protette e risultino compromesse: rischi come la perdita di reputazione, perdita di fiducia da parte dei clienti e perdita dei ricavi.

Questa realtà non è presente solo nelle grandi organizzazioni internazionali, anche le PMI devono prestare molta attenzione alla protezione dei dati e delle reti. Peraltro difendersi solo dalle minacce provenienti dall'esterno dell'azienda non è sufficiente, occorre invece essere vigili anche nei confronti dei rischi all'interno dell'organizzazione. Bisogna considerare infatti che alcuni dipendenti potrebbero avere accesso a informazioni sensibili o documenti finanziari. È indispensabile perciò che le imprese applichino delle *policy* e le *best practice* per salvaguardare i dati vitali, senza ovviamente trascurare le attività di gestione.

Per salvaguardare i dati le imprese necessitano di pratiche e soluzioni capaci di integrare la sicurezza a vari livelli. Tra questi troviamo:

- **Sicurezza della rete**: utilizzo di dispositivi di rete intelligenti capaci di lavorare come una prima linea difensiva in tempo reale. Questi dispositivi isolano tutti gli utenti finché la loro autorizzazione non è stata verificata e subito dopo possono concedere l'accesso a determinate informazioni.
- **Software-Defined Networking**: sicurezza end-to-end automatizzata per *switch* di rete, router e punti di accesso wireless, che garantisce la protezione contro *botnet*, e *malware*.
- **Analisi della sicurezza**: grazie ad indagini non intrusive è possibile analizzare i dati in fase di trasferimento. Queste indagini permettono di segnalare e isolare il traffico di rete in caso di anomalie.

- **Autenticazione multifattoriale**: software capace di rilevare i casi in cui una richiesta di accesso proviene da un dispositivo o luogo sconosciuto. Richiedendo all'utente di inserire un *passcode* inviato all'account di posta elettronica conosciuto dall'utente stesso, e in questo modo si possono ridurre i furti di dati [71].

Nonostante poi l'aumento di questi attacchi *cyber* di alto rilievo, grandi perdite di dati e attacchi *ransomware*[72], molte organizzazioni non dispongono del budget necessario per creare un programma di sicurezza informatica. Per prevenire un attacco da questi virus, basta seguire semplici consigli: è necessario per esempio fare un inventario dei propri dispositivi digitali, in questa maniera quando si subirà un attacco *ransomware* si saprà dove intervenire; aggiornare il *personal computer* ogni volta che il sistema lo richiede; fare il *backup* quotidianamente di tutti i computer che sono presenti nell'azienda e infine segmentare i *network* in modo che i dati non vengano salvati tutti all'interno dello stesso file.

Per esempio un "deposito" per ogni sorta di dati, che può contenere le credenziali di autenticazione o informazioni finanziarie, e che rappresenta un obiettivo per gli utenti malintenzionati, sono i *Server* applicativi. Essi infatti essendo formati da una mole così vasta di dati, rappresentano prede per gli aggressori. È consigliabile in questi casi, per rafforzare il server, configurare l'infrastruttura che circonda un'applicazione in modo da difendere il server dagli attacchi, o più semplicemente molte vulnerabilità dei server possono essere riparate mantenendo il sistema aggiornato[73]

Tutte queste misure sono perciò fondamentali affinché le imprese possano evitare un *Data Breach,* un incidente di sicurezza in cui i dati sensibili e riservati vengono copiati e rubati da un soggetto non autorizzato. A questo proposito, L'*International Organization for Standardization*[74]*,* ha recentemente pubblicato delle linee guida sull'assicurazione per l'esigenza di *cybersecurity,* che è sempre più avvertita dalle società e in più la domanda di assicurazione è aumentata nel tempo; il mondo assicurativo perciò e del *risk management*, per rispondere a questa problematica, ha predisposto modelli di Analisi e Trattamento del rischio, che riguardano misure per assottigliare il rischio stesso. Per far fronte perciò a frodi informatiche da parte di malviventi, prendono in considerazione la polizza assicurativa.

---

[71] Cfr. C. Keegan – D. Conde – L. Matuson, *Best Practise per la protezione dei dati e la business continuity in un mondo mobile, guida per le piccole e medie imprese,* pubblicato su: https://d3alc7xa4w7z55.cloudfront.net/static/upload/protected/201/0122/2016-oss-hpe-best-practice-protezione-dati-pro.pdf.

[72] I *ransomware* sono virus informatici che rendono inaccessibili i dati dei computer infettati e chiedono il pagamento di un riscatto per ripristinarli.

[73] Cfr. L. Brotherston – A. Berlin, *La sicurezza dei dati e delle reti aziendali, tecniche e best practice per evitare intrusioni indesiderate,* Tecniche Nuove, 2017, pag 103.

[74] La ISO, *International Organization for Standardization,* è un'organizzazione indipendente che ha come scopo quello di elaborare standard diretti a dare soluzioni a problemi di interesse globale.

Le imprese in particolare, sfruttano un processo integrato di *Risk Managment*, che include l'ambito *Cyber*; questo approccio fa si che si possa prevenire e mitigare l'impatto di un rischio informatico, in quanto prevenirlo totalmente non è possibile. La copertura assicurativa può servire a tutelarsi da questi accadimenti, ma è l'ultimo dei passi da compiere di un processo che parte invece con l'analisi della realtà aziendale: dal tipo di business che conduce, l'attività e le caratteristiche. Un'assicurazione di questo genere deve poi prevedere la copertura di una vasta gamma di dati, guasti e contenuti, in particolare la copertura riguarda danni immateriali diretti e indiretti, sia cioè che si tratti di una distruzione dell'archivio sia he riguardi la reputazione dell'azienda. Chi deve assicurarsi per paura di ricevere un attacco *cyber*, sono le organizzazioni che posseggono processi interni tecnologici, come la produzione o la distribuzione, raccolgono informazioni sui clienti come i dati di pagamento online e posseggono un *database* di dati su clienti e fornitori.

Sicuramente questi accorgimenti risultano fondamentali per le organizzazioni per evitare attacchi informatici. Così facendo le imprese possono tirare un sospiro di sollievo e cercare di evitare di essere accusate di mancata tutela della *privacy* e proteggersi da possibili *data breach*.

CAPITOLO 4
IL CASO YAHOO:
ANALISI DELLE MISURE TECNICHE ED ORGANIZZATIVE ADOTTATE A SEGUITO DEI *DATA BREACH* DEL 2013 E DEL 2014

4.1. Il contesto di riferimento

In tema di violazione di dati personali (*data breach*) su larga scala, caso emblematico è quello che ha interessato Yahoo, ovvero la celebre società Americana fondata nel 1994 da David Filo e da Jerry Yang e registrata presso lo Stato del Delaware l'anno successivo, vittima di una serie di attacchi informatici che, a partire dal 2010, ne hanno dimostrato tutta la vulnerabilità[75].

La scarsa resistenza agli attacchi dimostrata da un soggetto per sua natura perennemente esposto a continue minacce ne ha irrimediabilmente compromesso la *brand reputation*.

In questa sede, si intende descrivere il *personal data breach* del 2010, confrontando la reazione dimostrata da Google (anch'essa coinvolta in veste di vittima) con quella dimostrata da Yahoo, ed infine analizzare i successivi *data breach* del 2013 e del 2014, focalizzando l'attenzione sulle misure tecniche ed organizzative di volta in volta adottate.

Infine, lo studio che ci si accinge a compiere si intreccia inevitabilmente con le vicende che hanno segnato, nel 2017, l'acquisizione da parte di Verizon del *core business* di Yahoo.

Tale processo di acquisizione va letto attraverso le lenti della "responsabilizzazione", *rectius*, della "*accountability*", così come intesa ai sensi dell'art. 5, par. 2, del GDPR, per comprendere tutto il peso e tutta la rilevanza che l'adozione di adeguate *policy / procedure* interne ad un'organizzazione è in grado di assumere.

In particolare, la storia della società IT statunitense risulta emblematica se si osservano due punti di vista distinti: da un lato la frequenza con la quale è stata vittima, nel corso di pochi anni, di una serie di importanti *data breach*, dall'altro lato il numero di interessati coinvolti: gli utenti del motore di ricerca nato dalla "*Jerry and Dave's Guide to the World Wide Web*", infatti, sono stati vittima dei due *data breach* più estesi della storia della rete, violazioni di dati personali che hanno visto inesorabilmente compromesse l'integrità, la riservatezza e la disponibilità dei dati personali di 500 milioni di utenti nel 2014 e di 1 miliardo di utenti nel precedente attacco del 2013[76].

[75] Cfr. Lawrence J. Trautmat e Peter C. Ormerod, *Corporate directors' and officers' cybersecurity standard of care: the Yahoo data breach*, "American University Law Review, LXVI (2017)", pag. 1249

[76] Ivi, pag. 1233 ss.

4.2. Le origini di Yahoo

"*Yahoo nasce come una Guida per il reperimento e la selezione delle informazioni digitali nella rete, che mira principalmente alla diffusione delle informazioni*"[77]: così la stessa società si descrive nel Rapporto annuale prodotto ai sensi della Sezione 13 e 15 (d) del "*Security Exchange Act* del 1934", per l'anno fiscale terminato nel dicembre del 2016.

In base al diritto americano, infatti, tutte le società quotate in borsa sono obbligate a produrre tale report, imposto dal "*Securities and Exchange Act of* 1934", che regola lo scambio delle transazioni dei titoli nel mercato secondario ovvero quel mercato in cui ha luogo lo scambio di titoli già in circolazione, e non di prima emissione[78]. Tali transazioni, secondo quanto stabilito dall'art. 1 dell'"*Exchange Act*", sono di pubblico interesse, e ciò rende necessario la loro regolamentazione.

Ed è nell'aprile del 1996 che la società di Sunnyvale lancia un'*Initial Public Offering*, ovvero un'Offerta pubblica iniziale di titoli azionari, decisa a quotarsi sul mercato azionario telematico statunitense, il NASDAQ (*National Association of Securities Dealers Automated Quotation system*), collocando per la prima volta i propri titoli sul mercato azionario.

Il successo fu innegabile: le azioni di Yahoo aumentarono del 154% in un solo giorno. Per tutto il decennio successivo, Yahoo fu il leader indiscusso tra i motori di ricerca esistenti in rete, un primato rimasto salvo fino alla comparsa di quello che sarà il suo principale competitor: Google.

Tanto celere è stata la crescita di Yahoo il giorno del suo ingresso nel mercato borsistico, quanto altrettanto inarrestabile sarà il decadimento delle sue azioni dopo il rifiuto dell'Offerta Pubblica di Acquisto avanzata da Microsoft nel 2008, processo che vide il suo ultimo epilogo solo con la definitiva acquisizione da parte di Verizon nel 2017.

Come anticipato, il progetto "Yahoo" (acronimo di "*Yet Another Hierarchical Officious Oracle*") è partito già nel 1994, quando la società venne fondata da Jerry Yang e David Filo, per essere registrata l'anno successivo nello stato del Delaware.

All'origine del progetto vi era un'idea tanto semplice quanto utile: la catalogazione dei *bookmarks* che i due studenti dell'Università di Stanford creavano ogni volta che individuavano un sito di loro interesse allora presente nel "world wide web"[79].

---

[77] YAHOO! INC, *ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934*
For the fiscal year ended December 31, 2016, "http://annualreports.com/Company/yahoo", ultima consultazione 21.09.2019.

[78] U.S. SECURITY AND EXCHANGE COMMISSION, *The Laws That Govern the Securities Industry, Fast Answers*, "https://www.sec.gov/answers/about-lawsshtml.html", ultima consultazione 21.09.2019.

[79] Andrew CLARK, *How Jerry's guide to the world wide web became Yahoo*, "The Guardian", 18.02.2001, ultima consultazione 21.09.2019.

Difatti, la società nasce come la "*Jerry and David's Guide to the World Wide Web*", un sito sul quale venivano raccolti e catalogati i link di accesso agli altri siti della rete, un sito che ne rendeva più semplice l'individuazione attraverso la suddivisione in tipologie[80].

La funzionalità e l'utilità di un simile strumento fu subito chiara a tutti gli internauti: dapprima a beneficiarne furono solo gli altri studenti della Standford University; quell'esiguo numero, in ogni caso, era destinato a crescere in misura esponenziale nel giro di pochi anni.

L'elevato numero di visitatori raggiunti, assieme ai servizi che vennero di anno in anno implementati, ha posto inevitabilmente il problema del trattamento dei dati personali.

In particolare, solo la profilazione dei propri utenti ha, infine, permesso da un lato, a Yahoo, di personalizzare l'esperienza di navigazione e l'offerta di servizi perfettamente ritagliati in base alle esigente dell'utente e / o consumatore, dall'altro lato, agli "*Advertisers*", di segmentizzare gli utenti e definire il preciso"*target*" di riferimento cui rivolgersi.

4.3. La struttura organizzativa e del personale in Yahoo Inc. e in Verizon Communications Inc.

Yahoo Inc, fondata nel 1994 da David Filo e Jerry Yang, all'epoca studenti di Stanford, rappresenta un caso per certi versi singolare. In essa sono state poste in essere diverse strategie, eppure con il passare degli anni i problemi non sono stati pochi. Da quando Terry Semel si è dimesso da CEO nel 2007, Carol Bartz è venuto a sostituire la sua posizione, senza tuttavia, migliorare la situazione. Nel 3° trimestre del 2010, Yahoo Inc ha rinunciato in gran parte alla propria tecnologia di ricerca e al proprio sistema di annunci, esternalizzandolo a Microsoft.

La società ha firmato un accordo per pagare a Microsoft il 12% delle sue entrate nette nella ricerca. Il problema in questo caso era che Yahoo aveva sperimentato il sistema pubblicitario, ma piuttosto tardi dopo la firma dell'accordo. Di conseguenza, il sistema non ha funzionato e questo ha accelerato il declino anno dopo anno.

Un altro piano è stato elaborato da Scott Thompson, che è stato assunto come CEO di Yahoo nel gennaio 2012. Il suo piano era quello di concentrarsi sul *core* di Yahoo e riorganizzare la società per evitare distrazioni. Ciò, tuttavia, non ha salvato la società dalla crisi poiché anche Thompson non aveva una visione chiara di ciò che doveva essere fatto in Yahoo.

Nel 2007, Yahoo ha cercato di potenziare il proprio business per competere con altri concorrenti forti, come Facebook, Twitter. Stato acquistato Flickr; tuttavia, la compagnia non è riuscita ad evolvere il

[80] *Ibidem.*

proprio modello di business rispetto ai concorrenti. In breve, a Yahoo sono mancate innovazione e creatività[81].

Sul piano del personale, Yahoo ha molteplici volte effettuato operazioni di ristrutturazione interna. La ricetta è stata sempre la stessa: ridurre i costi attraverso una contrazione consistente nel numero di dipendenti, con tagli fino al 15% dell'organico a livello mondiale, anno dopo anno.

Ora Yahoo fa parte di Verizon e la struttura organizzativa utilizzata è sostanzialmente la stessa di molte altre società tecnologiche. In essa troviamo il direttore generale nel livello superiore, che fornisce la visione e la direzione per l'organizzazione, con una composizione di dirigenti di livello C: CMO, CFO, CTO, COO, ecc. Sotto questi dirigenti di livello C, vi è chi esegue le funzioni più specifiche per l'azienda, come gestione delle vendite, marketing, sviluppo del prodotto, piattaforme, tecnologia interna.

Verizon Communications Inc. è una *holding company*, ad oggi tra i leader nel settore della fornitura dei servizi di comunicazione a banda larga, con una stabile presenza in almeno 150 paesi in tutto il mondo, e collocata, nel 2013, al primo posto tra le migliori imprese in cui lavorare per manager di nazionalità differenti, in base alla classifica stilata dal *Diversity MBA Magazine* del 2013[82].

L'acquisizione di Yahoo è stata annunciata nel 2016, con l'obiettivo dichiarato di acquisire un capitale di 1.3 miliardi di utenti, e rafforzare, in virtù di tale acquisizione, la propria posizione dominante in termini di *digital advertising*[83].

Verizon Communications Inc., dopo aver acquisito Yahoo Inc., ha annunciato una nuova struttura operativa focalizzata su tre aree rivolte ai clienti: Consumer, Business e Verizon Media Group/Oath. La società ha previsto che i gruppi saranno supportati da una rete e da un'organizzazione IT e da funzioni di personale a livello aziendale. Le modifiche sono entrate in vigore il 1° gennaio 2019. Verizon aveva previsto, inoltre, di passare alla rendicontazione finanziaria nell'ambito della nuova struttura durante il secondo trimestre 2019.

Verizon Consumer Group includerà il segmento consumer sia per le attività wireless che per quelle cablate, compreso il wireless all'ingrosso. Sarà guidato da Ronan Dunne, attualmente vice presidente esecutivo e presidente di Verizon Wireless.

Verizon Business Group includerà le imprese wireless e wireline, le piccole e medie imprese e le amministrazioni pubbliche, nonché le reti wireline all'ingrosso e Verizon Connect, il settore telematico dell'azienda. Sarà guidato da Tami Erwin, attualmente vice presidente esecutivo - Wireless Operations.

---

[81] Cfr. https://illiabusiness.wordpress.com/2013/09/22/yahoo-inc-significant-post-crisis-changes-in-organizational-structure/

[82] Classifica consultabile sul sito https://diversitymbamagazine.com.

[83] VERIZON, Annual report 2016, p. 7.

Verizon Media Group/Oath si trova all'intersezione tra media, pubblicità e tecnologia, aiutando le persone ad accedere e ricevere media, intrattenimento, giochi, notizie, commercio e altri servizi. Sarà guidato da Guru Gowrappan, precedentemente annunciato come CEO di Oath.

L'organizzazione Global Network & Technology di Verizon, che servirà a tutte le operazioni dell'azienda, sarà guidata da Kyle Malady, attualmente direttore delle operazioni di rete e responsabile della tecnologia. Non ci sono stati, invece, mutamenti nella leadership per le funzioni del personale a livello aziendale[84].

Tra i principali punti di forza di Verizon, significativa è la sua capacità in termini di capitali e in termini di competenze tecniche nella transazione del mercato delle comunizioni dalla tecnologia 4G a quella 5G.

A tale scopo, numerosi "*5G labs*" sono stati fondati nel tempo, per permettere agli ingegneri di Verizon di esplorare le potenzialità della "*5G technology*", nonché preparare gli stessi ad affrontare le nuove sfide che ne deriveranno nella prospettiva della *cyber-security*[85].

Anche la tutela della *privacy* delle "*customers'information*" passerà dalla sicurezza dei sistemi sui quali poggeranno tutte le attività di Verizon, e sulle misure tecniche ed organizzative a tal fine implementate.

A riprova di quanto detto, la società ha dichiarato, nell'Annual Reort del 2018, uno sforzo costante al fine della implementazione di "*security services*" orientati a mitigare, monitorare e gestire i rischi legati ai *cyber-attacks*.

Infatti, tra le sfide che oggi appaiono mettere più in difficoltà gli attuali operatori del mercato vi è proprio la capacità di sviluppare e mantenere un solido *s*istema di gestione integrato delle informazioni e dei meta dati, soprattutto se si considera l'ingente numero di dati (personali, oltre che digitali) che verranno prodotti attraverso l'uso del 5G.

4.4. Il primo *data breach*

La prima violazione di dati personali ad essere registrata a danno di Yhaoo risale al 2010, nonostante i principali *data breach* ad essere ricordati siano quelli del 2013 e del 2014, in ragione delle dimensioni assunte in termini di volume di dati personali oggetto della violazione e di interessati coinvolti.

Ad ogni modo, prima ancora che sotto questi profili, l'attacco del 2010 rileva per il numero di società che ne furono vittime: venne sferrato, infatti, non già avverso una singola compagnia, bensì contro

[84] Cfr. https://markets.businessinsider.com/news/stocks/verizon-realigns-organization-structure.
[85] VERIZON, Annual report 2018, p. 10.

un consistente numero di società operanti nel mondo IT, alcuni dei soggetti meglio rappresentativi di tutto l'universo della *Silicon Valley*, tra gli altri anche Google[86].

In particolare, il 12 gennaio di quell'anno, l'attacco venne annunciato dalla stessa Google.

Secondo le prime informazioni diffuse la settimana successiva all'attacco furono addirittura una ventina le società che si fecero trovare impreparate ad affrontare quello che è stato ricostruito come un attacco hacker interamente programmato e supportato dall'allora Governo Cinese, verosimilmente diretto ad acquisire e-mail e codici appartenenti ad attivisti cinesi per i diritti umani[87].

Tuttavia, seppure l'origine dell'attacco venne inizialmente ricondotta ad alcuni computer ubicati presso due istituti di ricerca cinesi[88], uno dei quali diretto da corpi militari[89], le successive indagini sono state in grado di ricollegare l'attacco esclusivamente ad alcuni server situati in Taiwan[90].

Quale ne sia stata l'origine, si è trattato di un attacco particolarmente sofisticato: oltre alla tradizionale tecnica del *phishing*, sono state sfruttate delle vulnerabilità tecniche a livello *software* che hanno permesso di assumere il controllo da remoto degli elaboratori coinvolti nell'attacco[91].

Ad ogni modo, sebbene permanga un fitto velo di nebbia su una vicenda di cui ancora oggi non riescono a definirsi in maniera esaustiva ed incontestabile tutti i dettagli, appare, al contrario, piuttosto evidente il risultato che ne scaturì: l'inevitabile consapevolezza, maturata nelle società vittime dell'attacco, circa la necessità di adottare virtuose politiche e procedure interne, teleologicamente orientate a contrastare il *cybercrime*[92].

A tal proposito, il portavoce di Yahoo, subito dopo la diffusione della notizia dell'attacco, dichiarò: "Yahoo di regola non rende pubbliche questo tipo di informazioni, in ogni caso la Compagnia prende molto seriamente il problema della sicurezza, e assume azioni adeguate al singolo caso di *data breach*"[93].

Quanto affermato pone immediatamente due questioni: l'una, la sussistenza di precisi obblighi di informazione, a favore degli utenti / interessati, in capo agli attori del mercato IT, in occasione della compromissione della riservatezza, integrità, disponibilità dei dati personali trattati; l'altra, il divieto di porre in essere pratiche commerciali scorrette ed ingannevoli.

---

[86] Ivi, pag. 1265.

[87] Cfr. A. Jacobs, M. Helft, *Google Citing Attack, Threatens To Exit China*, "The New York Times", 12.01.2010, ultima consultazione 19.08.2019.

[88] Il primo la "*Shanghai Jiatong University*", il secondo la "*Lanxiang Vocational School*" istituita con il supporto dell'esercito cinese.

[89] Cfr. J. Markoff e D. Barboza, *2 China Schools Said to Be Tied to Online Attacks*, "The New York Time", 18.02.2010.

[90] *Ibidem*.

[91] A. Jacobs, M. Helft, op. cit.

[92] Lawrence J. Trautmat e Peter C. Ormerod, op. cit., pag. 1265.

[93] Versione in lingua originale: "*Yahoo does not generally disclosethat type of information, butwe take security very seriously and we take appropriate action in the event of any kind of breach*". Jack SCHOFIELD, *Google, Yahoo, Adobe and who?*, "The Gurdian", 14.01.2010.

Ad essere essenziale, cioè, è la necessaria coerenza tra quanto pubblicamente annunciato da un lato, e quanto concretamente fatto in termini di azioni concrete per garantire la sicurezza dei dati personali dall'altro: in un'ottica di massima trasparenza, quanto comunicato all'esterno deve corrispondere a quanto realizzato all'interno dell'organizzazione.

La prima questione trova la sua soluzione nel dettato normativo.

Sebbene gli Stati Uniti d'America abbiano dimostrato un approccio estremamente liberale anche con riferimento al tema *privacy*, e non si siano dotati di una norma organica e completa al pari dell'Unione Europea[94], in ogni caso sul punto sono intervenuti:

i) il *Federal Trade Commission Act*, che, indirettamente, riconosce, e condanna, quale pratica commerciale scorretta ed ingannevole il mancato rispetto dell'obbligo di garantire agli utenti / consumatori adeguate informazioni riguardo la sicurezza dei propri dati personali[95];

ii) la *Security and Exchanges Commission's Corporate Finance Disclosure Guidance*, che prevede l'obbligo di comunicare a tutti gli investitori l'eventuale *data breach* subito di cui la compagnia sia venuta a conoscenza, e ciò per soddisfare evidenti fini di tutela dell'interesse patrimoniale degli *stakeholders*[96].

La seconda questione sarà oggetto di discussione nel paragrafo che segue.

4.5. Le misure tecniche ed organizzative seguite al *data breach* del 2010

Nei giorni che seguirono alla diffusione delle informazioni relative all'attacco del 2010, sia Google sia Yahoo riconobbero, a ragione, il tema della *cyber-security* come un'assoluta priorità, senonché, dall'analisi degli eventi accaduti negli anni immediatamente successivi, appare quantomai evidente come Yahoo, nei fatti, non abbia mai accompagnato le sue dichiarazioni pubbliche con azioni concrete, inequivocabilmente rivolte verso la direzione in astratto indicata[97].

Giunge a supporto di siffatte considerazioni il confronto, riportato di seguito, tra quanto messo in atto dai due principali attori, storicamente contrapposti, del mercato americano dei servizi digitali: Yahoo da un lato, Google dall'altro.

Tuttavia, prima di procedere ad una breve analisi delle misure tecniche ed organizzative adottate a seguito del *data breach* del 2010, a questo punto è opportuno fissare una breve premessa.

---

[94] Resta da considerare che nell'analisi delle normative in vigore sul territorio americano potrebbe includersi, senza timore, anche il GDPR, nei limiti di cui all'art. 3, par., lett. a) e b) dello stesso Regolamento.

[95] Lawrence J. Trautmat e Peter C. Ormerod, op. cit., pag. 1237.

[96] *Ibidem*.

[97] Cfr. N. Perlroth, V. Goel, *Defending Against Hackers Took a Back Seat at Yahoo, Insiders Says*, "The New York Times", 28.09.2016, ultima consultazione 19.08.2019.

Infatti, occorre, innanzitutto, evidenziare come le *policy / procedure* adottate da Google già prima del 2010 abbiano permesso alla stessa oltre che di monitorare il *work flow* dei dati personali trattati, altresì di riconoscere tempestivamente la violazione di dati personali subita.

Pertanto, nonostante la vulnerabilità dimostrata, Google è stata in grado di venire a conoscenza dell'attacco ed individuarne l'origine: degli hackers cinesi che hanno sfruttato una falla presente in una vecchia versione di Internet Explorer; l'obiettivo: ottenere l'accesso al network interno della società, attraverso l'esecuzione di codice da remoto[98].

Terminata questa breve premessa, è possibile procedere con l'analisi di quanto avvenuto dopo l'attacco del 2010 sul piano sia dell'organizzazione interna delle due società, sia delle misure tecniche di cui è stata proposta ed approvata l'implementazione.

Innanzitutto, pare doveroso riconoscere lo sforzo sopportato da Google a seguito del 2010, in coerenza con quello che divenne il nuovo motto della società, "*Never again*"[99]:

i) venne implementata una Infrastruttura di gestione dei dati interna, adeguata e resiliente, allo scopo di impedire il verificarsi di una nuova intrusione da parte di soggetti non autorizzati negli *accounts* dei propri utenti, quanto al piano delle misure tecniche ed organizzative;

ii) altresì, furono assunti centinaia di ingegneri con competenze specialistiche in materia di *cybersecurity* nell'ottica del rafforzamento dell'organizzazione interna[100];

Altrettanto convincente non fu la risposta di Yahoo: al virtuosismo di Google si è opposta, infatti, la scarsa sensibilità dimostrata, nei fatti, dall'allora *Chief Executive Officer* (CEO) di Yahoo, Merissa Mayer, in netta discrasia con quanto pubblicamente professato[101].

Un'importante prova a dimostrazione di quanto affermato, tra le altre, il fatto che Yahoo abbia cominciato a destinare dei fondi per ottenere informazioni circa le vulnerabilità dei propri sistemi direttamente dagli "hacker" solo tre anni dopo Google, ossia solo nel 2012[102] - tale attività viene definita con l'espressione "*Ethical hacking*".

In ogni caso, la corretta gestione della sicurezza in maniera metodica e strutturata non può prescindere dal considerare quale primo *step* di base un'adeguata analisi del livello di protezione di partenza, strumentale ad ottenere un'istantanea affidabile ed immediata della situazione "*as is*", ed altrettanto funzionale a programmare le fasi di "*to do*".

---

[98] Cfr. B. Johnson, *Chinese hackers used Microsoft broswer to launch Google strike*, "The Guardian", 14.01.2010.
[99] N. Perlroth, V. Goel, op. cit.
[100] *Ibidem*.
[101] Lawrence J. Trautmat e Peter C. Ormerod, op. cit., pag. 1265.
[102] N. Perlroth, V. Goel, op. cit.

A tal fine, strumento insostituibile risulta l'insieme delle attività e degli strumenti che si collocano nell'ambito del "V.A. / P.T.", ovvero: *Vulnerability Assessment / Penetration Test*[103].

La valutazione delle vulnerabilità ed i test di penetrazione sono riconducibili a quella serie di misure tecniche di base la cui implementazione risulta necessaria *ex lege*[104], come anche per ottenere certificazioni internazionali quali la certificazione ISO 27001.

L'obiettivo di tale attività: accertare che l'organizzazione sia in possesso di un'infrastruttura per la gestione dei dati personali in grado di garantire una certa resistenza e resilienza agli attacchi esterni cui è esposta, anche a tutela dello stesso patrimonio informativo immateriale della società, che potrebbe essere compromesso a seguito di un attacco sferrato con successo.

In dettaglio, l'attività di V.A. identifica, quantifica, nonché classifica per indice di rischio le vulnerabilità note e quelle individuate *ex novo*, tra le quali, ad es., software non aggiornato, misconfigurazione degli applicativi del sistema, utilizzo di *default password*[105].

In seguito, le vulnerabilità così individuate vengono sfruttate dall'operatore che procede al P.T., per simulare scenari di attacco complessi attraverso strumenti automatizzati.

Ad ogni modo, non può trattarsi di un'attività "*spot*", al contrario la stessa deve fondarsi su una programmazione periodica, che ne garantisca il regolare svolgimento: le V.A. / P.T. devono collocarsi, cioè, all'interno di un processo di "*Vulnerability management*"[106], la cui predisposizione è competenza del *Security Officer*.

Secondo la norma ISO / IEC 27002 "*tali attività dovrebbero essere pianificate, documentabili e ripetibili*".

L'espletamento di una simile attività con cadenza regolare assicura che siano tempestivamente individuate ed affrontate le vulnerabilità rese note, di volta in volta, quale risultato dei vari *assessment* portati a termine.

L'adozione di specifiche procedure interne per la protezione dei dati personali viene indicata dall'Enisa quale la prima delle misure tecniche / organizzative che l'organizzazione dovrebbe implementare: documentare i metodi di espletamento delle attività svolte in materia di *privacy* si

---

[103] EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY, *ENISA Threat Landscape Report 2016*
15 Top Cyber-Threats and Trends, 2016, pag. 65.

[104] La prima norma a fare riferimento a tali strumenti è stata l'ormai abrogato DECRETO DEL PRESIDENTE DELLA REPUBBLICA del 28 luglio 1999, n.318: "Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675", che all'art. 4, comma 1, lett. c) prevede, alla lettera, che: "*gli elaboratori devono essere protetti contro il rischio di intrusione ad opera di programmi di cui all'art. 615-quinquies del codice penale, mediante idonei programmi, la cui efficacia ed aggiornamento sono verificati con cadenza almeno semestrale*".

[105] ENISA, *ENISA Threat Landscape Report 2016*, cit., pag. 19 ss.

[106] "*Vulnerability Management*" è il termine con cui si indica il processo, con l'espressione "*Vulnerability Scanning*" si indica, invece, la singola attività in sé per sé considerata.

pone, infatti, come *step* essenziale nell'ottica della tutela dai dati personali, la base sulla quale fare poggiare tutte le successive misure[107].

In ogni caso, le strategie adottate da Yahoo dopo il 2010 si sono dimostrate particolarmente carenti, e non già avuto esclusivamente riguardo al profilo delle "misure organizzative", bensì anche considerando l'ulteriore profilo delle misure propriamente tecniche che chi tratta i dati personali è chiamato ad implementare; un esempio: meno del 5% degli *account* violati era protetto da una *password* valida[108].

A riguardo, l'implementazione *by design* di un meccanismo di autenticazione in grado di rilevare e non consentire l'utilizzo di password che non rispettino un certo livello di complessità si colloca tra le principali misure tecniche che ad oggi possono ricondursi all'art. 32 del GDPR, nella direzione di assicurare un efficace controllo degli accessi.

Non mancano ulteriori esempi di misure tecniche da considerare essenziali nell'ottica della sicurezza dei dati personali, rispetto alle quali, tuttavia, il Management board di Yahoo si è espresso in senso negativo, le principali:

i) il sistema di cifratura *End to end* dell'intera infrastruttura digitale di Yahoo, osteggiato poiché avrebbe impedito l'accesso ai contenuti delle comunicazioni che venivano inviate tra gli utenti - pertanto, da ciò sarebbe derivata l'incapacità della stessa Yahoo di indicizzare ed individuare le informazioni acquisibili da tali messaggi, per ritagliare, in base alle esigenze espresse dagli utenti, i nuovi servizi ad essi offerti[109];

ii) l'implementazione di un sistema interno di tipo proattivo capace di individuare gli attacchi alla sicurezza dei dati personali, ovvero un meccanismo di *Intrusion-detection*[110] al fine di contenere i costi legati alla *cyber-security.*

A riguardo, se il controllo dei pacchetti di dati in transito da e verso la rete avviene ad opera del *firewall*, è solo attraverso i sistemi di reportistica quale il sistema di rilevamento delle intrusioni (*IDS, intrusion detection system*) che è possibile provvedere al controllo approfondito dei pacchetti: l'IDS è un *tool* strumentale alla generazione di *warning* ogni qualvolta è analizzato traffico potenzialmente malevolo[111].

Altresì, laddove lo stesso dispositivo sia in grado non già esclusivamente di produrre degli allarmi, bensì anche di filtrare autonomamente il traffico sospetto, in tal caso si parla di sistemi di prevenzione

---

[107] ENISA, Manuale, cit., pag. 62.
[108] Cfr. Doug GROSS, *Yahoo hacked, 450,000 passwords posted online*, "CNN Business", 13.07.2012.
[109] Lawrence J. Trautmat e Peter C. Ormerod, op. cit., pag. 1266.
[110] *Ibidem*.
[111] Cfr. James F. Kurose, Keith W., *Reti di calcolatori e internet*, Milano-Torino, Pearson, 2013, sesta edizione, p. 683 e ss.

delle intrusioni (*IPS, intrusion prevention system*)[112], e non già esclusivamente di *tool* che necessitano il coinvolgimento dell'operatore;

iii) infine, *the last but not the least*, la *CEO* di Yahoo si oppose al *reset* automatico di tutte le password degli utenti interessati dal *data breach*[113].

Tale misura, considerata e presentata dagli ingegneri di Yahoo quale misura base ed essenziale a tutela della sicurezza dei dati personali, secondo la Mayer avrebbe spinto molti utenti a rinunciare al proprio *Yahoo's account*, e a rivolgersi agli altri *competitors* sul mercato digitale[114].

Di talché, come detto, ne venne impedita l'adozione.

A valle di quanto detto fin ora, è facile comprendere le ragioni delle dimissioni di Mr. Stamo, ex *Chief Information Secutiry Officer* (CISO) di Yahoo, rassegnate solo un anno dopo la sua assunzione, in quanto in perenne contrasto con il Management board, in particolare il Vice-Presidente Bonforte.

La figura di Bonforte è piuttosto centrale nell'economia della vicenda, tanto quanto quella di Marissa Mayer.

Il risultato: la compagnia americana ha pagato più volte il prezzo della perenne vulnerabilità cui è stata condannata a causa delle scelte del proprio Management board.

4.6. Il secondo *data breach*

In un'immaginaria classifica delle violazioni di dati personali che si sono succedute nella storia della rete, il *data breach* del 2013 rimane, ad oggi, quello che ha fatto segnare il più alto record in termini di numero di interessati coinvolti: 1 miliardo di utenti[115].

Disparate sono state le tipologie di dati personali degli interessati oggetto della violazione: i nomi, i numeri di telefono, le date di nascita, le passwords nonché, infine, le "*security questions*", non sottoposte a cifratura[116].

A riguardo, il rischio maggiore paventato dalla stessa Yahoo era rappresentato dalla possibilità che tali domande di sicurezza potessero essere facilmente utilizzate per modificare le password personali degli utenti[117].

[112] *Ibidem*.
[113] Lawrence J. Trautmat e Peter C. Ormerod, op. cit., p. 1267.
[114] Ivi, pag. 1266.
[115] Ivi, pag. 1237.
[116] *Ibidem*.
[117] Cfr. V. Goel, E. Lichtblau, *Yahoo Says 1 Billion User Accounts Were Hacked*, "The New York Times", 14.12.2016, ultima consultazione 12.08.2019.

In ogni caso, è stato escluso con certezza l'accesso a password non criptate, dati delle carte di pagamento degli utenti o più in generale informazioni relative ai conti correnti bancari aperti dagli utenti[118].

L'attacco, infine, venne ricondotto ad un non meglio precisato "*state-sponsored hacker*"[119].

4.7. Il terzo *data breach*

Se l'attacco del 2013 ha dimostrato quanto vasti possano essere gli effetti di un unico *data breach*, quello del 2014 ha dimostrato come la mancata assunzione di misure tecniche e organizzative adeguate determini una perenne esposizione agli attacchi.

Difatti, nel 2014 Yahoo ha subito una terza violazione di dati personali, che ha coinvolto 500 milioni di utenti.

Tra i dati personali ai quali gli *hacker* hanno avuto illecitamente accesso si contano i nomi, il giorno di nascita, il numero di telefono, l'indirizzo email, la password criptata (hashed password), le domande di sicurezza, sia criptate sia non criptate degli utenti.

Nel 2017, il Dipartimento di Giustizia Americano ha indiziato, per questo attacco, due membri dell'intelligence russa[120].

Secondo gli esperti, gli hacker hanno avuto accesso al codice sorgente di proprietà di Yahoo, ed hanno realizzato delle copie dei dati personali degli utenti contenuti nei *data base* di proprietà della compagnia americana[121].

4.8. Le misure tecniche organizzative implementate / non implementate

Una volta tratteggiati brevemente i contorni degli attacchi del 2013 e del 2014, è possibile concentrarsi sull'analisi dettagliata delle misure tecniche ed organizzative adottate, nonché delle misure che la compagnia avrebbe potuto implementare, cui ha, invece, deciso di rinunciare.

È bene precisare e rimarcare che l'adozione di siffatte misure si configura, in ogni caso, nei termini di un generico obbligo di legge, formalmente previsto dal *Federal Trade Commission Act*.

Secondo quanto previsto da tale norma, infatti, misure di sicurezza ragionevoli ed appropriate, sia fisiche, sia tecniche, sia amministrative devono essere implementate al fine di garantire l'integrità, la riservatezza e la disponibilità dei dati personali.

---

[118] Lawrence J. Trautmat e Peter C. Ormerod, op. cit., pag. 1233.
[119] *Ibidem*.
[120] Cfr. V. Goel, E. Lichtblau, *Russian Agents Were Behind the Yahoo Hack, U.S. Says*, "The New York Times", 15.03.2017, ultima consultazione 31.07.2019.
[121] Lawrence J. Trautmat e Peter C. Ormerod, op. cit., pag. 1270.

Il modello di riferimento dalla FTC è lo *standard* fissato dal WISP, ovvero il *Written Information Security Plan*, un approccio ormai consolidato, una procedura che comprende ed è riassumibile in quattro *step* essenziali:

i) l'individuazione del rischio;

ii) l'analisi del rischio;

iii) la predisposizione di misure adeguate al livello di rischio presentato dal singolo caso concreto;

iv) un'*assessment* della efficacia dimostrata da tali misure[122].

4.9. Le misure adottate

La compagnia IT americana non è arrivata completamente impreparata alla prova dei *data breach* del 2013 e del 2014: verranno illustrate di seguito alcune misure tecniche implementate dalla società americana già prima di subire i due attacchi.

Innanzitutto, essenziale si è rivelato in entrambi gli attacchi il "*passwords hashing*": in virtù della "funzione di Hash", ai valori inseriti ad ogni accesso dall'utente quale chiave di sicurezza per accedere al proprio account vengono applicati algoritmi teoricamente irreversibili, che, a parità di condizioni iniziali, sono in grado di produrre quale risultato sempre la stessa sequenza di cifre e lettere.

La paternità dell'algoritmo *Secure Hash Algorithm* (SHA) è riconosciuta al *National Institute of Standard and Technology* (NIST), che nel 1993 ha dunque implementato quello che, ancora oggi, risulta essere uno dei fondamenti della crittografia moderna[123].

Tale funzione è computazionalmente efficiente, considerate le risorse e il tempo richiesti per l'esecuzione delle operazioni: una volta eseguita, il risultato è il *mapping* di una stringa di dimensioni casuali in una nuova stringa di dimensione fissata[124].

Di talché, ad essere registrata nei data base di Yahoo, per essere poi processata dai sistemi gestionali di autenticazione, non è la password in chiaro inserita di volta in volta dall'utente prima di effettuare l'accesso al proprio account, bensì quella cifrata, ovvero l'*hashed password*, una sequenza dalla quale, tuttavia, non è possibile risalire alla stringa originaria.

Questo processo, pertanto, assicura un duplice vantaggio: ogni volta che l'utente inserisce la stessa password il sistema produce lo stesso risultato (e la stringa prodotta è sempre riconosciuta dal sistema); al contempo, nel caso in cui un soggetto non autorizzato abbia accesso ai DB contenenti le

[122] Ivi, pag. 1243 e pag. 1280.
[123] Cfr. W. Stallings (a cura di) L. Salgarelli, *Crittografia e sicurezza delle reti*, Mc-Graw Hill, 2° edizione, 2013, pag. 370.
[124] Cfr. Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vastone, *Handbook of applied cryptography*, 1996, pag. 33.

hashed password, questo non potrebbe risalire alla password concretamente utilizzata dall'utente ad ogni accesso.

Parimenti, sono state sottoposte al processo di cifratura anche parte delle *security questions* che gli utenti possono selezionate in caso di smarrimento della password.

Mentre, per tutte le domande di sicurezza registrate in chiaro e oggetto del *data breach*, la stessa Yahoo ha provveduto a renderle invalide, assieme all'invito a modificare la propria password personale rivolto a tutti gli utenti i cui account erano stati coinvolti dall'attacco del 2013[125].

Infine, in base alle dichiarazioni rilasciate dalla società, i fondi destinati a rafforzare l'organizzazione interna, e in particolare il ramo dedicato alla sicurezza informatica, videro un incremento del 60 % nel periodo tra il 2015 e il 2016[126].

4.10. Le misure "adeguate" non implementate

Nonostante gli sforzi profusi, le misure tecniche e organizzative implementate dalla società, tuttavia, non sono mai risultate pienamente convincenti agli occhi dei commentatori.

Ben Johnson, *co-founder* e *chief security strategist* presso "*Carbon Black*", una compagnia specializzata sul tema della sicurezza informatica, intervistato dal New York Times ha affermato che "*Typically companies get compromised multiple times due to the same vulnerability or employee culture*": il fatto che a distanza di un anno sia stata sfruttata la stessa vulnerabilità tradisce il contegno piuttosto negligente imputabile alla società[127].

Sotto il profilo prettamente tecnico, a riprova di quanto affermato fin ora, risulta, innanzitutto, sintomatica l'assenza di un sistema di crittografia end-to-end.

Attraverso il sistema di crittografia end-to-end il terminale di origine, o sorgente, esegue la crittografia dei dati che verranno trasmessi all'*host* o terminale di destinazione. Con il terminale di destinazione viene condivisa la chiave necessaria a decrittare i dati inviati dal terminale sorgente.[128].

Infine, per rendere sicuro tutto il traffico dei dati, su tutti i collegamenti sarebbe opportuno, poi, utilizzare, contestualmente al sistema di crittografia end-to-end il sistema di crittografia di canale.

Con la crittografia di canale ciascun collegamento vulnerabile viene dotato a entrambe le estremità di un sistema di crittografia: il sistema di crittografia end-to-end non può cifrare l'intero pacchetto: è esclusa, ad es., l'intestazione; la crittografia di canale, invece, è strumentale alla cifratura della intestazione del medesimo pacchetto già cifrato con la crittografia end-to-end, per impedire che

[125] V. Goel, E. Lichtblau, *Yahoo Says 1 Billion User Accounts Were Hacked*, op. cit.
[126] Lawrence J. Trautmat e Peter C. Ormerod, op. cit., pag. 1268.
[127] V. Goel, E. Lichtblau, op. cit.
[128] W. Stallings, op. cit., pag. 212 e ss.

l'intercettazione dei pacchetti, ad es., possa rivelare i nodi in cui avviene il maggior scambio di dati della rete[129].

Ciò premesso, ne deriva che, non applicando al "*cleartext*" o "*plaintext*" un algoritmo di cifratura, non è possibile assicurare che il trattamento dei dati personali avvenga in modo sicuro.

Di talché, tale tipo di tecnologia, applicata alle unità / driver di archiviazione, riesce a garantire tanto la riservatezza del contenuto dei dati trattati quanto l'integrità degli stessi durante la trasmissione (evitando alterazioni dovute a cause fortuite o a manipolazioni); parimenti è assicurata la sicurezza operativa (a tale scopo divengono essenziali anche dispositivi operativi, come *firewall* e sistemi di rilevamento delle intrusioni)[130].

In aggiunta, un'ulteriore criticità rimarcata da Ben Johnson riguarda lo *storage* dei dati: l'estensione del *data breach* è direttamente proporzionale al volume e alle diverse tipologie di informazioni che vengono conservate nello stesso DB[131].

A tale proposito, misure tecniche volte ad assicurare la *privacy compliance*, pertinenti alla certificazione ISO 27001 e perfettamente conformi agli stessi principi ispiratori del GDPR, sono, da un lato la conservazione e la strutturazione dei soli dati pertinenti al trattamento e la suddivisione degli spazi logici di archiviazione, dall'altro lato la pseudonimizzazione dei dati archiviati.

In ogni caso, la riflessione circa l'adozione di tali misure non può prescindere da un'approfondita analisi del rischio (ADR), passaggio individuato quale fondamentale anche nel WISP. A riguardo, il legislatore europeo ha distinto più livelli di analisi: all'innalzarsi del livello di rischio si innalzano, proporzionalmente, le garanzie procedurali previste[132].

Solo attraverso l'ADR è possibile approfondire il contesto delle attività cui è connesso il trattamento dei dati, nonché l'impatto che può concretamente prodursi sui diritti e sulle libertà delle persone fisiche all'accadimento di una minaccia, di origine ambientale oppure di origine umana, che riesca ad incidere sulla sicurezza dei dati personali.

Parimenti, risulta palese l'inadeguatezza delle politiche e delle procedure aziendali interne a Yahoo destinate al monitoraggio, nonché alla produzione di report relativi ad eventuali *data breach*[133].

Preme, infine, rimarcare come il nodo centrale risulti l'assenza di un sistema interno che assolva una duplice funzione: da un lato la continua produzione di report sullo stato del *workflow* dei dati aziendali, e dall'altro, la trasmissione delle informazioni ai vertici aziendali, ovvero tutti i soggetti che partecipano al *decision making process*, e che dunque devono essere adeguatamente e

---

[129] *Ibidem*.
[130] James F. Kurose, Keith W., op. cit., pag. 625.
[131] V. Goel, E. Lichtblau, op. cit.
[132] M. G. Stanzione, *Il Regolamento europeo sulla privacy: origini e ambito di applicazione,* "Europa e diritto privato", IV (2016), pagg. 1263-1264.
[133] Lawrence J. Trautmat e Peter C. Ormerod, op. cit., pag. 1283.

tempestivamente informati, un sistema, in conclusione, che sia in grado di operare secondo un approccio di tipo *bottom-up*[134].

Tali procedure di gestione dei flussi di dati dovrebbero essere oggetto di approvazione da parte del management dell'azienda, resi accessibili a tutti i dipendenti e sottoposti a revisione con cadenza almeno semestrale laddove se ne ravveda l'occorrenza[135].

Ad essere richiesto è, pertanto, uno sforzo di tipo continuativo, e non meramente occasionale.

A riguardo, il contenuto minimo di tali *policy / procedure* interne dovrebbe comprendere alcuni elementi chiave, quale:

i) la definizione di una chiara catena delle responsabilità;

ii) la descrizione delle misure tecniche organizzative;

iii) un piano periodico delle attività di formazione da sottoporre a tutto il personale;

iv) un piano di gestione dei *personal data breach*.

Quanto a quest'ultimo punto, risulta fondamentale la definizione di una procedura della gestione degli incidenti di sicurezza e l'implementazione di sistemi gestionali a ciò dedicati. In particolare, non è sufficiente riconoscere tali eventi, bensì, i sistemi di reportistica adottati dall'azienda devono essere in grado di risalire alle cause, illecite o accidentali, delle violazioni di dati personali, al fine di individuare la natura dello stesso evento e selezionare le misure adeguate e proporzionate da adottare.

È evidente, anche sotto questo profilo, la carenza in termini di *Business Intelligence* dimostrata dalla società americana: i portavoce di Yahoo hanno affermato, infatti, di essere venuti a conoscenza del *data breach* del 2013 solo dopo aver analizzato alcuni file contenenti, secondo "*un-named third party*" del tutto sconosciuta, informazioni riferibili agli utenti che fruivano dei servizi offerti da Yahoo[136].

4.11. Analisi delle misure organizzative

In questo paragrafo si effettuerà una panoramica sull'evoluzione nel tempo dell'atteggiamento di Yahoo in termini di *privacy compliance*, attraverso l'analisi degli *Annual Report* prodotti da Yahoo a fini fiscali e delle misure organizzative inserite nei programmi di spesa.

Tale analisi si basa sulla consapevolezza che, al fine di garantire, da un lato, la tutela dei dati personali degli interessati, e dall'altro, di riflesso, la tutela del patrimonio economico nonché della *brand reputation* della società che tratta quei dati, è fondamentale accompagnare alle misure tecniche di cui

[134] Ivi, pag. 1247.
[135] ENISA, Manuale, cit., pag. 66.
[136] V. Goel, E. Lichtblau, op. cit.

si è discusso in precedenza altrettanto adeguate misure organizzative, tenuto conto, in ogni caso, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento.

In particolare, tra le principali misure organizzative volte a definire una chiara catena delle responsabilità vi è la strutturazione di un organigramma completo che contempli delle figure dedicate esclusivamente alla "*information security*".

Si analizzerà, pertanto, come tale evoluzione si sia tradotta anche in termini di organigramma aziendale ed a livello di *management board*, osservando e parimenti dimostrando, con l'aiuto delle due figure in calce al presente paragrafo, come nel tempo sia inevitabilmente aumentato il peso specifico della questione "*privacy*" anche all'interno di una società che non ha fatto certo della *data protection* il principio cardine di tutte le sue strategie d'impresa.

Dalla lettura del primo *Annual Report* del 1996, un dato risalta immediatamente agli occhi: non è presente alcun riferimento né al tema della riservatezza né al tema della protezione dei dati personali[137].

Lo stesso avviene l'anno successivo: tra le altre figure che compongono il *mangement board*, tuttavia, spicca il *Chief Technology Officer*, chiamato a valutare, selezionare e suggerire al consiglio direttivo e al *Chief Executive Officer* le tecnologie che possono essere applicate ai prodotti o ai servizi che un'azienda produce, una figura, tuttavia, prevalentemente di natura tecnica[138].

Solo nel 1998 la questione della protezione dei dati personali si vede per la prima volta riconosciuta a chiare lettere in sede di *Annual Report*, ma esclusivamente in termini di "*legal proceedings and claims*", dai quali possa derivare un danno economico patrimoniale considerevole per la società: tale approccio assimila il diritto alla *privacy* a tutti gli altri rischi d'impresa che il titolare è consapevole di assumere sulle proprie spalle una volta intrapresa l'attività – e ciò in ragione delle ingenti spese che potevano derivare da un'eventuale controversia giuridica in cui si dimostri il suo mancato rispetto da parte di Yahoo[139].

Ancora nel 2000 tra le figure che compongono il *management board* si distinguono: il "*Chief Financial Officer*", il "*Business Operations and Chief Sales and Marketing Officer*", il "*Communications Services, and Chief Technology Officer*", nonché una figura addetta al "*Commerce & Network Services*" ed una figura destinata alle "*International Operations*"[140].

---

[137] YAHOO! INC, 1996 *ANNUAL REPORT, Select Financial Data*, "http://annualreports.com/Company/yahoo", ultima consultazione 21.09.2019.

[138] YAHOO! INC, 1997 *ANNUAL REPORT, Select Financial Data*, "http://annualreports.com/Company/yahoo", ultima consultazione 21.09.2019.

[139] YAHOO! INC, 1998 *ANNUAL REPORT, Select Financial Data*, "http://annualreports.com/Company/yahoo", ultima consultazione 21.09.2019.

[140] YAHOO! INC, 2000 *ANNUAL REPORT, Select Financial Data*, "http://annualreports.com/Company/yahoo", ultima consultazione 21.09.2019.

L'invasione della *privacy*, dunque, non era considerata ancora una condotta da stigmatizzare. Parimenti, la protezione dei dati personali non costituiva ancora un diritto da proteggere, bensì semplicemente una tra i possibili fattori di rischio che potevano originare delle spese non programmate ed in grado di determinare una variazione nelle stime relative al *cash flow* della società.
A riguardo, è interessante notare come solo dal 2003 in poi si discorra di *privacy* in termini di "*privacy right*", dalla cui violazione può verosimilmente dipendere una "*substantial monetary liability*" in cui la società rischia di incorrere proprio a causa della violazione di quello che finalmente viene riconosciuto alla stregua di un diritto[141].
Altresì, nel medesimo Report annuale del 2003, viene riportata l'avvenuta implementazione di "*network security measures*" da rendere operative tanto al verificarsi di minacce che trovino la loro sorgente in fenomeni ed eventi catastrofici quali terremoti, inondazioni, eruzioni vulcaniche, fenomeni atmosferici, quanto al verificarsi di minacce di natura ambientale o tecnologica, le quali, sfruttando con successo le vulnerabilità del sistema, possono comportare un evidente rischio per i server ed i sistemi di Yahoo[142].
Ciò rinvia immediatamente a due misure organizzative fondamentali: tanto al *business continuity plan,* ovvero quel processo finalizzato ad assicurare la "*prevenzione e la gestione efficace di eventi critici mediante sistemi di prevenzione, strutture organizzative, regole operative e mezzi tra loro coerenti*", quanto al *disaster recovery plan*, ossia quel complesso di "*interventi organizzativi, tecnologici e logistici che consentono di ripristinare la continuità dei processi e delle infrastrutture aziendali resi non operanti o inaccessibili a seguito di eventi critici*"[143].
In particolare, proprio al fine di ridurre la possibilità di disastri che possano pregiudicare o in ogni modo inficiare il proprio *business*, Yahoo, tra le altre misure organizzative adottate, afferma di distribuire periodicamente i propri server in nuovi data centre sparsi in tutto il mondo.
Nell'*Annual Report* relativo al 2004[144] viene compiuto un ulteriore passo in avanti: emerge immediatamente la consapevolezza che anche a livello normativo la tutela della *privacy* sta diventando una necessità di tipo pressante; per la prima volta, infatti, si parla non già esclusivamente

[141] YAHOO! INC, *ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934*
For the fiscal year ended December 31, 2003, "http://annualreports.com/Company/yahoo", ultima consultazione 21.09.2019.
[142] *Ibidem*.
[143] ISTITUTO SUPERIORE DELLE COMUNICAZIONI E DELLE TECNOLOGIE DELL'INFORMAZIONE, *LA SICUREZZA DELLE RETI*
nelle infrastrutture critiche, p. 180 e ss.
[144] YAHOO! INC, *ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934*
For the fiscal year ended December 31, 2004, "http://annualreports.com/Company/yahoo", ultima consultazione 21.09.2019.

di *privacy* (come mero diritto alla riservatezza), bensì anche di *data protection*, nell'accezione di vera e propria tutela da garantire ai dati personali oggetto di trattamento.
A riguardo, si fa riferimento esplicito al *Children's Online Privacy Protection Act,* al *Federal Trade Commission Act*, e dunque alla sistematica emanazione di tutta una serie di norme aventi quale *communis ratio* la tutela dei dati personali.
A tale scopo, viene citata la pubblicazione delle *privacy policies* su tutte le pagine web facenti parte del dominio di Yahoo.
Difatti, se è vero che qualsiasi organizzazione che si trovi a gestire dati personali ho l'obbligo di trattare tali dati nella massima trasparenza, è al contempo innegabile il fatto che, per garantire tale trasparenza, è necessario (ma non sufficiente) informare gli interessati sulle modalità e i mezzi che caratterizzano il trattamento.
Di talché, la redazione e la redazione e la pubblicazione delle *privacy policy* e delle *policy procedure* sono riconosciute, ad oggi, come delle misure organizzative irrinunciabili per una società che intenda documentare:
- che il trattamento dei dati avviene nel rispetto pieno e puntuale del principio di trasparenza;
- l'esistenza di una chiara catena delle responsabilità;
- l'avvenuta adozione di misure tecniche ed organizzative adeguate al livello di rischio presentato dal singolo trattamento.
In particolare, ad oggi, i concetti di processo e di procedura sono strettamente correlati: per processo, in termini aziendali, deve intendersi quell'insieme di attività interdipendenti l'una dall'altra, teleologicamente orientate a produrre un output specifico a seguito di un determinato input. Le attività e le operazioni svolte nel processo, poi, seguono le regole stabilite nelle procedure.
Tali procedure, di regola, dovrebbero stabilire:
- regole chiare in materia di controllo degli accessi: gli utenti e / o i dipendenti possono avere accesso solo ai dati di cui necessitano realmente – ciò presuppone che l'architettura del sistema di accesso sia progettata *by design* in modo corrispondente;
- l'uso esclusivo di programmi e/o applicazioni formalmente autorizzati dall'azienda, e non già *software* prelevati da Internet o forniti da terze parti, ed in ogni caso non ulteriori rispetto a quelli richiesti dalle attività progettuali;
- l'utilizzo delle sole credenziali di autenticazione fornite dalla società;
- l'adozione di procedure di *change management* o di *log management* per avere sempre un'istantanea puntuale di tutte le variazioni apportate alle applicazioni in fase di sviluppo e in modo da poter tenere traccia degli accessi effettuati e delle azioni compiute da ogni operatore;
- la formazione e l'aggiornamento professionale continui di tutto il personale.

Le procedure più complesse, infine, possono prevedere veri e propri sistemi di gestione della sicurezza delle informazioni (SGSI o *ISMS – Information Security Management System*), e basarsi su standard internazionali quali la nuova ISO 27701, relativa all'"*information security management*". Si tratta di una serie di buone pratiche e standard a cui la società può decidere di adeguarsi su base volontaria, e che prevedono di *default* tutte quelle contromisure tecniche e organizzative la cui implementazione è opportuna al fine di prevenire e / o ridurre il rischio[145].

A riguardo, nel successivo report relativo al 2008, Yahoo riconosce che disattendendo le proprie *policy* - o compromettendo anche solo la percezione che gli utenti maturano circa il rispetto delle stesse da parte di Yahoo - ciò può comportare un importante danno all'immagine della società, che si tradurrebbe in una flessione del numero degli utenti e, in ultima istanza, del numero degli "*advertising partners*" e della mole di profitti generati grazie ad essi[146].

Per evitare tutto ciò sono implementate le "*network security measures*". Tuttavia, non esiste il "rischio zero": ad es., l'elevato numero di server sui quali sono ospitati i sistemi di Yahoo impedisce di assicurare una adeguata ridondanza degli stessi.

Ad ogni modo, affinché la tutela della *privacy* trovi spazio e venga declinata anche in termini di *management board*, dunque con la previsione di una figura specifica all'uopo nominata, bisognerà attendere il 2014: è questo il primo anno in cui viene individuato un *Chief Information Officer*, una figura apicale a capo di una sezione dell'azienda completamente dedicata alla gestione, organizzazione e strutturazione del *workflow* delle informazioni e dunque dei dati, la fonte da cui le informazioni promanano[147].

Parimenti, dello stesso anno è l'assunzione di Alex Stamos, nella funzione di "*Chief Information Security Officer*" (CISO) con l'obiettivo dichiarato di proseguire il percorso già intrapreso nella direzione della implementazione e programmazione di strategie volte a garantire la tutela dei dati personali degli utenti di Yahoo.

Nonostante le apparenze, la reale attitudine del *management board* nei confronti della questione *privacy* risulta dalla ferrea opposizione che la CEO Marissa Mayer ed il Vice-Presidente Bonforte opposero alle richieste di Stamos.

---

[145] Andrea TOMMASI, *Come proteggere le informazioni in azienda tra Cloud, costi e GDPR*, "Key4Biz", 17.09.2019, ultima consultazione 21.09.2019.

[146] YAHOO! INC, *ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934*
For the fiscal year ended December 31, 2008, "http://annualreports.com/Company/yahoo", ultima consultazione 21.09.2019.

[147] YAHOO! INC, *ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934*
For the fiscal year ended December 31, 2014, "http://annualreports.com/Company/yahoo", ultima consultazione 21.09.2019.

A riguardo, il *cybersecurity team*, posto alle dipendenze del CISO, ha assunto presto l'appellativo di "*Paranoids*", e le richieste del team si sono infrante più volte senza seguito contro il costo presentato dalle *privacy enhancing technologies* proposte di volta in volta.

Un tale atteggiamento produsse, come risultato fisiologico, l'esodo di molti ingegneri specializzati verso i principali competitors di Yahoo, quali, tra gli altri, i più importanti: Apple, come anche Facebook e Google.

Dimodoché, se già nel 2012 vennero adottati dei "*rigorous hiring protocols*" per garantire l'assunzione di nuovi talenti, ed in ogni caso esclusivamente di personale altamente specializzato, allo stesso tempo Yahoo si caratterizzava per una significativa carenza nella capacità attrattiva e di stabilizzazione dei rapporti di lavoro instaurati con il proprio personale[148].

Di talché, se da un lato la società poteva vantare una marcata rigidità in ingresso, dall'altro lato la stessa accusava un'inaccettabile emorragia di dipendenti che avevano maturato una significativa esperienza nel settore *infomration security*.

In conclusione, ciò che emerge da questa analisi è sicuramente l'ennesima prova a testimonianza dell'attitudine tutt'altro che virtuosa di Yahoo nei confronti della questione della tutela dei dati personali: la *privacy* veniva classificata dal *management board* esclusivamente nei termini di una verosimile minaccia alle casse societarie.

Riconoscere la cogenza del tema della protezione dei dati personali solo nella fase patologica sicuramente è un atteggiamento che non paga: l'adozione delle adeguate misure organizzative già nella fase fisiologica della progettazione e / o gestione del prodotto e / o servizio è un passaggio ineludibile, nonché strumentale, *in primis* ai fini della corretta gestione del *workflow* dei dati all'interno dell'azienda - ed è per tale ragione che essa deve essere riconosciuta come un'esigenza pressante già nel momento in cui il dato viene acquisito, e non, al contrario, durante la fase patologica, una volta che il danno è stato già cagionato – *deinde* per la tutela del patrimonio societario, sia informativo sia economico, sotto il profilo delle sanzioni amministrative evitate, come anche del valore aggiunto che il prodotto e / o il servizio che sia *privacy oriented* è in grado di esprimere sul mercato rispetto ai prodotti e / o servizi offerti dagli altri *competitors*.

[148] YAHOO! INC, *ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934*
For the fiscal year ended December 31, 2012, "http://annualreports.com/Company/yahoo", ultima consultazione 21.09.2019.

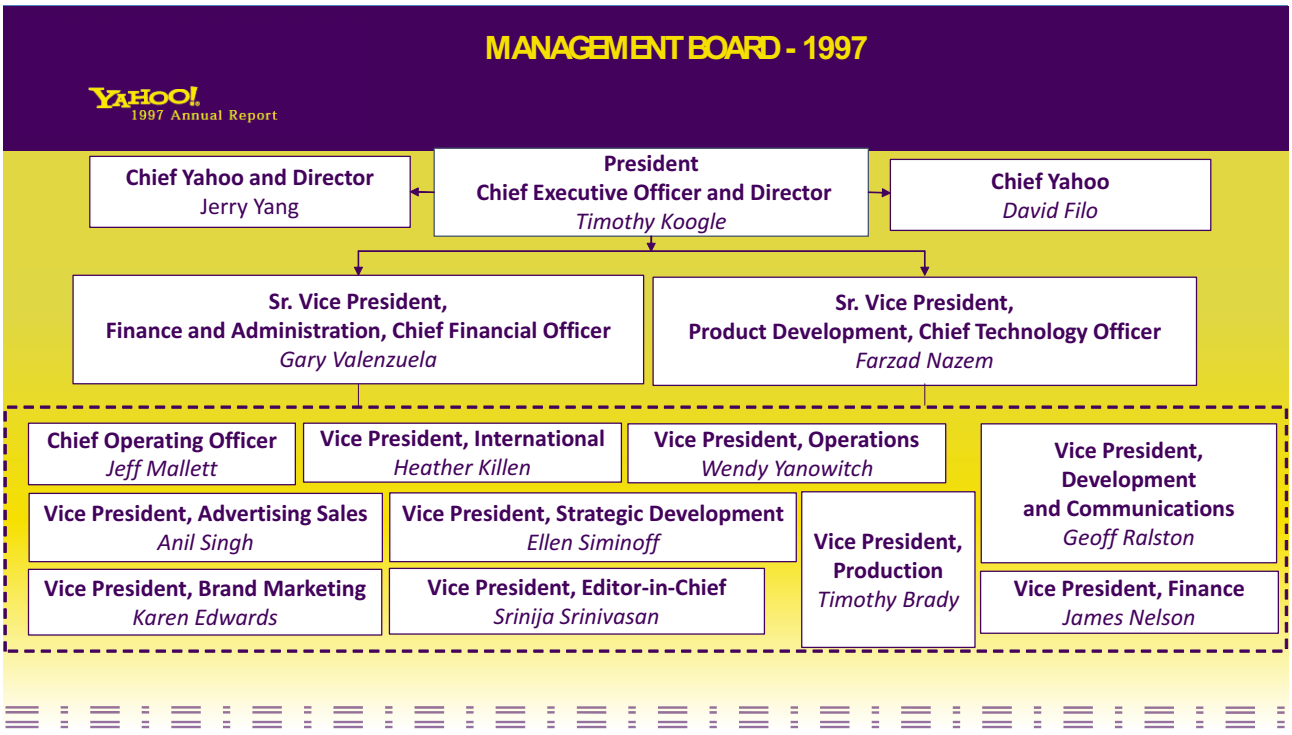

FIGURA 1

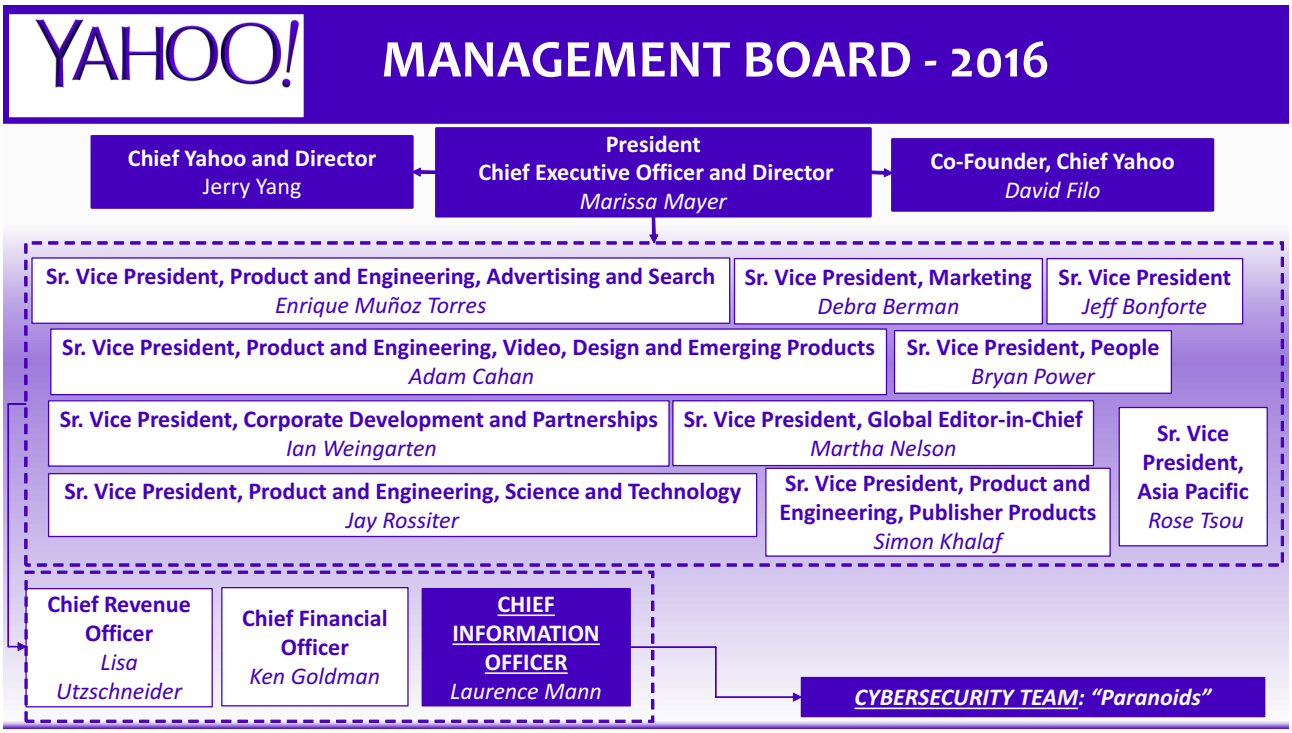

FIGURA 2

4.12. Analisi della struttura dell'*Executive Board* di Verizon in termini di *privacy compliance*

Nel tentativo di comprendere se l'atteggiamento di Verizon nei confronti della questione della *data protection* possa o meno essere assimilato a quello della acquisita Yahoo, occorre innanzitutto concentrarsi sull'organigramma aziendale, ed in particolare sui componenti l'*Executive Board*.
Indicativa della maggiore strutturazione dell'organigramma interno di Verizon, se osservato dalla prospettiva della tutela dei dati personali, un dato emerge immediatamente rispetto a Yahoo: la presenza di un *Executive Vice President and Chief Information and Technology Architect*.
Quanto a questa carica, è emblematica l'attribuzione nelle mani della stessa figura aziendale del potere e delle responsabilità che sorgono da un lato in ordine alla gestione e al monitoraggio del *workflow* dei dati (nonché, tra gli altri, anche dei dati personali) e, parimenti, dall'altro in materia di architettura del *software* - e dunque anche con riferimento all'applicativo impiegato per la stessa gestione dei dati, come anche di tutte le tecnologie che andranno a far parte del parco applicativo di Verizon e che saranno gli strumenti attraverso i quali i trattamenti dei dati verranno effettuati: solo concentrando entrambi questi profili su un unico soggetto cui spetterà assumere le relative decisioni è possibile garantire l'implementazione e lo sviluppo di *software* realmente *Secure by design*, che contemperi le esigenze operative della società e la tutela della dignità della persona.
La Sicurezza *by Design* ed i principi afferenti non sono un *unicum* in ambito *privacy*: al contrario, è l'approccio *risk-based* ad essere stato traslato e proiettato anche sul piano della gestione dei dati personali.
Secondo l'opinione espressa dall'OWASP (*The Open Web Application Security Project*), l'architettura del *software* non può prescindere da una fase di analisi in cui considerare aspetti quali la sussistenza di un sistema di controlli a più livelli, o quantomeno la verifica circa l'attribuzione dei *privileged accounts* esclusivamente ai soggetti per i quali ciò sia indispensabile, riducendo, così, i connessi rischi ad un elevato numero di utenti "privilegiati".
Questo è l'insieme di verifiche che spetta portare a termine al *Chief Information and Technology Architect*, che, contestualmente, deve essere in grado di implementare e rendere pienamente operativo un sistema integrato di gestione del *workflow* dei dati, nonché un sistema di *data* e *metadata management*, operazione resa sempre più complessa dal numero sempre crescente di dati che quotidianamente gli operatori economici del settore delle telecomunicazioni si trovano a gestire.
Altresì, altrettanto significativa è la figura dell'*Executive Vice President of Public Policy*: questa figura risponde all'esigenza di inserire all'interno delle aziende delle figure ibride e altamente specializzate, a metà strada fra il profilo tecnico ed il profilo giuridico.

Siffatta carica attribuisce, a chi la riveste, una serie di competenze in ordine alle *policy strategy* della società: tale ruolo è fondamentale anche in termini di *awareness*, che questa figura deve essere in grado di maturare in anticipo rispetto a tutti gli altri membri dell'*Executive Board*, per guidarne, con la sua lungimiranza, il *decision-making process*.

4.13. Obblighi di *compliance* e rapporto con gli *shareholders* e gli *stakeholders*

Il principio cardine che oggi ricorre nella gestione dei dati personali, come disciplinati dal Reg. (UE) 2016/679, in contrapposizione con quanto previsto in materia di dati non personali, la cui circolazione è disciplinata dal Reg. (UE) 2018/1807, si può riassumere con il termine inglese: "*accountability*".

Quanto a tale principio, non è presente nella lingua italiana un termine che gli sia perfettamente corrispondente; tuttavia, i commentatori sono abbastanza concordi nel tradurlo in italiano come principio di "responsabilizzazione".

In particolare, ad essere richiesta è non già esclusivamente l'adozione delle misure volte a garantire l'integrità, la riservatezza e la disponibilità dei dati, bensì anche la documentabilità di tali misure.

A tale riguardo, nel Marzo 2018, in ragione delle nuove e sempre più pressanti sfide che il *cyber*-spazio comporta, è stata presentata una *proposalcalling* da parte degli azionisti di Verizon, per imporre dei vincoli più stringenti in termini di responsabilità sull'operato dei membri *Senior* del *company's board*: l'idea alla base è quella di porre in correlazione le *senior executive compensation* con l'efficacia delle misure tecniche ed organizzative implementate, per quanto di competenza, in materia di *cybersecurity* e *data protection*[149].

Le preoccupazioni degli investitori sono tanto più fondate quanto più si considerano, ad es., le criticità sorte all'acquisto di Yahoo - e le conseguenti attività necessarie per rendere *privacy compliant* i nuovi *assets* acquisiti: nonostante dal punto di vista delle misure tecniche ed organizzative siano numerose le *cyber security solutions* che la società è in grado di offrire, attingendo alle competenze altamente specializzate dei propri dipendenti, tra i quali *Security risk manager and operators*, *Infrastructure security manager*, *Application Security Engineers*, nonché *Incident Response Analysts,* tuttavia gli attacchi *cyber* impongono una valutazione periodica e un rinnovamento ed una ricerca costanti delle vulnerabilità che possono essere sfruttate da eventuali minacce.

In virtù della proposta in discussione, la *compliance* in materia di *cyber security* verrebbe ad essere equiparata, a tutti gli effetti, ai tradizionali fattori di computazione delle compensazioni

[149] https://trilliuminvest.com/wp-content/uploads/2018/03/Trillium-Press-Release-Verizon-Shareholders-Demand-Cyber-Security-and-Dat-Privacy-Accountability.pdf.

dell'*Executive Board*, dipendenti, di regola, da parametri quali i guadagni per ciascuna azione, ovvero il *cash flow* e i guadagni ottenuti al netto delle spese sostenute.

Sebbene già chiarito precedentemente, pare opportuno ribadire come proprio sul rispetto del princicpio di *accountability*, citato all'inizio del presente paragrafo, si basi l'obbligo giuridico di fornire tutte le informazioni relative al trattamento, pendente in capo a chi effettua qualsiasi operazione sui dati personali degli interessati, ovvero i soggetti cui quei dati sono riconducibili (al contrario, se la persona fisica non è in alcun modo individuabile, neppure con l'ausilio di dati ulteriori, *nulla questio* in termini di *data protection*).

È proprio con riferimento a tale obbligo che Verizon non ha saputo dimostrare in ogni occasione piena coerenza tra quanto professato nelle dichiarazioni *spot* dei propri portavoce da un lato, ed il contegno dimostrato durante la fase operativa del trattamento dei dati degli *stakeholders* dall'altro.

A riguardo, pare opportuno segnalare quanto riportato da Karl Bode in un articolo pubblicato sul sito "www.vice.it" nell'estate del 2018[150]: il servizio di VPN (*Virtual Private Network*) implementato da Verizon assieme al colosso McAfee, prevedeva dei "Termini d'uso del servizio" piuttosto opachi - rinviava, infatti, all'informativa generica prevista per tutti i servizi offerti dal partner di Verizon McAfee, una *policy privacy* sicuramente meno "*compliant*" dal punto di vista della *data protecion*, avuto particolare riguardo agli stringenti vincoli che Verizon aveva promesso di imporsi per il trattamento dei dati personali degli utenti raccolti nell'ambito della fornitura del servizio di VPN.

Tale servizio, in particolare, si poneva come un requisito tecnico imprescindibile e strumentale all'offerta di un ulteriore prodotto da parte di Verizon: un'applicazione di "*Safe Wi-fi*" per garantire la massima riservatezza e la massima protezione alla navigazione e alle comunicazioni dei propri utenti.

Ad ogni modo, l'attuale informativa ha ricucito lo strappo, assicurando quanto segue a tutti gli utenti del colosso americano che usufruiranno del servizio in discorso: "*Safe Wi-Fi app utilizes proprietary technology [...] uses information obtained from your device, including IP address and Wi-Fi access point data*" ed in ogni caso "*Neither Verizon nor its third party licensor(s) or vendors access or collect any information that you send or receive through your Safe Wi-Fi secure connection*" [151], ponendo, dunque, uno stringente margine alla circolazione dei dati personali dei propri utenti, assicurando loro una tutela piuttosto robusta.

[150] Karl BODE, *Verizon didn't bother to write a privacy policy for safe wi-fi privacy*, "Vice" 6.08.2018, ultima consultazione 29.09.2019.

[151] VERIZON INC, *Terms of Services for the Verizon Safe Wi-Fi App*, consultabile al seguente link "https://www.verizonwireless.com/support/safe-wifi-legal/".

4.14. Epilogo

In conclusione, il dato storico è sicuramente piuttosto impietoso: la *brand reputation* di Yahoo, a seguito delle rivelazioni dei *data breach* del 2013 e del 2014, risulta piuttosto appannata, e con essa risulterà parimenti ridimensionata la somma originariamente offerta da Verizon ai fini dell'acquisizione del *core Internet business* di Yahoo (da 4.8 a 4.48 miliardi di dollari, una differenza di 350 milioni di dollari)[152].

Ciò dimostra quanto l'adozione di strategie ormai piuttosto diffuse, quali, tra le altre, sistemi di reportistica di tipo SIEM (*Security Information and Event Management*), lo sviluppo di tecnologie di cifratura end-to-end in combinazione con la cifratura di canale, nonché strumenti di *Intrusion-detection System* come anche di *Intrusion-prevention System*, pienamente riconosciute quali *best practices* o quali *standard* comunque richiesti *ex lege*[153], siano elementi fondamentali, che vanno a confluire all'interno del patrimonio immateriale dell'azienda, in termini di *Know-how* che l'azienda può sia sfruttare al proprio interno, sia offrire ai propri clienti.

Sulla base di queste premesse, dovrebbe risultare quantomai superfluo rimarcare che la definizione di adeguate *policy* / *procedure* dedicate esclusivamente al trattamento dei dati personali è ormai un passaggio imprescindibile per ottimizzare l'organizzazione interna dell'azienda.

E proprio la carenza di un corretto sistema interno di gestione del *workflow* dei dati personali è stato alla base della perenne vulnerabilità dimostrata dalla compagnia americana.

Infine, per concludere questa breve analisi, appare opportuno un accenno pure al diverso profilo delle responsabilità che possono sorgere in capo alle società, connesse alla violazione degli adempimenti previsti dalle diposizioni in materia di tutela dei dati personali.

È evidente, nel caso specifico oggetto di studio, la violazione, da parte di Yahoo, di due importanti doveri previsti dal diritto americano nei confronti degli *shareholders*: il primo dei due consiste nel generico dovere di controllo, in capo al management, il cui adempimento non può prescindere da un corretto processo di trasferimento delle informazioni ai vertici aziendali.

Una simile violazione risulta particolarmente grave nell'ipotesi in cui dalla stessa dipenda un importante pregiudizio al patrimonio dell'intera società.

Di talché, è innegabile la stretta correlazione ed il rapporto di causa effetto che può essere ricostruito tra la mancata predisposizione di un processo interno che assicuri che tutte le informazioni rilevanti

[152] Lawrence J. Trautmat e Peter C. Ormerod, op. cit., pag. 1285.

[153] Ad es., in Italia il Provvedimento dell'Autorità Garante per la Protezione dei dati personali del 27 novembre 2008, modificato con Provvedimento del 25 giugno 2009, prevede la registrazione di tutte le operazioni compiute dagli Amministratori di Sistema, attraverso sistemi di *log management*.

giungano ai vertici aziendali, da una parte, e la violazione del dovere in capo al "*corporate board*" di essere sempre informato, dall'altra.

Secondo importante obbligo violato da Yahoo è quello di comunicare agli *shareholders* tutte le informazioni relative ai *data breach*. Tali informazioni devono essere pertinenti, come già detto, complete, adeguate, nonché tempestive, per tutelare degli investitori, e per garantire loro scelte pienamente informate.

Entrami i due doveri fin qui indicati promanano da un più generico dovere di diligenza, in particolare dal dovere, in capo al soggetto che tratta i dati, di garantire la sicurezza dei dati personali oggetto del trattamento.

A riguardo, sulla base del Report annuale interno prodotto da Yahoo, reso noto il primo marzo del 2017, appare chiaro come alcuni membri rilevanti dell'Ufficio Legale della società già nel tardo 2014 fossero a conoscenza del fatto che erano stati effettuati accessi non autorizzati a dei *privileged account* della società, sfruttando alcune falle nei relativi *management tool*[154].

Pertanto, ad oggi, nessun dubbio permane sul fatto che il *Legal Team* di Yahoo avesse adeguate informazioni quantomeno per avviare ragionevolmente un'analisi più approfondita; al contempo, seppure la condotta dei *Senior Executives* di Yahoo non possa configurarsi nei termini di una vera e propria "*intentional suppression of relevant information*", tuttavia è in ogni caso innegabile che la medesima integri una violazione del dovere di trasparenza e di diligenza[155].

[154] Cfr. K. Swisher, *Yahoo's Head Lawyer Is Taking the Fall for Its Hacking, While CEO Marissa Mayer Is Getting Her Pay Docked*, "RECODE", 1.03.2017, ultima consultazione 19.08.2019

[155] Lawrence J. Trautmat e Peter C. Ormerod, op. cit., pag. 1283.

CONCLUSIONI

Negli ultimi anni, il fenomeno della digitalizzazione ha completamente travolto le realtà aziendali. Il processo di trasformazione digitale, ormai, viene considerato dalle organizzazioni un passo quasi obbligato da compiere, seppur non facile, per rimanere competitive sul mercato. Le imprese, perciò, nonostante fatichino in un primo momento a capire l'importanza della digitalizzazione e ritardandola nel tempo, ad un certo punto del loro ciclo di vita la considerano necessaria.

La *Digital Trasformation*, infatti, consente alle aziende di crescere dal punto di vista della produttività e della redditività, impattando soprattutto nel rapporto con i clienti, i quali percepiscono una *customer experience* migliore, che è il motivo principale che le spinge al cambiamento.

In questa nuova realtà, le organizzazioni dovranno munirsi di strumenti per far fronte ai pericoli e ai rischi a cui vanno incontro; il mercato digitale, infatti, è turbolento e competitivo e non bisogna sottovalutare gli attacchi da parte dei *cyber* criminali che possono presentarsi in qualsiasi momento; esempio rappresentativo è il caso di *data breach* di *Yahoo*.

Per queste ragioni, le organizzazioni dovranno mutare la struttura da funzionale a matrice o divisionale, diffondere una nuova cultura organizzativa e promuovere personale con elevante competenze digitali. I dati infine rivestono un ruolo fondamentale, grazie ai quali le imprese possono raccogliere informazioni preziose per le loro decisioni aziendali.

Tutto ciò permetterà di orientare le imprese, che adottano questa tecnologia, verso un nuovo scenario; queste riusciranno infatti non solo ad aumentare l'efficienza, anche in termini economici, all'interno dell'azienda, ma questo processo comporterà un cambiamento di *leadership*, un modo di pensare del tutto diverso rispetto al passato, nuovi modelli di business e sicuramente un uso sempre maggiore della tecnologia per migliorare il rapporto con i propri clienti e con tutti coloro che fanno parte dell'azienda.

Con il tempo le imprese noteranno che esistono divere ragioni per le quali è opportuno intraprendere e portare a termine il percorso di Trasformazione Digitale: come già anticipato, una maggiore efficienza aziendale, esperienza dei clienti cambiata in meglio, aumento dei profitti e allineamento rispetto la concorrenza. Per quanto concerne in particolare il penultimo punto, l'aumento dei profitti, è opportuno precisare che le organizzazioni che avvieranno la Trasformazione Digitale, noteranno grazie ad essa che ulteriori vantaggi riguarderanno le spese in conto capitale e le spese operative: nonostante molti considerano che l'adozione di questo processo possa tradursi in maggiori costi, in realtà la digitalizzazione dei processi può far risparmiare in media il 40% incidendo proprio sulle spese in c/c e sulle spese operative, apportando miglioramenti in termini di efficienza, affidabilità e sicurezza.

In termini di *Digital Trasformation* perciò, il "sogno" di un'impresa, ciò che essa vuole diventare in una prospettiva futura è un punto di riferimento per i propri clienti, offrire loro cioè delle soluzioni innovative per aiutarli e assisterli; per fare questo quindi è necessario accelerare la conoscenza con i nuovi paradigmi digitali per sfruttare al meglio queste opportunità; con il tempo infatti le imprese percepiranno un legame diverso con i propri clienti, un legame cioè basato su una maggiore fiducia.

In conclusione si può affermare che l’adozione di questo processo, nonostante comporti dei rischi e difficoltà in un primo momento, rappresenta per le imprese una vera e propria opportunità per rimanere competitive sul mercato e soddisfare la propria clientela.

BIBLIOGRAFIA

Adams, K., "The Sources of Innovation and Creativity". Washington: National Center on Education and The Economy, 2005.

Allen T.D., Eby L.T., Lentz E., "The role of interpersonal comfort in mentoring relationships", Journal of Career Development, 31, 155-169, 2005.

Anderson E., Sbannon A.L., "Toward a conceptualization of mentoring", 1988.

Anthohy, R.N., Hawkings, D.F., Macrì, D.M., Kenneth, A.M., "Sistemi di controllo. Analisi economiche per le decisioni aziendali", McGraw-Hill, Milano, 2004.

Armstrong M., "Human Resourse Management", Practice, 2010.

Baldassi, S., Superare la resistenza al cambiamento: i tre passi del change management", 2012.

Baraldi S., Devecchi C., "I sistemi di pianificazione, programmazione e controllo", Giappichelli Editore, Torino, 1994.

Bartlett C.A., Ghoshal S., "Building Competitive Advantage through People", 2010.

Bassetti M., "Un Sistema integrato di gestione delle risorse umane", settima edizione, 2007.

Bharadwaj, A., Sawy, OA.El., Pavlou, PA., Venkatraman, N., "Digital business strategy: toward a next generation of insights", MIS Q. 37, 2013.

Boccardelli P. – Iacovone D. (a cura di), *"L'impresa" di diventare digitale. Come la rivoluzione tecnologica sta influenzando la gestione di impresa*, Il Mulino, 2017.

Braverman H., *Lavoro e capitale monopolistico: la degradazione del lavoro nel XX secolo*, Einaudi, 1978.

Brotherston L. – Berlin A., *La sicurezza dei dati e delle reti aziendali, tecniche e best practice per evitare intrusioni indesiderate,* Tecniche Nuove, 2017

Caroli, M., "Il marketing per la gestione competitiva del territorio. Modelli e strategie per attrarre (e far rimanere) nel territorio persone, imprese e grandi investimenti", Franco Angeli, 2014.

Casalino N., Ciarlo M., "Dalla competizione alla collaborazione sui servizi: valutazione e formulazione di strategie a sostegno dell'innovazione", Proceedings of XXXIV Convegno di Economia Aziendale - AIDEA 2011 "Aziende di servizi e servizi per le aziende - La ricerca di un percorso di sviluppo sostenibile per superare la crisi", 13-14 ottobre, Università di Perugia, 2011.

Casalino, N., "Gestione del cambiamento e produttività nelle aziende pubbliche. Metodi e strumenti innovative", volume, pp. 1-201, Cacucci Editore, Bari, 2008.

Casalino, N., “Innovation's governance and investments for enhancing Competitiveness of Manufacturing SMEs”, 2012.

Casalino, N., “Innovazione e organizzazione nella formazione aziendale”, pp. 1-212, Collana di Economia Aziendale - Serie Scientifica diretta da Nicola Di Cagno, n.10, Cacucci Editore, 2006.

Casalino, N., “Learning to Connect: a training model for public sector on advanced E-Government services and InterOrganizational cooperation”, International Journal of Advanced Corporate Learning (iJAC), Austria, vol. 7, no.1, pp. 24-31, 2014.

Casalino, N., “Piccole e medie imprese e risorse umane nell'era della globalizzazione”, Collana di Studi di Tecnica Aziendale, n.90, pp. 1-273, Wolters Kluwer Italia, 2012.

Casalino, N., Ciarlo, M., “ICT Adoption and Organizational Change. An Innovative Training System on Industrial Automation Systems for enhancing competitiveness of SMEs”, Proceedings of 14th International Conference on Enterprise Information Systems - ICEIS 2012, June 28 - July 1, 2012, Wroclaw, Poland, a cura di Maciaszek L., Cuzzocrea A., Cordeiro J. (Eds.), INSTICC, Setubal, Portugal, pp. 236-241, ISBN 978-989-8565-11-2, 2012.

Casalino, N., Ciarlo, M., De Marco, M., Gatti, M., “ICT Adoption and Organizational Change. An Innovative Training System on Industrial Automation Systems for enhancing competitiveness of SMEs”, Proceedings of 14th International Conference on Enterprise Information Sy-stems - ICEIS 2012, Maciaszek, L., Cuzzocrea, A., Cordeiro, J. (Eds.), INSTICC, Setubal, Portugal, pp. 236-241, 2012.

Casalino, N., D'Atri, A., Braccini, A.M., “A Management Training System on ISO Standards for Organisational Change in SMEs, International Journal of Productivity and Quality Management (IJPQM)”, Inderscience Publishers, USA, vol. 9 no. 1, pp.25-45, 2012.

Casalino, N., D'Atri, A., Manev, L., “A quality management training system on ISO standards for enhancing competitiveness of SMEs”, Proc. 9th International Conference on Enterprise Information Systems - ICEIS 2007, 12-16 giugno, Funchal, Madeira - Portogallo, Cardoso J., Cordero J., Filipe J. Eds., INSTICC, Setubal, Portugal, pp. 229-235, 2007.

Casalino, N., Ivanov, S., Nenov, T., “Innovation's Governance and In-vestments for Enhancing Competitiveness of Manufacturing SMEs”, Law and Economics Yearly Review Journal, vol. 3, part 1, pp. 72-97, Queen Mary University, London, UK, 2014.

Casalino, N., Saso, T., Borin, B., Massella, E., Lancioni, F., Digital Competences for Civil Servants and Digital Ecosystems for More Effective Working Processes in Public Organizations, LNCS, Springer, Heidelberg, Germany, 2019.

Consolini, M., Di Saverio, M., Loasses, C. & Richini, P. “Indicazioni per la programmazione e la realizzazione di iniziative per l’educazione all’imprenditorialità”, Roma, ISFOL, 2013.

Contaldo A. – Peluso F., *Cybersecurity, la nuova disciplina italiana ed europea alla luce della direttiva NIS,* Pacini Giuridica, 4 luglio 2018.

Corradini I., *Internet delle cose. Dati, sicurezza e reputazione,* Franco angeli, 2017

Cristoforetti G. – Lodi G., *Human Revolution: Quarta rivoluzione industriale e innovazione sociale*, Imprimatur editore, 2017.

Daft R.L., Organizzazione Aziendale, 6 ed., Maggioli-Apogeo, 2018.

Di Taranto G., *Dalle infrastrutture materiali di comunicazione alle reti immateriali di connessione*, in C.B. Lopez et al. (a cura di), *Vie e mezzi di comunicazione in Italia e Spagna in età contemporanea*, Rubbettino, 2013.

Edwin, E. Gerloff, "Strategie organizzative". McGraw-Hill, Milano, 1989.

Finaf s.p.a - "Modello di organizzazione, gestione e controllo ex d.lgs. 231/2001".

Floridi L., *La Rivoluzione dell'informazione,* Codice, 2012.

Fontana F., "Il sistema organizzativo aziendale", Franco Angeli, 1999.

Fontana F., "Lo sviluppo del personale", Giappichelli, 1994.

Fontana F., Caroli M., "Economia e gestione delle imprese", McGraw-Hill, 2013.

Garrison, R.H., Noreen, E.W., "Programmazione e controllo. Managerial accounting per le decisioni aziendali", Mcgraw-Hill, Milano, 2004.

Garzia F., *Sicurezza delle comunicazioni, telecomunicazioni, criptografia, steganografia, digital watermarking, reti cablate, reti wireless, comunicazioni vocali, protezione delle intercettazioni,* EPC, 2012.

Giacomazzi, F., Camisani Calzolari M., "Impresa 4.0 – Marketing e comunicazione digitale a direzioni", Financial Times - Pearson, Milano, 2010.

Gilchrist A, *Industry 4.0: The Industrial Internet of Things*, Apress, 2016.

Gilster P., *Digital Literacy,* John Wiley & Sons Inc, 1997.

Giustiniano L., "Strategie, organizzazione e sistemi informativi: dall'IT alignment all'IT governance", Franco Angeli, 2013.

Giustiniano L., Prencipe A., "La digital transformation di una multi-utility. Tecnologia e persone, fattori chiave dell'esperienza ACEA", Harvard Business Review Italia, 2017.

Gjergji, R., Lazzarotti V., Visconti F., "Innovazione, internazionalizzazione e performance: Il contributo di noi giovani imprenditori", 2016.

Goel V., Lichtblau E., *Russian Agents Were Behind the Yahoo Hack, U.S. Says*, "The New York Times", 15.03.2017, ultima consultazione 31.07.2019.

Goel V., Lichtblau E., *Yahoo Says 1 Billion User Accounts Were Hacked*, "The New York Times", 14.12.2016, ultima consultazione 12.08.2019.

Gross D., *Yahoo hacked, 450,000 passwords posted online*, "CNN Business", 13.07.2012.

Günther A., *Sulla distruzione della vita nell'epoca della terza rivoluzione industriale*, in Id. (a cura di), *L'uomo è antiquato*, Torino, Bollati Boringhieri, 2007.

Jacobs A., Helft M., *Google Citing Attack, Threatens To Exit China*, "The New York Times", 12.01.2010, ultima consultazione 19.08.2019.

Johnson B., *Chinese hackers used Microsoft broswer to launch Google strike*, "The Guardian", 14.01.2010.

Kurose F. James, Keith W., *Reti di calcolatori e internet*, Milano-Torino, Pearson, 2013, sesta edizione.

Legrenzi, P., "Creatività e innovazione", Bologna: Il Mulino, 2005.

Magone A. – Mazali T., *Industria 4.0, Uomini e Macchine nella Fabbrica Digitale*, Guerini e Associati, 2017.

Markoff J. e Barboza D., *2 China Schools Said to Be Tied to Online Attacks*, "The New York Time", 18.02.2010.

McKinsey&Company, A future that works: automation, employment, and productivity. McKinesy Global Institute, 2017.

Menezes J. Alfred, Van Oorschot C. Paul, Scott A. Vastone, *Handbook of applied cryptography*, 1996.

Minztberg, H., "The structuring of organization", Englewood Cliffs – Prentice Hall, 1979.

Parolini, C., "Business Planning - Dall'idea al progetto imprenditoriale", Milano-Torino: Pearson, 2011.

Perlroth N., Goel V., *Defending Against Hackers Took a Back Seat at Yahoo, Insiders Says*, "The New York Times", 28.09.2016, ultima consultazione 19.08.2019.

Porter, M.E., "Competitive Advantage: Creating and Sustaining Superior Performance", The Free Press, New York, 1985.

Potito, L., "Le operazioni straordinarie nell'economia delle imprese", Giappichelli Editore, Torino, 2006.

Prunesti A. – Bombardieri M., *Chief Digital Officier Gestire la Digital Trasformation per persone e organizzazioni,* Franco Angeli, 2019.

Rifkin J., *La terza rivoluzione industriale*, Mondadori, 2011.

Rogers, D., "The network is your customer: 5 strategies do thrive in a digital age", Yale University Press, UK, 2011.

Sartori L., *Il Divario digitale. Internet e le nuove disuguaglianze sociali*, Il Mulino, 2006.

Schwab K., *La quarta rivoluzione industriale*, Franco Angeli, 2016.

Secchi R. – Rossi T., *Fabbriche 4.0 percorsi di trasformazione digitale della manifattura italiana,* Guerini Next, 2018.

Simon H.A., "A formal Theory of the employment relation", trad. it. Causalità, razionalità, organizzazione, Il Mulino, 1985.

Stallings W. (a cura di) Salgarelli L., *Crittografia e sicurezza delle reti*, Mc-Graw Hill, 2° edizione, 2013.

Stanzione M. G., *Il Regolamento europeo sulla privacy: origini e ambito di applicazione,* "Europa e diritto privato", IV (2016).

Swisher K., *Yahoo's Head Lawyer Is Taking the Fall for Its Hacking, While CEO Marissa Mayer Is Getting Her Pay Docked*, "RECODE", 1.03.2017.

Thomas, H. Davenport, "Innovazione dei processi - Progettare il lavoro attraverso l'Information Technology". Franco Angeli, Roma,1995.

Trautmat J. Lawrence e Peter Ormerod C., *Corporate directors' and officers' cybersecurity standard of care: the Yahoo data breach*, "American University Law Review, LXVI (2017)"

Verganti, R., "Design driven innovation", Harv. Bus. Sch. 40, 2009.

Weizmann H.C., "Gestione delle risorse umane e valore dell'impresa", Milano, Franco Angeli, 2010.