Università degli Studi di Padova

Dipartimento di Diritto Privato e Critica del Diritto

Corso di Laurea in Consulente del Lavoro a.a. 2022/2023

Titolo tesi: Etica e diritto dell'intelligenza artificiale nella prospettiva europea

Relatore: Letizia Mingardo

Studente: Miriam Bosco

INTRODUZIONE……..…..……..3

1 INTELLIGENZA ARTIFICIALE E PRINCIPI ETICI……...…....7

1.1 DEFINIZIONE DI INTELLIGENZA ARTIFICIALE……...7
1.2 I PRINCIPI ETICI A FONDAMENTO DELL'INTELLIGENZA ARTIFICIALE…….9
1.3 IL CONCETTO DI SOFT ETHICS E IL CONCETTO DI GOVERNANCE..13
1.4 L'INTELLIGENZA ARTIFICIALE A BENEFICIO DELLA SOCIETA'….....16
1.5 IL PERCORSO VERSO LA PROPOSTA DI REGOLAMENTO EUROPEO.....20

2 INTELLIGENZA ARTIFICIALE E DIRITTI DEI LAVORATORI……...……26

2.1 DEFINIZIONE DI INTELLIGENZA ARTIFICIALE SECONDO L'UNIONE EUROPEA…….……26
2.2 DESTINATARI DELL'ARTIFICIAL INTELLIGENCE ACT……..…27
2.3 I PRESUPPOSTI DELLA NORMATIVA DELL'ARTIFICIAL INTELLIGENCE ACT.....27 **2.4 GLI OBBIETTIVI DELL'AI ACT**……29
2.5 I CONTENUNTI DELLA PROPOSTA DI REGOLAMENTO……..…...37
2.6 I DIRITTI FONDAMENTALI DA TUTELARE……...……..39

3 INTELLIGENZA ARTIFICIALE E PRIVACY DEI LAVORATORI……43
3.1 LE NUOVE TECNOLOGIE UTILIZZATE NELL'AMBITO LAVORATIVO……...43
3**.2 IL REGOLAMENTO 2016/679 E IL NUOVO CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI**……...……45
3.3 LO STATUTO DEI LAVORATORI…….....48
3.4 IL NUOVO DECRETO TRASPARENZA……..……..53
3.5 IL FENOMENO DEL BRACCIALETTO ELETTRONICO E LA PEOPLE ANALYTICS……...……...56

CONCLUSIONE……...……64

BIBLIOGRAFIA.....68

INTRODUZIONE

Quello di cui andremo a trattare in questo scritto riguarda una tematica attuale e in continua evoluzione. Parleremo di Intelligenza artificiale, all'interno della prospettiva europea. Per prima cosa, è fondamentale allora dare una definizione concreta di quella che è oggi l'intelligenza artificiale, del momento evolutivo a cui siamo arrivati e di come stia sempre più entrando nella nostra vita quotidiana. Sotto quest'ultimo punto di vista in realtà, ormai non si può dire che l'IA stia entrando a far parte delle nostre vite, infatti sarebbe più opportuno dire che è già entrata nelle nostre vite, nella nostra quotidianità e nei vari ambienti in cui si svolge la vita di tutti i giorni. Per prima cosa dobbiamo partire da una piccola descrizione dell'evoluzione avvenuta negli ultimi anni e dando una definizione di intelligenza artificiale, la quale, come vedremo, non è univoca e della quale non esiste una che sia completamente esaustiva. Data l'esponenziale crescita di questi sistemi e la loro entrata in tutti gli ambiti della nostra quotidianità, è importante procedere con l'analisi di quelli che sono i rischi che porta con sé. Per fare questo passo, non si può non andare a menzionare quelli che sono i principi etici che vanno in qualche modo a delimitare e a tutelare tale fenomeno. In questo caso ci vengono in aiuto vari esperti ed autori, in particolare vedremo come Floridi risulta fondamentale per la disamina di questa questione. L'etica, insieme al diritto è alla base della nostra vita, infatti etica e diritto ci permettono di avere un ordine all'interno della società. Proprio per questo motivo, questi principi devono essere applicati anche ai sistemi di intelligenza artificiale. Come vedremo, non possiamo prendere in considerazione l'etica solamente in senso generale, ma sarà opportuno spiegare come si suddivide l'etica, per poi poter parlare di soft ethics e della governance. In questo modo potremmo capire come soft ethics e governance si intrecciano tra di loro e ci permettono di creare una sorta di limite o di area all'interno della quale il diritto può poi muoversi per poter regolamentare l'intelligenza artificiale. Questo ci porterà a capire come è importante andare a sviluppare un'intelligenza artificiale che vada a beneficio dell'umanità e della società in cui viviamo. Essendo tali sistemi di IA così presenti all'interno della nostra quotidianità, questo ci permette di poterli sfruttare al meglio delle nostre possibilità, avendo come primo scopo quello di poterne avere sempre un beneficio. Un beneficio per la collettività, in termini di risparmio di energie e costi, ma senza andare a togliere l'autonomia umana nei confronti di tali

sistemi. Dopo queste considerazioni, che saranno utili perché saranno la nostra base di partenza, possiamo passare a vedere quali sono le norme che ci tutelano oggi dai possibili rischi e problemi che creano i sistemi di intelligenza artificiale. È necessario, primo di arrivare al punto, capire quali sono stati i passi che ci hanno portato ad una prima proposta di regolamento europeo che vada a regolamentare l'intelligenza artificiale. Una volta illustrato il percorso evolutivo, possiamo soffermarci ad analizzare più a fondo quella che è l'Artificial Intelligence Act. Queto regolamento ci fornisce anch'esso una definizione di Intelligenza Artificiale, coniata dall'Unione Europea e si propone come base di regolamentazione di questo fenomeno per i sistemi giurisdizionali dei paesi membri. Prima di andare al punto focale, è importante capire chi sono i destinatari di tale proposta, i quali vengono definiti direttamente dalla normativa stessa. Vedremo come tale normativa va coinvolgere in primo piano gli Stati membri sicuramente, ma anche i soggetti interessati in maniera diretta ovvero, tutti coloro che rientrano nel processo di produzione di questi sistemi fino al consumatore finale. Dopo i destinatari, bisogna andare definire in maniera chiara quelli che sono i presupposti alla base della normativa. Tali presupposti hanno come scopo quello di poter permettere agli utilizzatori di acquistare fiducia nei confronti di tale fenomeno sapendo che alla base vi è una normativa che in caso di problemi, vada a tutelarli. Insieme ai presupposti, non si possono non andare a citare gli obbiettivi dell'Unione, la quale, come potremo vedere vuole assicurare lo sviluppo di sistemi di Intelligenza artificiale sicuri, che vadano a beneficio dell'utilizzatore e che rispettino il diritto dello stesso. Dopo aver elencato ciò che sta alla base dell'atto che andremo ad esaminare e quali sono gli scopi, si può arrivare ad esaminare in maniera più profonda quelli che sono i contenuti della proposta, che, come vedremo, sono molteplici. Per prima l'atto a previsto di dividere i sistemi in base ai livelli di rischio che portano con se, questo per poter creare regole e tutelare diritti in maniera mirata, in base se siamo di fronte ad un sistema a rischio basso, alto o inaccettabile. Dopo aver capito a fondo di cosa tratta la normativa ecco che è utile capire quali sono i diritti fondamentali da tutelare. Tali diritti, ormai li conosciamo tutti, ma bisogna metterli in confronto con la proposta di regolamento. Da qui, dopo un'analisi dei diritti fatta da un punto di vista generale, possiamo scendere nello specifico e andare a prendere uno dei diritti più importante, ma più difficili da tutelare oggi, soprattutto nei confronti di questo fenomeno in continua evoluzione. Il diritto di cui parleremo è il diritto alla privacy. Un

diritto che è già sancito in varie normative, atti e documenti, il quale è sempre in continua evoluzione, perché deve adeguarsi ai tempi. Come ben sappiamo, proprio lo sviluppo di nuovi fenomeni, di nuovi rischi, porta molto spesso il Garante per la Protezione dei Dati Personali a doversi pronunciare su questioni sempre diverse. Ecco che in questa prospettiva dobbiamo mettere a confronto il diritto alla privacy con l'Intelligenza artificiale, poiché il primo deve adeguarsi e trasformarsi in base ai rischi portati dal secondo. La privacy però non va guardata solamente in generale, ma ciò che interessa veramente a noi è la privacy nell'ambito lavorativo. Da qui partiamo andando a definire quindi quelle che sono le nuove tecnologie utilizzate all'interno degli ambienti di lavoro, le quali riguardano tutta la vita del rapporto lavorativo, dalla fase di selezione fino alla fase di cessazione. Dato l'utilizzo di queste nuove tecnologie, non si può non guardare a quelle che sono le normative attuali che ci permettono di poter tutelare la nostra vita privata. In ragione di questo è importante partire dal Codice in materia di protezione dei dati personali, il quale parte anche esso da una normativa a livello europeo, trasposta poi nell'ordinamento italiano. Tale codice ci permette di definire cosa rientra all'interno della nostra vita privata e cosa no, quali sono quindi quelle informazioni che devono rimanere nascoste o che comunque io ho il diritto di scegliere se far conoscere o meno agli altri. Anche qui, partiamo dal generale per arrivare poi al particolare, infatti parliamo di privacy sì, ma privacy del lavoratore. Dato questo presupposto, non possiamo non andare ad illustrare ed esaminare lo Statuto dei Lavoratori, soprattutto dopo la riforma del Jobs Act del 2015. In questo caso sarà utile prendere in considerazione quelle norme che riguardano il potere di controllo del datore di lavoro. questo poter è stato delimitato dal legislatore tramite questa normativa, proprio per andare a eliminare o ridurre comunque al minimo il rischio di violazione alla riservatezza del datore di lavoro. Questo diritto è una prerogativa, perché non tutto quello che faccio nella mia vita privata, può e deve essere conosciuto dal mio datore di lavoro. da qui, infatti, vedremo gli obblighi che ha il datore di lavoro nei confronti dei lavoratori in tema proprio di controlli su di essi. Dopo aver esaminato queste normative meno recenti, passiamo a prendere in considerazione una normativa nuova, la quale è stata emanata nel 2022, ovvero il cosiddetto Decreto Trasparenza. Tale nuova normativa si inserisce a pieno nell'ambito delle normative riguardanti la sfera del lavoro e tratta già in parte dell'evoluzione tecnologica nell'ambito lavorativo. In questo senso, quindi, c'è già stato un piccolo passo avanti nella

giurisdizione italiana. Dopo aver fatto tutta un'esposizione delle normative che vanno a tutelare il lavoratore in materia di privacy, lavoro e nuove tecnologie, ho voluto illustrare un nuovo strumento che ha fatto molto scalpore, ovvero il braccialetto elettronico. Tale braccialetto offre una grande possibilità di controllo al datore di lavoro nei confronti del lavoratore. Un controllo che in molti casi potrebbe diventare costante. Tuttavia non si può parlare di controllo senza andare a parlare di valutazione della performance del lavoratore e quindi del fenomeno della *People Analytics*. Tali tipo di nuovo tecnologia potrebbe rientrare in questo nuovo concetto e portare a rischi molti alti in materia di privacy, quindi è necessario capire come questi due elementi possano intrecciarsi fra loro e che tutele abbiamo a disposizione. Infine come ultima cosa, ho deciso di fare un breve accenno all'utilizzo di sistemi di Intelligenza Artificiale nell'ambito del reclutamento dei lavoratori, dando uno sguardo alla normativa vigente e alla nuova proposta di regolamento.

1 INTELLIGENZA ARTIFICIALE E PRINCIPI ETICI

1.1 DEFINIZIONE DI INTELLIGENZA ARTIFICIALE

Prima di arrivare a dare una definizione di Intelligenza Artificiale, è importate fare un passo indietro e comprendere come siamo arrivati allo sviluppo di questa forma di intelligenza, la quale ormai è presente in tutti gli strumenti tecnologici che utilizziamo nella nostra vita quotidiana. Lo sviluppo dell'Intelligenza artificiale è stato possibile e continua ad essere possibile grazie alla crescita continua della potenza di calcolo dei software, alla crescita della capacità di archiviazione ed elaborazione dei dati e grazie ai costi sempre più contenuti. Altro fattore che incide sempre di più su questa crescita è il fatto che noi essere umani interagiamo ogni giorno di più con contesti digitali. Questo diventa ancor più evidente nel momento in cui ci rendiamo conto che ormai il numero di dispositivi digitali è maggiore rispetto alla popolazione umana. Ecco che, da questa crescita sempre più veloce e da queste interazioni, nasce il termine *onlife*. Questo termine è stato coniato da Luciano Floridi, il quale spiega come nella realtà attuale la gran parte delle persone vive sempre più frequentemente *onlife*, ovvero sia online, sia offline nell'infosfera[1], sia digitalmente che analogicamente. Questo tipo di interazioni, ha portato però alla raccolta di una quantità di dati enorme, da qui infatti nesce la necessità di proteggere la privacy dei soggetti interessati. Questo perché questa quantità di dati raccolti, nella maggior parte di casi porta a poter identificare una persona e alla raccolta di informazioni strettamente personali a lei riconducibili. La privacy in questo modo diventa una questione sempre più rilevante ed urgente e così il legislatore ha capito che era necessario arrivare a emanare una normativa Europea sulla protezione dei dati personali e che è diventato fondamentale istituire il Garante per la protezione dei dati personali o Garante privacy. Fatta questa premessa, ora è fondamentale capire che cos'è l'Intelligenza Artificiale[2]. Per prima cosa, dobbiamo tenere in considerazione che quando

[1] Lo spazio semantico costituito dalla totalità dei documenti, degli agenti e delle loro operazioni, dove per "documenti" si intende qualsiasi tipo di dato, informazione e conoscenza, codificata e attuata in qualsiasi formato semiotico, gli "agenti" sono qualsiasi sistema in grado di interagire con un documento indipendente (ad esempio una persona, un'organizzazione o un robot software sul web) e il termine operazioni include qualsiasi tipo di azione, interazione e trasformazione che può essere eseguita da un agente e che può essere presentata in un documento.

[2] Prima di dare una definizione, ci tengo a precisare che all'interno del concetto di IA rientra in parte anche una branca della robotica. Paolo Moro precisa come ormai alcuni robot siano dotati di intelligenza artificiale e imitino i ragionamenti, quali la comprensione del linguaggio naturale, l'apprendimento automatico, ma

si parla di IA non abbiamo una sola ed unica definizione. L'IA può essere definita come *l'insieme degli studi e delle tecniche, pertinenti all'informatica, (...) che mirano alla realizzazione delle macchine o programmi in grado di risolvere problemi e di riprodurre attività proprie dell'intelligenza umana o che comunque ne simulino il comportamento*. [34] Luciano Floridi, invece, non da una definizione precisa di intelligenza artificiale, ma prende inizialmente in esame la definizione secondo cui l'intelligenza artificiale è l'intelligenza mostrata dalle macchine, in contrasto però con l'intelligenza naturale mostrata agli esseri umani. Capiamo bene che questa definizione è poco utile. Lo stesso Floridi arriva a dire che l'IA non è un termine scientifico, ma un'espressione generica. Bisogna tenere presente poi che l'intelligenza artificiale prende in considerazione due settori, ovvero il settore ingegneristico e il settore cognitivo. Per quanto riguarda il primo settore, esso pone il suo interesse sulla riproduzione del comportamento intelligente. Oggi utilizziamo sempre più sistemi di IA per eseguire compiti che risulterebbero impossibili per intelligenza umana. Ecco che l'intelligenza artificiale riproduttiva ottiene sempre più risultati e sostituisce in vari contesti l'intelligenza umana. Per quanto riguarda invece il settore della scienza cognitiva, essa pone il suo centro sulla produzione dell'intelligenza, il quale rimane ancora un settore irrealizzato. Dopo queste considerazioni, rimane da comprendere il ruolo dell'essere umano di fronte a questi sistemi. Uno dei rischi più grandi è quello secondo cui gli esseri umani stanno diventando nuovi mezzi di produzione digitale. La questione è semplice, molto spesso l'IA necessita di capire ed interpretare ciò con cui entra a contatto, per cui ha bisogno di noi per svolgere il proprio compito. Questa tendenza prende il nome di "computazione basata sull'umano"[5]. Per comprendere meglio ciò di cui stiamo parlando, risulta necessario ricorrere ad un esempio. L'esempio che tratteremo riguarda Amazon, il quale descrive il tipo di sistema IA appena citato, come "intelligenza artificiale artificiale". Questo servizio consente ai richiedenti di una

anche i comportamenti, quali la capacità di decidere, attraverso la retroazione (feedback) o l'apprendimento automatico (machine learning), e la reazione a stimoli esterni. Per questi motivi, l'autore dice che siamo di fronte a macchine come noi (P. Moro, "Macchine come noi. Natura e limiti della soggettività robotica", in "Intelligenza artificiale. Il diritto, i diritti, l'etica", a cura di Ugo Ruffolo, Giuffrè, 2020, pagine 45-61.

[3]Enciclopedia Treccani.

[4]"L'intelligenza artificiale comprende un ampio insieme di ricerche e tecnologie diverse, accomunate dall'obbiettivo di realizzare sistemi artificiali capaci di comportamenti intelligenti*.". (*G. Sartor F. Lagioia*, "*Le decisioni algoritmiche tra etica e diritto*"*, in "Intelligenza artificiale. Il diritto, i diritti, l'etica", Giuffrè, a cura di Ugo Ruffolo, 2020, pagine 63-92).

[5]Esempio più celebre: un automa in grado di giocare a scacchi costruito alla fine del XVIII secolo. Era un automa falso però, perché al suo interno si nascondeva un giocatore umano che ne controllava le azioni meccaniche.

determinata prestazione di sfruttare l'intelligenza dei lavoratori umani, detti anche "fornitori", per realizzare compiti che richiedono l'intelligenza umana e che i computer non sono ancora in grado di realizzare. Il servizio consiste nel fatto che i fornitori possono sfogliare una lista di compiti da svolgere, sceglierne uno ed eseguirlo, in cambio di un compenso stabilito dal richiedente. Quindi la formula vincente, in questo caso, è macchina smart più intelligenza umana, uguale sistema ingegnoso. Il secondo esempio nel quale gli esseri umani stanno diventando sempre più parte è quel meccanismo che li vede come clienti influenzabili. Questo meccanismo, si colloca nell'ambito del settore pubblicitario. Per poter rendere il sistema più fluido, il settore pubblicitario ha bisogno di più informazioni possibili. Per fare questo è necessario uno scambio, fornendo sevizi gratuiti online. In cambio di questi, il settore pubblicitario riesce ad ottenere informazioni sui clienti. Questo tipo di lavoro, fa in modo che il cliente sia sempre più visto come un mezzo per arrivare ad un determinato fine. L'IA acquista perciò un ruolo cruciale, ritagliando, ottimizzando e decidendo molti processi. Diventa fondamentale in questo contesto, poter immaginare e prevedere come sarà il futuro dell'intelligenza artificiale e come sarà il nostro rapporto con essa, proprio per evitare di andare incontro a rischi o pericoli.

1.2 I PRINCIPI ETICI A FONDAMENTO DELL'INTELLIGENZA ARTIFICIALE

Luciano Floridi, nel suo libro "Etica dell'Intelligenza artificiale. Sviluppi, opportunità e sfide", si focalizza particolarmente sui principi etici dell'intelligenza artificiale. Data la grande portata di questo fenomeno e i notevoli progressi fatti da tali sistemi, in molti hanno cercato di proporre varie iniziative volte alla definizione dei principi da porre alla base dell'intelligenza artificiale, la quale deve essere vista da un punto di vista vantaggioso per l'uomo. Date queste innumerevoli iniziative, è facile andare incontro a ripetizioni e ad un eccessivo numero di principi. Quello che si deve cercare di fare è invece, provare a riunire questi principi. Questo può essere fatto guardando ai principi bioetici fondamentali, i quali sono: dignità umana, beneficenza, non maleficenza, autonomia e giustizia, dai quali poi è importante arrivare al principio di intellegibilità e responsabilità. Il primo principio è quello della dignità umana, considerata come valore intrinseco dell'essere umano. L'utilizzo dell'IA può essere uno strumento attraverso il quale poter avere nuovi mezzi per accrescere la dignità stessa della vita dell'uomo. L'IA però può essere un'arma a doppio taglio, poiché i sistemi che utilizzano tale intelligenza

possono portare alla nascita di nuove minacce nei confronti dell'integrità morale e fisica, nel momento in cui viene meno il valore intrinseco di ogni individuo. Da qui diventa indispensabile che l'uomo sia consapevole di relazionarsi ad una macchina e ne ottenga anche il controllo, poiché il fine ultimo è quello di poter migliorare l'agire umano e i suoi diritti. [6]Procediamo la nostra analisi, prendendo ora in esame il secondo principio, ovvero quello di beneficenza. Con riguardo a questo secondo principio le tecnologie di IA devono essere create a beneficio degli esseri umani. Il termine beneficienza, o per meglio dire "benessere", può essere definito in vari modi, ovvero: "lo sviluppo dell'IA dovrebbe in definitiva promuovere il benessere di tutte le creature senzienti", oppure "necessita di dare priorità al benessere umano come risultato in ogni design di sistema", ed infine può essere intesa nella maniera più semplice e chiara possibile, ovvero come "l'IA deve essere sviluppata per il bene comune e a beneficio dell'umanità". Quello che emerge, come denominatore comunque di tutte queste possibili definizioni è che l'IA deve essere sviluppata a beneficio dell'uomo e dell'ambiente che lo circonda. Il terzo principio viene definito come non maleficenza[7], il quale si occupa proprio di privacy e sicurezza. Questo principio ha a priori come funzione, quella di mettere in guardia dalle possibili conseguenze negative che possono derivare da un utilizzo eccessivo e sbagliato dei sistemi IA. Di conseguenza, risulta essere di particolare rilevanza il tema della privacy personale. Quindi, diventa necessario evitare usi impropri di questi sistemi ed è fondamentale che essi operino all'interno di limiti sicuri. In questo contesto, diventa fondamentale anche il concetto di responsabilità, poiché chi utilizza sistemi di IA dovrebbe riconoscere e assumersi le proprie responsabilità nel momento in cui opera in maniera scorretta. Ecco che allora, legato proprio al concetto di responsabilità, troviamo il quarto principio, cioè quello di autonomia. Si parla di autonomia perché quando decidiamo di utilizzare questi sistemi, inevitabilmente cediamo una parte del nostro potere decisionale proprio all'IA. Quindi parlare di autonomia in questo contesto,

[6]Questo principio non viene citato all'interno del libro di Luciano Floridi, ma viene citato da Lorenzo d'Avack nel suo saggio "La rivoluzione tecnologica e la nuova era digitale: problemi etici", in "Intelligenza Artificiale. Il diritto, i diritti, l'etica", Giuffrè, a cura di Ugo Ruffolo, 2020, pagine 3-28).

[7]Questo stesso principio viene citato anche da Lorenzo d'Avack, ma viene unito al principio di beneficenza; infatti, lui parla del principio di "Beneficienza e non maleficenza". Egli molto sinteticamente ci spiega come tali sistemi oltre a dover aiutare a migliorare il benessere dell'umanità, dovrebbero anche non danneggiare gli esseri umani e la società (L. D'Avack, "La rivoluzione tecnologica e la nuova era digitale: problemi etici", in "Intelligenza Artificiale. Il diritto, i diritti, l'etica", Giuffrè, a cura di Ugo Ruffolo, 2020, pagine 3-28).

significa trovare un equilibrio tra il processo decisionale guidato dagli esseri umani e quello guidato dall'IA [8]. Il rischio, in questo caso, riguarda proprio la crescita dell'*autonomia artificiale.* L'autonomia dell'IA non deve andare a compromettere l'autonomia umane nello stabilire i limiti e le norme. Ecco che il concetto di autonomia può essere riassunto in questo: deve essere promossa l'autonomia umana, gli esseri umani quindi devono mantenere il proprio potere decisionale, esercitando la libertà di scelta dove serve. Passiamo ora al principio successivo, ovvero il quinto, quello che riguarda la giustizia. La decisione di prendere decisioni o delegarle alla macchina, si collega proprio a questo principio di giustizia. L'IA deve essere sviluppa per promuovere la giustizia ed eliminare le discriminazioni, deve contribuire alla giustizia globale e alla parità nell'accedere ai benefici di tali tecnologie.[9] Ed infine l'IA deve aiutarci a promuovere la diversità e prevenire l'insorgenza di nuove minacce alla giustizia. Questi sono i principi base, ai quali si aggiunge poi, un ultimo principio fondamentale, ovvero quello dell'esplicabilità o intellegibilità. Quando si parla di questo principio, si fa chiaramente riferimento alla necessità di poter comprendere e di poter rendere conto dei processi decisionali dell'IA. Questo principio può essere racchiuso in due termini importanti, che troveremo spesso nel corso di questa trattazione, ovvero il termine trasparenza[10] e il termine responsabilità. [11] Come ben sappiamo, nella maggior parte dei casi, il funzionamento di questi sistemi e la loro struttura, è intellegibile o non comprensibile a chiunque, a parte agli studiosi esperti in materia. L'intellegibilità completa e fa da comune

[8]Secondo Lorenzo D'Avack, l'autonomia deve essere intesa come "rispetto dell'autodeterminazione e scelta delle persone" (L. D'Avack, "La rivoluzione tecnologica e la nuova era digitale: problemi etici", in "Intelligenza Artificiale. Il diritto, i diritti, l'etica", Giuffrè, a cura di Ugo Ruffolo, 2020, pagine 3-28).

[9]"Ciò implica la facilitazione ad un'educazione alle discipline digitali per acquisire abilità digitali in termini di competenze e motivazione all'uso delle tecnologie informatiche, in particolar modo nelle aree culturali e nei contesti sociali svantaggiati, così da evitare forme di marginalizzazione o discriminazione. Questa deve essere una lotta politica e sociale nel rispetto della *Carta dei diritti fondamentali dell'Unione Europea* che afferma il principio di uguaglianza di tutti i cittadini e della nostra *Costituzione* che riconosce pari dignità sociali.", D'Avac, "(L. D'Avack, "La rivoluzione tecnologica e la nuova era digitale: problemi etici", in "Intelligenza Artificiale. Il diritto, i diritti, l'etica", Giuffrè, a cura di Ugo Ruffolo, 2020, pagine 3-28).

[10]Secondo Sartor Giovanni e Lagioia Francesca può essere intesa anche come spiegabilità, poiché tutti i processi, i meccanismi e gli scopi devono essere comunicati apertamente e le decisioni degli algoritmi devono essere spiegabili agli interessati sia direttamente che indirettamente*.". (*G. Sartor F. Lagioia*, "*Le decisioni algoritmiche tra etica e diritto*"*, in "Intelligenza artificiale. Il diritto, i diritti, l'etica", Giuffrè, a cura di Ugo Ruffolo, 2020, pagine 63-92).

[11]Di questi due principi ne tratta anche Lorenzo d'Avack nel saggio "La rivoluzione tecnologica e la nuova era digitale: problemi etici", contenuto nel libro "Intelligenza Artificiale. Il diritto, i diritti, l'etica", a cura di Ugo Ruffolo, Giuffrè, 2020, pagine 3-28.

denominatore agli altri quattro principi, poiché se vogliamo che l'IA rappresenti un beneficio, è necessario che chiunque possa comprendere come essa opera, se opera per il nostro bene o se ci espone a rischi e pericoli. Se vogliamo poi, che l'IA promuova l'autonomia umana e non la limiti, la questione su chi deve decidere deve avere alla base la conoscenza dell'IA e bisogna poter sapere come essere agirebbe al nostro posto ed infine affinché l'IA possa essere giusta, è necessario poter comprendere sempre chi è da ritenere eticamente e legalmente responsabile di fronte a pericoli o esiti negativi e questo richiede che si conosca il sistema utilizzato. Questo quadro di principi etici, così come appena descritti, potrebbe essere utile come spazio all'interno del quale poter costruire nuove leggi e regole. Questo, a seguito di questa considerazione, può essere sia abilitante, ma anche vincolante, non in senso negativo perché ci dà modo di poter stabilire nuovi regolamenti che vada a limitare quei fenomeni come la criminalità online. Da questo quadro, sono derivati cinque documenti importanti, di cui ne cito due in particolare, per il loro collegamento con l'Unione Europea. Il primo documento deriva dal primo forum globale europeo sull'impatto sociale dell'IA, il quale poi è stato adottato per proporre alla commissione europea venti raccomandazioni concrete per "una società della buona IA", il quale è stato a sua volta adottato da "Le Linee guida etiche per l'IA affidabile ", le quali sono state pubblicate da un gruppo di esperti sull'IA della Commissione Europea. Il vero problema di oggi quindi, non è l'innovazione tecnologica, la quale come ben sappiamo è in costante evoluzione e cresce ad una velocità strabiliante e nella maggior parte dei casi è un vantaggio, non uno svantaggio, ma la governance del digitale. Parliamo di governance, o meglio di *governance digitale*, come viene denominata da Floridi. È importante dare subito una definizione di questo nuovo termine. La *governance digitale* è la pratica di stabilire e attuare politiche, procedure e standard per il corretto sviluppo, utilizzo e gestione della tecnologia. In altre parole, la *governance digitale* è l'insieme delle raccomandazioni e linee guida adottate nei confronti dei sistemi di IA. Oltre alla governance però, dobbiamo tenere sempre presente la regolazione, chiamata da Floridi *regolazione digitale*. Governance e regolazione non sono la stessa cosa, ma molto spesso si sovrappongono tra di loro. Ecco che allora, possiamo parlare di governance e regolazione, riferendoci all'insieme delle leggi e norme applicate ed elaborate, al fine di andare a regolamentare i soggetti che forniscono e utilizzano sistemi di intelligenza artificiale. Un esempio importante di questo incontro tra governance e regolazione è il

Regolamento generale in materia di protezione di dati personali. Tutto questo si intreccia poi con l'etica già citata, la quale si occupa proprio di andare a studiare e valutare i problemi morali legati alla circolazione dei dati e delle informazioni, agli algoritmi e le relative pratiche. Va precisato che quando parliamo di studio dei dati e informazioni ci riferiamo anche allo studio del trattamento, della registrazione, della cura, della diffusione, condivisione ed utilizzo dei dati stessi. In questo contesto attuale e appena delineato, l'etica acquista un'importanza fondamentale, poiché essa, definendo ciò che è socialmente accettabile o preferibile e ciò che di contro non lo è, aiuta la legislazione e le norme a formarsi e costruisce una sorta di spazio all'interno del quale creare queste nuove regole. Facendo un passo indietro però, ciò che è altrettanto rilevante in tutto questo è la *compliance*, ovvero la conformità alle norme, che è cioè la relazione attraverso la quale la regolazione modella la governance. La quale comunque rimane insufficiente senza l'etica, che ci dà i confini entro cui poterci muovere. Tutto questo spiega anche la decisione del Garante europeo per la protezione dei dati personali di creare nel 2015 il Comitato consultivo etico, il quale ha il compito di andare ad analizzare le nuove sfide etiche causate dallo sviluppo del mondo digitale e dalla normativa vigente, soprattutto per quanto riguarda la normativa in materia di protezione dei dati personali.

1.3 IL CONCETTO DI SOFT ETHICS E IL CONCETTO DI GOVERNANCE

Dopo aver parlato dei principi etici dell'IA, dobbiamo precisare una distinzione tra hard ethics e soft ethics. Prima di fare questo, è necessario distinguere tre diversi campi: meta-etica, teorie morali ed etica applicata. La meta-etica si occupa dei pilastri del sistema normativo, dei concetti chiave di giustizia e ingiustizia. Le teorie morali, invece, fanno riferimento ai vari modi in cui i filosofi hanno definito le nozioni di obbligatorio, proibito e permesso. Infine, l'etica applicata concerne invece i dilemmi morali che nascono in uno specifico settore dell'esperienza. Questa distinzione ci serve per capire meglio la distinzione che viene fatta tra hard ethics e soft ethics. Per aiutarci ancora di più, in primo luogo possiamo paragonarla in parte alla distinzione che viene fatto in diritto, tra soft law e hard law, anche se in realtà quando parliamo di etica la distinzione non è così netta poiché, molto spesso le due realtà si intrecciano fra loro. Quando parliamo di hard ethics facciamo riferimento ai valori, diritti, responsabilità, ovvero nel momento in cui l'etica

contribuisce a costruire il diritto, siamo di fronte all'hard ethics[12]. La soft ethics, invece, comprende lo stesso ambito normativo dell'hard ethics, ma lo fa prendendo in considerazione quello che dovrebbe o non dovrebbe essere fatto a prescindere dalla normativa vigente, tuttavia senza andare contro la normativa stessa. Da questo deriva che entrambi le due anime dell'etica, hanno come presupposto fondamentale il principio secondo cui il dovere implica il potere. In maniera più esplicita, questo vuole dire che un soggetto ha il dovere di compiere una determinata azione, se alla base ha la possibilità di poterla mettere in atto. Bisogna sempre tenere presente che, quando parliamo di Unione Europea e ci troviamo di fronte ad un approccio etico, essa pone sempre alla base di esso tre atti emanati dall'Unione, che tutt'oggi stanno alla base delle nostre normative. Questi tre atti sono la Dichiarazione Universale dei diritti dell'uomo, la Convenzione europea dei diritti dell'uomo e la Carta dei diritti fondamentali dell'Unione Europea. Quindi lo spazio ne risulta in un certo senso limitato, o comunque circoscritto. Come ben sappiamo la normativa, anche quella Europea è necessaria, ma molte volte non basta, perciò diventa importante prende in considerazione l'etica, la quale può essere utilizzata. Se, dopo averla presa in considerazione, viene utilizzata in maniera corretta può essere un aiuto per sfruttare al meglio le innovazioni digitali. In questo senso, torna utile prendere già in considerazione, in parte, una normativa, che analizzeremo successivamente, ovvero il GDPR. È opportuno prendere in considerazione questo documento, in modo da poter capire come normativa ed etica possono intrecciarsi e aiutarsi tra loro. Iniziamo, prendendo in considerazione cinque elementi fondamentali. In primo luogo, dobbiamo tenere presenti le implicazioni etiche, giuridiche e sociali del GDPR, ad esempio nei confronti delle organizzazioni. Questa normativa è stata costruita per armonizzare le norme sulla protezione dei dati personali in tutta l'unione Europea, per proteggere e far rispettare la privacy dei dati dei cittadini europei, a prescindere da dove vivano, ed infine per migliore il modo in cui, questo tema della privacy e della sua protezione, viene affrontato dalle organizzazioni. Il secondo elemento è il fatto che il GDPR ha novantanove articoli. Nonostante il numero di articoli, come accade la maggior parte delle

[12]Di questa distinzione ne parla anche Ugo Pagallo, il quale specifica come l'hard ethics riguardi la discussione su questioni riguardanti la meta-etica, su ciò che va proibito o permesso, in rapporto ai problemi unici delle tecnologie "emergenti", quindi etica applicata. La soft ethics invece ha il compito di completare o irrobustire il quadro giuridico già esistente ("Etica e diritto dell'Intelligenza Artificiale nella governance del digitale: il Middle-out Approach", in "Intelligenza Artificiale: il diritto, i diritti, l'etica", a cura di Ugo Ruffolo, Giuffrè, 2020, pagine 29-44).

volte, anche qui la normativa non copre tutto, ma lascia delle zone grigie. Queste zone grigie sono zone di incertezza normativa, che portano o possono portare ad interpretazioni e che nel momento in cui vengono applicate a circostanze nuove, mai viste, richiedono un passo in avanti, un aggiornamento. Questo caso appena citato, è molto frequente nell'ambito dell'Intelligenza Artificiale, data la sua continua e veloce evoluzione. Ecco che, il legislatore, per agevolare la comprensione del significato degli articoli ha deciso di introdurre la normativa con ben centosettantatre "considerando". Questi considerando sono il nostro terzo elemento da noi preso in considerazione, i quali hanno il compito di spiegare le ragioni alla base dell'atto emanato, ma essi non sono vincolanti e non dovrebbero avere un linguaggio normativo, proprio per il fatto che hanno la funzione di spiegazione. Solitamente, i considerando presenti negli atti emanati dall'Unione, compresi quelli del GDRP, vengono presi in considerazione dalla Corte di Giustizia per interpretare una direttiva, un regolamento e adottare una decisione nell'ambito di una controversia concreta. Nel caso del GDPR però, è importante precisare che questi considerando vengono presi in considerazione non solo dalla Corte di Giustizia, ma anche dal Comitato per la protezione dei dati personali, volto a garantire la corretta applicazione della normativa riguardante la privacy all'interno del territorio europeo. Proseguendo poi, il quarto elemento è caratterizzato dal fatto che anche i considerando richiedono un'interpretazione. Questa interpretazione di cui necessitano i considerando, in parte è fornita da un quadro etico, che aiuta ad interpretare e comprendere i considerando. Infine, il quinto ed ultimo elemento è caratterizzato dal fatto che gli articoli e i considerando sono il frutto di un lungo processo di negoziazione tra il Parlamento europeo, il Consiglio europeo e la commissione europea, il quale ha poi portato ad una proposta comune. In altre parole, questo quinto elemento consiste nella prospettiva che ha portato all'elaborazione del GDPR. In questo quinto punto l'hard ethics acquista un ruolo importante. L'hard ethics è l'elemento etico che ha guidato e motivato il processo che ha condotto all'elaborazione della legge, più precisamente al GDPR, mentre la soft ethics è alla base dei considerando. Tutto questo per dire che molte volte è necessario, prima di promuovere un gruppo di norma, avere alla base un approccio etico che permetta di sviluppare una IA che vada a promuovere il bene della società. L'etica, oltre ad essere alla base e precedente alla normativa, è anche successiva perché aiuta l'interpretazione della normativa stessa. Come ben sappiamo ormai a fianco allo sviluppo dell'IA e della

tecnologia, c'è anche la possibile comparsa o la manifestazione di nuovi rischi, perciò diventa fondamentale in questo contesto trovare un bilanciamento tra i benefici e i rischi, quindi evitare che queste tecnologie vengano utilizzate in maniera impropria o vengano utilizzate in maniera dannosa. È proprio in questa realtà che un approccio non solo normativo, ma anche etico risulta necessario e utile. I due vantaggi derivanti dall'utilizzo di un approccio etico sono i seguenti: in primo luogo, la soft ethics, può fornire una strategia basata sulle opportunità, perché consente ai soggetti di sfruttare il valore delle tecnologie digitali; l'hard ethics, da una soluzione alla gestione del rischio, poiché consente alle organizzazioni di anticipare ed evitare errori, che potrebbero costare molto cari ai soggetti utilizzatori. Tutto questo, però può funzionare solamente se abbiamo anche una legislazione adeguata.

1.4 L'INTELLIGENZA ARTIFICIALE A BENEFICIO DELLA SOCIETA'

Questo concetto, citato nel titolo, sta prendendo sempre più piede. Alla base ci sono sette fattori, i quali sono: falsificabilità e implementazione incrementale, garanzie contro la manipolazione, intervento contestualizzato in ragione del destinatario, spiegazione in ragione del destinatario e trasparenza, tutela della privacy [13] , [14][15] e consenso dell'interessato[16], equità e semantizzazione adatta all'umano. Partiamo con l'analisi del primo fattore, il quale riguarda l'affidabilità, requisito essenziale affinché la tecnologia

[13]Legato alla privacy, troviamo il concetto di big data, il quale indica la quantità di informazioni che possono essere raccolte in modo sempre più veloce ("Riflessioni su intelligenza artificiale e protezione dei dati personali", in "Intelligenza artificiale. Il diritto, i diritti, l'etica", a cura di Ugo Ruffolo, Giuffrè, 2020, pagine 237-250).

[14]Giusella Finocchiaro definisce i dati con l'espressione "nuovo petrolio", poiché costituiscono la nuova risorsa dell'economia digitale ("Riflessioni su intelligenza artificiale e protezione dei dati personali", in "Intelligenza artificiale. Il diritto, i diritti, l'etica", a cura di Ugo Ruffolo, Giuffrè, 2020, pagine 237-250).

[15]Del tema privacy in rapporto alle nuove tecnologie, ne tratta già Anna Chiara Zanuzzi, nel suo saggio "Internet of things e privacy. Sicurezza e autodeterminazione informativa, libro "Tecnodiritto. Temi e problemi di informatica e robotica giuridica", a cura di Paolo Moro, Claudio Sarra, FrancoAngeli, 2017, pagine 99-120, e Claudio Sarra nel suo saggio "Business Intelligence ed esigenze di tutela: criticità del c.d. Data Mining", contenuti nel libro "Tecnodiritto. Temi e problemi di informatica e robotica giuridica", a cura di Paolo Moro, Claudio Sarra, FrancoAngeli, 2017.

[16]Questa, è la questione etica principale, secondo Lorenzo D'Avack. Infatti, emerge sempre di più l'esigenza che gli utenti digitali possano avere un controllo nella gestione dei dati, a partire proprio dal consenso informato. Tale consenso deve sempre essere modificabile, ovvero l'interessato deve poterlo revocare, rettificare e chiedere la cancellazione dei dati raccolti ("La rivoluzione tecnologica e la nuova era digitale: problemi etici", contenuto nel libro "Intelligenza Artificiale. Il diritto, i diritti, l'etica", a cura di Ugo Ruffolo, Giuffrè, 2020, pagine 3-28).

possa essere sviluppata per il bene sociale. Sorge spontaneo allora chiedersi cosa c'entri l'affidabilità con la falsificabilità. La falsificabilità implica la specificazione e la possibilità di verifica empirica dei requisiti richiesti. La sicurezza rientra tra questi requisiti critici, il quale ormai è un requisito ovvio. Quindi un sistema che è affidabile dovrebbe essere falsificabile, cioè la sicurezza di tale sistema è specificata e verificabile. Senza questa falsificabilità il sistema non dovrebbe essere considerato affidabile, ecco perché la falsificabilità costituisce uno dei fattori cruciali per un'intelligenza artificiale sviluppata per il benessere sociale. È anche vero però che questa condizione può essere presente all'inizio, ma poi non esserci più, ecco perché la falsificabilità dovrebbe essere verificata ciclicamente. Quindi è importante la verifica fatta in maniera ciclica e i sistemi devono essere testati nel mondo reale per garantire il rispetto della falsificabilità. Il secondo fattore è quello che riguarda le garanzie contro la manipolazione. È molto diffuso l'utilizzo dell'IA per andare a prevedere modelli o tendenze future. Di fronte a questo utilizzo i sistemi di IA vanno incontro a due rischi: la manipolazione dei dati e l'eccessiva dipendenza da indicatori non causali. Quello che a noi interessa in questo contesto è quello che riguarda i dati che vengono forniti da questi sistemi. Tale problema non è un problema nuovo, ma in questo caso può portare ad esiti che vanno a violare il principio di giustizia. Ciò che sta alla base di questo è il fatto che nel momento in cui le informazioni che portano ad un determinato risultato sono note, allora un agente con tali informazioni può andare a modificare più facilmente una variabile predittiva. Con l'IA questo si complica, a causa della dimensione dell'IA stessa. Nel momento in cui poi, si possono modificare i dati, si riduce di conseguenza il potere predittivo del modello. Allo stesso tempo però, può sorgere un altro problema, cioè se ci si focalizza troppo sui dati non casuali, i quali sono correlati con, ma non sono la causa di un fenomeno, si può andare a distogliere l'attenzione dal contesto in cui il designer sta cercando di intervenire. Terzo fattore è l'intervento contestualizzato in ragione del destinatario. È fondamentale che il software possa intervenire nella vita degli utenti, ma senza privarli della propria autonomia. Qui entrano in gioco cinque dimensioni rilevanti per intervento contestualizzato in ragione del destinatario. Queste cinque dimensioni sono: 1) le caratteristiche individuali del destinatario dell'intervento; 2) le modalità di coordinamento tra il destinatario del sistema e il sistema stesso; 3) il significato o la finalità dell'intervento; 4) gli effetti dell'intervento; 5) la possibilità di disporre di opzioni.

Per quanto riguarda quest'ultima dimensione, questa possibilità significa che il destinatario, può liberamente scegliere se ignorare i consigli offerti o indirizzare il processo e richiedere un intervento diverso e più adatto alle sue esigenze. Il quarto elemento riguarda il campo della trasparenza, o almeno così possiamo sintetizzarlo. Questo perché le applicazioni IA devono essere disegnate in maniera da rendere spiegabili le operazioni e i risultati di tali sistemi e appunto trasparenti i loro scopi. Questi due requisiti essenziali, sono anche collegati tra di loro, perché le operazioni e i risultati dei sistemi riflettono gli scopi stessi dei designer umani. Questa trasparenza degli obbiettivi è alla base di altre garanzie riguardanti la protezione e può contribuire ad assicurare il rispetto della normativa stessa. Procedendo con la nostra analisi, passiamo al quinto settore, il quale riguarda proprio la privacy. Floridi, nel suo libro tratta di questo settore dicendo che è l'elemento con la letteratura più voluminosa e anche questo ci fa capire quanto risulti ancora più importante oggi soffermarci su questo argomento. La privacy è considerata una delle condizioni essenziali per la sicurezza e la coesione sociale. La sicurezza può essere compromessa, infatti, nel momento in cui uno stato o un designer malintenzionato ottiene il controllo sugli individui tramite la violazione della loro privacy. Il rispetto della privacy poi è una condizione essenziale per il rispetto della dignità dell'individuo stesso, questo perché le informazioni personali possono essere considerate come elementi che costituiscono l'individuo; quindi, la sottrazione di dati senza il consenso può costituire violazione della dignità umana. Alla privacy, si collega quindi il consenso degli utenti per l'utilizzo di dati personali[17]. Nel momento in cui, però siamo di fronte a situazioni di emergenza, quali per esempio la pandemia da Covid 19, l'obbligo del consenso può subire delle deroghe. Il consenso, quindi, è alla base della privacy, ma il consenso richiesto varia a seconda del contesto in cui viene prestato. Parlando dell'ambito sanitario, si può utilizzare una soglia di consenso cosiddetto presunto. In altre circostanze invece ricorrere ad un consenso di tipo informato, è la scelta più appropriata. Esiste poi una forma di consenso cosiddetta "consenso dinamico", la quale è ancora in evoluzione e in base alla quale gli individui possono andare a monitorare e regolare le

[17]Voglio fare ancora una precisazione riguardo a questo tema. Giusella Finocchiraro, precisa che il titolare del trattamento dati personali deve assicurare la qualità dei dati trattati non solo al momento della loro raccolta, ma anche nel corso del trattamento stesso attraverso un monitoraggio continuo ("Riflessioni su intelligenza artificiale e protezione dei dati personali", in "Intelligenza artificiale. Il diritto, i diritti, l'etica", a cura di Ugo Ruffolo, Giuffrè, 2020, pagine 237-250).

proprie preferenze sulla privacy e il livello stesso. Il consenso più problematico, però rimane quello riguardante lo spazio online. Gli utenti, molto spesso, non hanno la possibilità di scegliere e nel momento in cui accedono ad un servizio online sono posti di fronte all'alternativa "prendere o lasciare", come dice Floridi. Questa mancanza di possibilità di scelta e di conseguenza di protezione o consenso per usi secondari dei dati personali, porta allo sviluppo di software problematici. Per spiegare meglio questo concetto ho deciso di portarne un esempio. Un recente studio ha utilizzato immagini di volti caricati su un sito di incontri per addestrare un sistema di IA a riconoscere il genere di qualcuno sulla sola base di un esiguo numero di foto. Questo studio è stato approvato dal comitato etico, ma ha sollevato notevoli problematiche dal punto di vista del consenso, poiché non è concepibile che questi utenti potessero o volessero necessariamente dare il consenso per l'utilizzo dei loro dati personali. La privacy non è un problema nuovo e questo ormai lo si sa bene, ma rapportato all'intelligenza artificiale diventa un problema centrale, che ne accresce il suo significato dal punto di vista etico e normativo, e diventa centrale il tema del consenso. Da questo ne deriva che i designer devono necessariamente rispettare la soglia di consenso stabilita per il trattamento della raccolta dei dati personali. Il sesto fattore riguarda il concetto di equità. Il settimo ed ultimo fattore ci parla poi di semantizzazione[18] adatta all'uomo. Quest'ultimo fattore è fondamentale per mantenere e promuovere l'autonomia umana. Questo in ragione dell'IA può portare ad un primo problema. Può accadere che il sistema vada a definire la semantizzazione in modo diverso rispetto alle nostre scelte. Per esempio: utilizziamo un software per andare a dare una definizione del termine "violazione", che alla base ha un'applicazione che prevede il significato giuridico di tale termine. Se utilizziamo solamente questo software, però si finisce per limitare il ruolo dei giudici e della giustizia. In questo modo si limita la loro autonomia nel dare un significato alle cose, nel semantizzare. Il secondo problema è quello per cui il sistema non è in grado di definire tutti i significati e i sensi di una determinata cosa. La soluzione a questi due problemi, come ci spiega Floridi, è quella di fare una divisione tra i compiti che dovrebbero o non dovrebbero essere delegati ad un sistema di IA. I sistemi di IA, dovrebbero essere utilizzati per aiutare l'uomo alla definizione di significati, ma non per fornirla loro in maniera autonoma.

[18]Semantizzare: dare significato o conferire senso a qualcosa.

1.5 IL PERCORSO VERSO LA PROPOSTA DI REGOLAMENTO EUROPEO

Dopo questa analisi sull'Intelligenza Artificiale, sull'etica alla base di essa e su come può essere utile all'uomo se utilizzata nella maniera corretta, passiamo alla normativa che deve stare alla base dell'IA. Come bene sappiamo non c'è un quadro normativo specifico riguardante l'IA, ma c'è stata una proposta dell'Unione Europea, che tratteremo nel prossimo capitolo. Adesso vorrei soffermarmi su quali sono stati i vari passi che hanno portato alla scrittura di questo regolamento.[19] Il primo passo è stato avviato dall'emanazione delle "Linee guida etiche per un'IA affidabile", il secondo passo è stata l'emanazione del "Libro bianco sull'IA".[20] Documenti emanati sempre dall'Unione Europea.[21] Partiamo con un'analisi del primo documento in questione. Questo primo documento è stato emanato da una commissione di esperti sull'IA, la quale è stata istituita già nel giugno del 2018. Il documento è stato reso pubblico il giorno 8 aprile 2019. Tale documento prevede che alla base dello sviluppo dell'IA ci siano tre elementi essenziali, i quali sono: legalità, etica e robustezza. Con legalità si fa riferimento al fatto che l'intelligenza Artificiale deve sottostare e rispettare tutte le leggi e i regolamenti applicabili. Con l'etica si intende che l'IA deve assicurare l'adesione ai principi e valori etici. Infine, robustezza che deve essere considerata sia dal punto di vista etico, ma anche sociale, perché l'IA ci espone a nuovi rischi e danni. Ciascuna di queste tre componenti è necessaria, ma non sufficiente da sola allo sviluppo di un'IA affidabile, infatti le tre

[19]Paolo Moro, sottolinea come la diffusione dell'Ia ha portato l'Unione Europe a non poter più rimandare l'idea di dover iniziare a prendere in considerazione la possibilità di emanare un regolamento che trattasse proprio dei sistemi di Intelligenza Artificiale ("Intelligenza artificiale e tecnodiritto. Fondamentui etici ed innovazione legislativa", in "Etica, Diritto e Tecnologia, a cura di Paolo Moro, FrancoAngeli, 2021, pagine 7-24).

[20]Alla base di queste due normative c'è il principio di precauzione. Andrea Amadei, si sofferma su tale principio specificando come questo venga invocato anche nell'ambito dell' IA a causa dell'indecifrabilità della stessa e nell'incertezza che troviamo nell'individuare e prevenire possibili comportamenti emergenti e dannosi provenienti da questi sistemi ("La governance dell'Intelligenza Artificiale: profili e prospettive di diritto dell'Unione Europea", in "Intelligenza artificiale. Il diritto, i diritti, l'etica", a cura di Ugo Ruffolo, Giuffrè, 2020, pagine 571-590.

[21]Ci tengo a precisare che prima di questi due documenti importanti l'Unione ha fatto vari piccoli passi. Paolo Moro, ci illustra questi piccoli passaggi. Per prima cosa nella premessa della risoluzione del 16 febbraio 2017, il Parlamento ha constatato che l'umanità si trovava ormai di fronte a varie manifestazioni di IA, le quali stavano ormai dando il via a una rivoluzione industriale. Un altro piccolo passo è stato quello di andare ad istituire l'Alleanza europea per l'intelligenza artificiale. Altro passo è stato quello avvenuto nell'aprile 2019, quando la Commissione Europea ha approvato i requisiti fondamentali stabiliti negli orientamenti etici di un gruppo di esperti di altro livello sull'Intelligenza Artificiale("Intelligenza artificiale e tecnodiritto. Fondamentui etici ed innovazione legislativa", in "Etica, Diritto e Tecnologia, a cura di Paolo Moro, FrancoAngeli, 2021, pagine 7-24).

.

componenti dovrebbero cooperare in maniera armonica e sovrapporsi fra di loro. Il primo capitolo riguarda proprio i principi etici, i quali sono quelli di cui abbiamo già parlato precedentemente. In più ci viene detto che nel momento in cui si sviluppano questi sistemi è necessario fare particolare attenzione a tutte quelle situazioni in cui vengono coinvolti anche gruppi più vulnerabili, quali bambini o persone con disabilità, a quelle situazioni in cui vengono coinvolti anche gruppi storicamente più svantaggiati o a rischio di esclusione e quelle situazioni riguardanti uno squilibrio di potere, quali per esempio il rapporto tra il datore di lavoro e il lavoratore o tra imprese e consumatori. È importante poi saper riconoscere e tenere presente che i sistemi di IA, offrono sì vantaggi concreti alle persone e alla società, ma comportano anche dei rischi e possono portare ad avere effetti negativi, i quali possono risultare difficili da prevedere, individuare e misurare. A questo punto, se necessario è fondamentale adottare provvedimenti adeguati al fine di attenuare tali rischi, sempre proporzionanti però alla portata dei rischi stessi. Il secondo capitolo, si occupa di darci indicazioni su come realizzare un'IA affidabile, andando ad elencare sette requisiti che i sistemi di IA devono andare a soddisfare. Questi sette requisiti sono simili a quelli di cui abbiamo già parlato in precedenza. Inoltre, sempre questo secondo capitolo sottolinea come sia importante andare a favorire e sostenere la ricerca e l'innovazione dei sistemi di IA e del raggiungimento del rispetto dei requisiti richiesti. È necessario, inoltre, andare ad informare in maniera chiara e proattiva i portatori di interessi in merito alle capacità e ai limiti del sistema di IA, creando così aspettative realiste circa i modi in cui i requisiti vengono attuati. Bisogna agevolare la tracciabilità e la verificabilità dei sistemi di IA, in particolare in contesti o situazioni critiche. In tutto questo, si deve coinvolgere i portatori di interessi durante l'intero ciclo di vita del sistema di IA, promuovendo la formazione e l'istruzione, in modo che i portatori di interessi siano formati e informati in merito ad un'IA affidabile. Il terzo capitolo, infine, ci indica in maniera chiara quello che è necessario fare. In primo luogo, è necessario adottare una lista di controllo per poter valutare l'affidabilità nelle fasi di sviluppo, distribuzione o utilizzo dei sistemi di IA e adattarla allo specifico caso d'uso in cui il sistema vien applicato. In secondo luogo, è necessario tenere presente che questa lista di controllo non sarà mai esaustiva. L'IA affidabile non è una questione di caselle da spuntare, ma un processo continuo di individuazione e attuazione dei requisiti, di valutazione di soluzioni e miglioramento dei risultati ottenuti durante l'intero ciclo di vita

dell'IA. Il presente documento specifica come lo scopo di esso sia proprio quello di fornire una base per la costruzione di un IA affidabile e che i presenti orientamenti non intendono sostituire azioni politiche o regolamentazione attuali o future e non hanno nemmeno lo scopo di andare a scoraggiarne l'adozione. Questo intervento deve essere considerato come un intervento vivo da rivedere ed aggiornare nel corso del tempo, al fine di andare a garantire la costante pertinenza al passo con le evoluzioni tecnologiche, i nostri ambienti sociali e la nostra conoscenza. Infine, tale documento ha lo scopo di essere punto di partenza per una discussione riguardante proprio un'IA affidabile per l'Europa. Nella parte finale vediamo come il comitato ha deciso di fornire anche una serie di esempi per un'IA affidabile e allo stesso tempo ha fornito anche una serie di esempi riguardanti le preoccupazioni che l'IA ha destato. Ne cito solo due: *identificazione e tracciamento degli individui* e *sistemi IA nascosti.* L'IA offre la possibilità ad organismi pubblici e privati di identificare in modo sempre più efficiente le singole persone. Gli esempi di una tecnologia di questo tipo sono: i sistemi di riconoscimento facciale o altri metodi di identificazione che vanno ad utilizzare dati biometrici, quali, per citarne uno, il rilevamento automatico della voce. Questa identificazione automatica solleva grande preoccupazione sia dal punto di vista etico, sia dal punto di vista giuridico, poiché può portare ad effetti non previsti e non controllabili dal punto di vista sociale e psicologico. Per salvaguardare l'autonomia dei cittadini, risulta pertanto necessario ricorre a tecniche di controllo dell'IA, andando a definire in maniera trasparente se, quando e come l'IA può essere utilizzata per l'identificazione automatica degli individui e andare a differenziare quando siamo di fronte all'identificazione, da quando siamo di fronte alla sua tracciatura e localizzazione e tra la sorveglianza mirata e sorveglianza di massa. Questo diventa fondamentale per ottenere un'IA affidabile. L'applicazione di queste tecnologie deve necessariamente essere motivata dal diritto vigente e se la base giuridica di tale attività è rappresentata dal consenso, devono essere sviluppati mezzi pratici che permettono di dare un consenso verificato. Tutto questo viene applicato anche nei confronti dei dati personali "anonimi" che possono essere ri-personalizzati. Invece, per quanto riguarda i sistemi di IA nascosti, gli individui hanno il diritto di sapere sempre se sono di fronte ad un sistema di IA e se stanno interagendo con lui. Queste informazioni, spetta comunicarle agli operatori del settore dell'IA. Essi devono garantire che gli individui siano consapevoli del fatto che stanno interagendo con un sistema di IA o che

possono chiedere informazioni in merito e decidere se approvare o meno tale interazione. In conclusione, tale intervento, si sofferma sul consigliare un approccio basato sul rischio nel quale vadano tenute in considerazione anche le preoccupazioni che riguardano il lungo periodo e i possibili prossimi passi evolutivi dell'IA e che questi temi vengano riesaminati e tenuti sottocchio in maniera regolare. Dopo questo documento, passiamo al "Libro bianco sull'IA". Tale libro inizia dando una definizione di Intelligenza Artificiale. In questo documento viene sottolineato come l'IA può diventare un leader mondiale nell'innovazione nell'economia dei dati e nelle sue applicazioni. L'unione può quindi sviluppare "un'ecosistema di IA", in grado di fornire una serie di vantaggi:

- Ai cittadini, i quali potranno usufruire di nuovi vantaggi, quali per esempio una migliore assistenza sanitaria, sistemi di trasporto più sicuri, servizi pubblici migliore, ecc…
- Le imprese potranno, per esempio, avvalersi di nuove generazioni di prodotti e servizi nei settori in cui l'Unione è particolarmente forte, quali per esempio i macchinari, il trasporto, cybersicurezza, agricolture, ecc…
- L'interesse pubblico, in particolare i servizi di questo genere potranno avere benefici, come ad esempio la riduzione dei costi di fornitura dei servizi, migliore sostenibilità dei prodotti e migliore sicurezza dei cittadini dando alle forze dell'ordine strumenti più appropriati, ovviamente con adeguate garanzie nei confronti dei cittadini circa i loro diritti e le loro libertà.

Dopo questa introduzione il libro prosegue parlando di coordinazione e collaborazione tra gli stati membri, parlando di nuovi rischi, nuovi vantaggi e di come poter sfruttare l'IA al meglio. Il capitolo sul quale volevo soffermarmi è quello che riguarda la legislazione. Alla base di tutto ci sono una serie di normative che riguardano la protezione dei diritti fondamentali, dei diritti dei consumatori e in materia di sicurezza dei prodotti e responsabilità[22]. La commissione suggerisce che il quadro legislativo possa essere

[22] Giusella Finocchiaro suggerisce due alternative in materia di responsabilità. La prima consiste nell'adottare una disciplina sulla responsabilità basata sulla accountability, la quale impone al titolare del trattamento, da un lato, di adottare misure giuridiche, organizzative e tecniche volte alla protezione dei dati personali e dall'altro di doverne dimostrare l'efficacia e l'attuazione. L'accountability opera quindi su due livelli: l'attuazione di misure e procedura e la conservazione delle relative prove. La seconda alternative, ci suggerisce di andare a prevedere meccanismi di attribuzione della locazione del costo del danno cagionato su quei soggetti che potrebbero essere responsabili ("Riflessioni su intelligenza artificiale e protezione dei

migliorato per andare ad affrontare situazioni e i rischi di cui ora parlerò. Uno dei rischi riguarda l'effettiva applicazione e rispetto della normativa nazionale e dell'UE in vigore, questo perché molto spesso le caratteristiche stesse dell'IA rendono difficile garantire la corretta applicazione e il rispetto della normativa nazionale e europea. Molto spesso poi, ci si trova di fronte all'opacità dell'IA, la quale rende difficile individuare e dimostrare eventuali violazioni delle normative, diventa difficile attribuire le responsabilità e andare a soddisfare le condizioni per chiedere un risarcimento. Quindi risulta necessario adeguare o chiarire la legislazione in vigore. Successivamente, un aspetto essenziale è quello riguardante i limiti dell'ambito di applicazione della legislazione dell'UE vigente in materia di immissione nel mercato di prodotti e servizi. La normativa vigente, si applica ai prodotti, ma non ai servizi, per cui in linea di principio non si applica neanche ai servizi basati sull'IA. Poi si parla di funzionalità mutevole dei sistemi di IA. L'integrazione del software, compresa l'IA, nei vari prodotti può andare a modificare il funzionamento del prodotto stesso e dei sistemi durante il loro ciclo di vita. Questo vale, principalmente, per tutti quei sistemi che richiedono continui aggiornamenti del software che si basano sull'apprendimento automatico. Questo può portare a rischi nuovi che non erano presenti quando il sistema è stato immesso sul mercato. Altro tema poi è quello che riguarda l'incertezza in merito all'attribuzione delle responsabilità tra i diversi operatori economici lungo la catena di approvvigionamento: la legislazione UE in materia di sicurezza del prodotto attribuisce al fabbricante la responsabilità del prodotto immesso nel mercato e dei suoi componenti. Il rischio è quello che in alcuni casi le norme possano risultare poco chiare ed inoltre la legislazione UE in merito all'immissione dei prodotti difettosi lascia alle disposizioni nazionali il compito di andare a disciplinare la responsabilità di altri soggetti presenti nella catena dell'approvvigionamento. Ultimo rischio, riguarda l'evoluzione del concetto di sicurezza. L'uso dei sistemi di IA nei prodotti e nei servizi può portare a rischi nuovi che la legislazione UE non ha ancora preso in considerazione e affrontato in maniera esplicita. Questi rischi possono essere collegati a minacce informatiche, possono rientrare nell'ambito della sicurezza personale, ecc… Tali rischi possono essere presenti nel momento di immissione dei sistemi nel mercato o apparire a seguito di aggiornamenti. L'Unione dovrebbe avvalersi quindi degli strumenti a sua

dati personali", in "Intelligenza artificiale. Il diritto, i diritti, l'etica", a cura di Ugo Ruffolo, Giuffrè, 2020, pagine 237-250).

disposizione sui potenziali rischi connessi all'applicazione dell'IA. La commissione ha ritenuto che un futuro quadro normativo dell'IA debba essere a carico dell'operatore o degli operatori che si trovano nella posizione migliore per affrontare i rischi potenziali; quindi, la responsabilità è nei confronti di chi produce e immette il sistema di IA nel mercato. Oltre a chi riferire la responsabilità, bisogna definire l'ambito geografico di applicazione. Per la Commissione, è necessario che le norme future siano applicabili a tutti gli operatori economici interessati, i quali forniscono prodotti o servizi basati sull'Intelligenza Artificiale, all'interno dell'Unione Europea, a prescindere dal fatto che siano stabiliti o meno nell'Unione, in caso contrario gli obbiettivi dell'intervento legislativo potrebbero non essere riassunti a pieno titolo.

2 INTELLIGENZA ARTIFICIALE E DIRITTI DEI LAVORATORI

2.1 DEFINIZIONE DI INTELLIGENZA ARTIFICIALE SECONDO L'UNIONE EUROPEA

Dato che abbiamo già dato una definizione generale di intelligenza artificiale, partiamo subito andare a fornire quella che è la definizione di IA che ci dà l'Unione Europea. Secondo l'Unione, l'Intelligenza artificiale indica *i sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi.*[23] I sistemi basati sull'IA possono consistere in software che agiscono nel mondo virtuale (per esempio assistenti vocali, software per l'analisi delle immagini, motori di ricerca, sistemi di riconoscimento vocale e facciale); oppure incorporare l'IA in dispositivi hardware (per esempio in robot avanzati, auto a guida autonoma, droni o applicazioni dell'Internet delle cose). Molte tecnologie di IA richiedono dati per migliorare le loro prestazioni. Una volta raggiunto un buon livello di prestazioni, esse possono contribuire a migliorare e automatizzare il processo decisionale nello stesso campo. Anche la proposta di Regolamento del 21.4.2021 COM(2021) 206, che è stata approvata dal Parlamento Europeo ed entra così verso la fase finale prevista per l'approvazione, ha deciso di dettare una definizione non tanto di intelligenza artificiale, ma di Sistemi di Intelligenza Artificiale (sistema di IA)[24], i quali vengono definiti come un *"software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono"*. [25] Gli approcci a cui si fa riferimento sono:

- Approcci di apprendimento automatico, compresi l'apprendimento supervisionato, l'apprendimento non supervisionato e l'apprendimento per rinforzo, con utilizzo di un'ampia gamma di metodi, tra cui l'apprendimento profondo (*deep learning*);

[23] L'intelligenza artificiale per l'Europa, COM(2018) 237, 25 aprile 2018, 1

[24] Paolo Moro riporta come l'intelligenza artificiale consista in una famiglia di tecnologie in rapida evoluzione in grado di apportare una vasta gamma di benefici economici e sociali in tutti gli ambiti delle attività industriali e sociali (P.Moro, "Intelligenza artificiale e tecnodiritto. Fondamenti etici ed innovazione tecnologica", in "Etica, Diritto e Tecnologia", a cura di Paolo Moro, FrancoAngeli, 2021, pagine 7-24)

[25] Definizione contenuta nella proposta di Regolamento 21.4.2021 COM(2021) 206

- approcci basati sulla logica e approcci basati sulla conoscenza, compresi la rappresentazione della conoscenza, la programmazione induttiva (logica), le basi di conoscenze, i motori inferenziali e deduttivi, il ragionamento (simbolico) e i sistemi esperti;
- approcci statistici, stima bayesiana, metodi di ricerca e ottimizzazione.

2.2 I DESTINATARI DELL'ARTIFICIAL INTELLIGENCE ACT

La proposta di regolamento di cui parleremo, va a definire i destinatari di essa. Tale normativa ha come destinatari gli sviluppatori, i programmatori, i disegnatori, i produttori e i fornitori localizzati nei vari paesi facenti parte dell'Unione Europea e non solo. Il regolamento, infatti, guarda anche alla collocazione del prodotto, ovvero il sistema di IA, nel mercato europeo, vincolando così, qualunque produttore o utilizzatore di sistema la cui commercializzazione o il cui impiego avvengono all'interno del mercato europeo. Va precisato che, tra i destinatari di questo regolamento, ai privati, si affiancano anche le pubbliche amministrazioni, sia che queste provvedano a dotarsi *in house* di sistemi di IA, sia nel caso in cui recepiscano queste applicazioni all'esterno e li utilizzino per lo svolgimento dei propri compiti, questo si chiama *contracting out.* Sotto questo punto di vista, la normativa quindi parifica i soggetti pubblici e i soggetti privati, unificando il tipo di garanzie che l'uso dei sistemi di IA impone per tali soggetti.

2.3 I PRESUPPOSTI DELLA NORMATIVA DELL'ARTIFICIAL INTELLIGENCE ACT

La proposta di regolamento ha l'intenzione di stabilire regole armonizzate sull'intelligenza artificiale. Con intelligenza artificiale si intende quella famiglia di tecnologie in rapida evoluzione, che sono in grado di apportare benefici economici e sociali nell'ambito delle attività industriali e sociali. L'uso dell'intelligenza artificiale sicuramente porta con sé molteplici vantaggi economici, sociali, ambientali e fornisce vantaggi competitivi alle imprese e all'economia europea. Detto questo però, l'utilizzo dell'IA può far nascere nuovi rischi o conseguenze negative per le persone fisiche o la società stessa. L'interesse dell'Unione Europea è quello di preservare la leadership tecnologica dell'UE e assicurare che i cittadini europei possano usufruire di nuove tecnologie nel rispetto dei valori, dei diritti fondamentali e dei principi che stanno alla

base dell'Unione Europea. Con questa proposta l'Unione intende tenere fede ai vari impegni presi, quali l'impegno politico della presidente Ursula von der Leyen, la quale ha annunciato che l'Unione avrebbe presentato una normativa che permettesse di coordinare le implicazioni umane ed etiche dell'Intelligenza Artificiale. A seguito di questo annuncio l'Unione ha poi pubblicato il Libro bianco sull'intelligenza artificiale, il quale contiene le opzioni strategiche su come conseguire l'obbiettivo di promuovere l'adozione dell'IA, affrontandone però i rischi associati a determinati utilizzi di questa tecnologia. La presente proposta mira, in particolare, ad affrontare i rischi che derivano dall'utilizzo dell'IA al fine di sviluppare un sistema di fiducia, proponendo un quadro giuridico per un'IA affidabile. Questa normativa si prefigge di dare agli utenti la fiducia nei confronti dei sistemi di IA, incoraggiandone lo sviluppo nelle imprese, inoltre risponde alle richieste del Parlamento europeo e del Consiglio europeo, i quali hanno chiesto un intervento legislativo che vada ad assicurare il buon funzionamento del mercato interno per i sistemi di intelligenza artificiale. Tale normativa, contribuisce allo sviluppo di un'intelligenza artificiale sicura, affidabile e che rispetti i principi etici. I sistemi di IA posso essere impiegati in vari ambiti dell'economia e della società, anche al di fuori delle frontiere europee e circolare all'interno dell'Unione. Alcuni stati hanno già iniziato a prendere in esame l'adozione di regole a livello nazionale per garantire un uso e uno sviluppo sicuro dell'intelligenza artificiale e far sì che essa venga utilizzata nel rispetto dei diritti fondamentali. Anche per questo motivo, l'Unione Europea ha ritenuto opportuno garantire un livello di protezione costante ed elevato in tutto il suo territorio ed evitare così divergenze che vadano ad ostacolare la circolazione dei sistemi di IA e dei relativi prodotti e servizi che da esse ne derivano, all'interno del mercato unico. Pertanto, è opportuno stabilire degli obblighi uniformi per gli operatori e garantire, sempre in maniera uniforme, la tutela degli interessi pubblici e dei diritti delle persone all'interno dell'intera Unione. È vero, come detto, che l'intelligenza artificiale può fornire notevoli vantaggi alle imprese e alla società, d'altro canto però, essa può portare alla nascita di nuovi rischi, pregiudicare gli interessi pubblici e i diritti tutelati dalla legislazione europea. Si rende così necessaria la nascita di un nuovo quadro giuridico europeo che vada ad istituire regole armonizzate in materia di intelligenza artificiale, per promuoverne lo sviluppo, l'uso e l'adozione all'interno dell'Unione, garantendo al tempo stesso un elevato livello di protezione degli interessi pubblici, quali la salute, la sicurezza e la

protezione dei diritti fondamentali. Servono regole armonizzate che vadano a disciplinare l'immissione sul mercato di sistemi di intelligenza artificiale, la loro messa in servizio, in modo da poter garantire il buon funzionamento del mercato interno e consentendo a tali sistemi di poter beneficiare del principio della libera circolazione dei beni e dei servizi.

2.4 GLI OBBIETTIVI DELL'AI ACT

In questo contesto appena delineato, la normativa in attesa di approvazione, definisce al suo interno i seguenti obiettivi specifici: 1) assicurare che i sistemi di IA immessi sul mercato unico europeo e utilizzati nell'Unione siano sicuri e rispettino la normativa vigente in materia di diritti fondamentali e i valori sanciti dall'Unione; 2) assicurare la certezza del diritto, per facilitare gli investimenti e l'innovazione nell'Intelligenza Artificiale; 3) migliorare la *governance*[26] e l'applicazione della normativa già esistente in materia di diritti fondamentali e requisiti di sicurezza da applicare ai sistemi di IA; 4) rendere più facile lo sviluppo di un mercato unico per l'applicazione di sistemi di IA leciti, sicuri e affidabili e prevenire la frammentazione del mercato stesso.

2.5 I CONTENUNTI DELLA PROPOSTA DI REGOLAMENTO

La proposta di regolamento sostanzialmente stabilisce regole armonizzate per l'immissione nel mercato, la messa in servizio e l'utilizzo dei sistemi di intelligenza artificiale nell'Unione Europea, stabilisce il divieto di determinati sistemi di intelligenza artificiale, i requisiti che ogni sistema deve rispettare e gli obblighi per gli operatori di tali sistemi, regole di trasparenza e regole in materia di monitoraggio e vigilanza sul mercato unico.

Tale proposta individua tre categorie diverse di sistemi di Intelligenza Artificiale e la sottopone a vari regimi regolatori. Le tre categorie regolamentate sono:

1) Sistemi a rischio inaccettabili, che vengono quindi vietati;
2) Sistemi ad alto rischio;
3) Sistemi a basso o minimo rischio.

Partendo dall'analisi del primo gruppo possiamo dire che questo tipo di sistemi vengono vietati per il rischio inaccettabile collegato al loro utilizzo. I sistemi a rischio inaccettabile,

[26]Esercizio dell'autorità, della direzione e del controllo. Può essere riferita all'insieme delle istituzioni formali e informali che regolano l'attività e il funzionamento di una società, un ente pubblico o privato.

che vengono quindi vietati, sono quei sistemi che mirano a manipolare, in base a tecniche subliminali, la condotta delle persone, oppure sono quelli che, facendo leva sulla vulnerabilità dei soggetti che li utilizzano, mirano a condizionarne la condotta. In entrambi i casi, il divieto per questi tipi di sistemi scatta nel momento in cui, il loro utilizzo possa determinare danni fisici o psicologici all'utente o ad altri individui. Altri sistemi vietati sono quelli che vengono utilizzati dalle autorità pubbliche, ai fini della valutazione, o della classificazione dell'affidabilità delle persone fisiche per un determinato periodo di tempo, sulla base del loro comportamento sociale o di caratteristiche personali. In particolare, sono vietati nel momento in cui, questa valutazione comporta o un trattamento pregiudizievole o sfavorevole nei confronti di determinate persone fisiche o di interi gruppi di persone fisiche in contesti che non sono collegati ai contesti in cui i dati sono stati inizialmente raccolti, oppure nel momento in cui comportano un trattamento pregiudizievole o di sfavore nei confronti di persone fisiche o gruppi di persone fisiche che sia ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità. Sono altresì vietati i sistemi di identificazione biometrica remota "in tempo reale", ovvero sistemi di identificazione biometrica in cui il rilevamento dei dati biometrici, il confronto e l'identificazione, avvengono senza ritardi significativi. In quest'ambito sono incluse anche le identificazioni istantanee e quelle che avvengono con brevi ritardi limitati. In particolare, questo tipo di sistemi sono vietati nel momento in cui vengono utilizzati in spazi accessibili al pubblico ai fini di attività di contrasto, a meno che tale uso non sia strettamente necessario per la ricerca mirata di potenziali vittime di reato, minori compresi, o per la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone o di un attacco terroristico, o per il rilevamento, la localizzazione o l'azione penale nei confronti di un autore o di un sospettato di un reato. Per di più, anche qualora il riconoscimento facciale sia rivolto al raggiungimento degli obbiettivi sopracitati, la proposta di regolamento stabilisce che si debba tenere conto della situazione concreta, della gravità, la probabilità, l'entità del pregiudizio che potrebbe derivare dal mancato uso del sistema di identificazione e le conseguenze che l'impiego di esso potrebbe avere sui diritti e le libertà delle persone coinvolte. Ultima precisazione da fare, in merito a questi sistemi, riguarda l'obbligo per il quale l'uso di sistemi di riconoscimento facciale richiede una

previa autorizzazione dell'autorità giudiziaria o dell'autorità amministrativa, previa istanza motivata.

Il titolo terzo della proposta di regolamento tratta dei sistemi di intelligenza artificiale ad alto rischio e costituisce la parte preponderante e centrale della proposta. L'articolo 6 del regolamento contiene una classificazione dei sistemi ad alto rischio. La normativa ci dice che un sistema di IA viene considerato ad alto rischio se sono soddisfatti entrambe le seguenti condizioni:

- Il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto, o è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione Europea;
- Il prodotto stesso, il cui componente di sicurezza è il sistema di IA, in quanto prodotto è soggetto a una valutazione della conformità da parte dei terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione Europea.

Oltre a questi sistemi, l'Allegato III della presente proposta riporta un lungo elenco di sistemi considerati ad alto rischio. Questo elenco viene diviso in base ai settori presi in considerazione. Per esempio, per quanto riguarda il settore dell'occupazione, gestione dei lavoratori e accesso al lavoro autonomo, sono considerati ad alto rischio, i sistemi di IA destinati a essere utilizzati per l'assunzione o la selezione di persone fisiche, in particolare per pubblicizzare i posti vacanti, vagliare o filtrare le candidature, valutare i candidati nel corso di colloqui o prove e l'IA destinata a essere utilizzata per adottare decisioni in materia di promozione e cessazione dei rapporti contrattuali di lavoro, per l'assegnazione dei compiti e per il monitoraggio e la valutazione delle prestazioni e del comportamento delle persone nell'ambito di tali rapporti di lavoro. L'allegato III però, è stato modificato, e oltre all'elencazione fornita, per parlare di sistemi ad alto rischio, è necessario tenere conto anche dei rischi di danno alla salute e alla sicurezza e di eventuali rischi di impatto negativo sui diritti fondamentali.

Ultima categoria di sistemi di intelligenza artificiale, sono quelli a basso o minimo rischio. Questa categoria è residuale e si ricava per sottrazione, di conseguenza sono sistemi di intelligenza artificiale a minimo o basso rischio tutti quelli che non sono vietati o ad alto rischio.

La normativa, dopo aver definito i sistemi di IA e averli suddivisi in categoria, sancisce i requisiti che devono rispettare i sistemi di IA ad alto rischio. Innanzi tutto, in relazione a questi sistemi è istituito, attuato, documentato e mantenuto un sistema di gestione dei rischi. Questo dovrà essere mantenuto e aggiornato per tutto il ciclo di vita del sistema. Stiamo parlando di un processo attraverso il quale si vanno ad identificare e valutare i rischi, sia quelli conosciuti e prevedibili prima della messa in commercio, sia quelli che emergeranno in fase di monitoraggio dopo la messa in commercio, nel momento in cui il sistema viene utilizzato in maniera conforme alle sue finalità previste. Si vanno a valutare inoltre, i rischi legati all'analisi dei dati raccolti dal sistema di monitoraggio successivamente all'immissione sul marcato. Oltre all'individuazione, vi è anche la gestione dei rischi con lo scopo di cercare di eliminarli dove possibile, o comunque ridurli al minimo. Per fare questo è necessario cercare di ridurre i rischi già all'origine, attraverso un'adeguata progettazione e fabbricazione, l'attuazione dei rischi e il controllo di essi, dove non è possibile eliminarli. Per adempiere adeguatamente agli obblighi legati ai rischi, è necessaria un'adeguata informazione dei rischi e, ove opportuno, la formazione degli utenti. I sistemi di IA sono sottoposti altresì, ad una prova, al fine di individuare le misure di gestione dei rischi più appropriate e per garantire che i sistemi funzionino in modo conforme alla finalità per le quali sono stati previsti e che rispettino i requisiti richiesti. La procedura di prova del sistema può essere effettuata, non solo prima dell'immissione nel mercato, ma anche nel corso della vita del sistema stesso, a patto che tale procedura non vada al di là delle finalità previste per il sistema. Per quanto riguarda i dati e la governance di essi, l'Unione detta delle norme da rispettare. Uno dei temi fondamentali per l'Unione, che emerge proprio dalla lettura del regolamento, è la trasparenza dei sistemi presi in considerazione. Infatti, ogni sistema di IA deve essere disegnato e sviluppato in modo da assicurare un appropriato livello di trasparenza. Questi sistemi ad alto rischio devono essere accompagnati da istruzioni per l'uso in formato digitale o non digitale adeguate, che contengano informazioni concise, corrette, complete e chiare, che siano pertinenti, accessibili e comprensibili per gli utenti. Le informazioni che devono essere presenti sono l'identità e i dati di contatto del fornitore, del suo rappresentante autorizzato, le caratteristiche, le capacità e i limiti delle prestazioni del sistema di IA ad alto rischio, nonché la finalità prevista, le sue prestazioni per quanto riguarda le persone o i gruppi di persone sui quali il sistema viene a essere utilizzato, il

livello di accuratezza, robustezza e cybersicurezza su cui il dispositivo è stato testato, le caratteristiche degli input data, la durata attesa e ogni circostanza nota o prevedibile che possa portare ad un rischio per la salute, la sicurezza o altri diritti fondamentali. Deve contenere anche le eventuali modifiche apportate al sistema di IA ad alto rischio e le misure di sorveglianza umana. A tal proposito, il tema della sorveglianza umana, è un altro tema molto importante per tale proposta. Ogni sistema di IA ad alto rischio deve essere sviluppato e programmato in modo da assicurare un'efficace supervisione umana, detta anche *human oversight*. Si prevede che la presenza umana sia mirata a prevenire o ridurre al minimo i rischi per la salute, la sicurezza o altri diritti fondamentali che possono concretizzarsi anche quando i sistemi vengano utilizzati in conformità ai requisiti richiesti. La sorveglianza può essere garantita in vari modi elencati dalla normativa. Deve essere garantita attraverso almeno una delle misure messe a disposizione. Tali misure sono: misure individuate e integrate nel sistema IA ad alto rischio dal fornitore prima della sua immissione sul mercato o messa in servizio, ove possibile, oppure misure individuate dal fornitore prima dell'immissione sul mercato o della messa in servizio del sistema, adatte ad essere attuate dall'utente. Queste misure consentono alle persone alle quali viene affidata la sorveglianza umana di comprendere le capacità e i limiti del sistema di IA ad alto rischio ed essere in grado di monitorarne il funzionamento, in modo da poter individuare il prima possibile eventuali segnali di anomalie e disfunzioni e consentire loro di essere in grado di interpretare correttamente l'output dei sistemi di IA ad alto rischio, tenendo conto in particolare delle caratteristiche del sistema, degli strumenti e dei metodi di interpretazione disponibile. Queste misure consentono per di più, di essere in grado di decidere, in qualsiasi situazione particolare, di non utilizzare il sistema ad alto rischio o di ignorare, annullare o ribaltare l'output del sistema ed infine consente di essere in grado di intervenire sul funzionamento del sistema o di interromperne l'uso. Va precisato che per quel che concerne i sistemi di identificazione biometrica a distanza in tempo reale e a posteriori di persone fisiche, è previsto dal regolamento, che ogni decisione debba essere controllata ed eventualmente confermata da almeno due supervisori.

I requisiti da rispettare però non sono solo questi, in particolare vengono sanciti vari obblighi che devono essere rispettati da vari soggetti, quali i fornitori, i fabbricanti, gli importatori e gli utenti che utilizzano tali sistemi ad alto rischio. Seguendo l'ordine della normativa, partiamo dagli obblighi dei fornitori. I fornitori hanno l'obbligo di garantire

che i loro sistemi di IA siano conformi ai requisiti elencati nella normativa, devono disporre di un sistema di gestione della qualità, hanno il compito di redigere la documentazione tecnica del sistema ad alto rischio, devono garantire che il sistema sia sottoposto ad una pertinente procedura di valutazione della conformità prima della loro immissione nel mercato, devono rispettare gli obblighi di registrazione, adattare le misure correttive necessarie, informare le autorità nazionali competente degli Stati membri in cui hanno messo a disposizione il servizio nel caso di difformità e eventuali sanatorie, poi devono apporre il marchio CE ed infine, su rischiste dell'autorità nazionale competente, dimostrare la conformità del sistema. Anche gli importatori dei sistemi devono sottostare agli obblighi di fornitura della documentazione tecnica, della marchiatura CE che deve recare il sistema e devono avere eseguito l'appropriata procedura di valutazione della conformità. Così come gli importatori, anche i distributori di tali sistemi sono soggetti ai medesimi doveri. Non solo questi soggetti devono sottostare a dei doveri previsti dalla normativa, ma anche gli utenti hanno degli obblighi ben precisi. Gli utenti sono tenuti ad utilizzare i sistemi conformemente alle istruzioni per l'uso che accompagnano i sistemi, devono garantire che i dati di input siano pertinenti alla finalità prevista del sistema, sono tenuti a monitorare il funzionamento del sistema. Data l'importanza del mercato unico europea, l'Unione ha deciso di stabilire regole armonizzate anche in tema di immissione di tali sistemi ad altro rischio nel mercato. Per quel che concerne l'immissione nel mercato di questi sistemi, il regolamento prevede, la verifica della conformità di tali sistemi ai requisiti previsti. Il modello scelto dalla Commissione è rappresentato dalla procedura di marchio di conformità europea, ovvero la cosiddetta marchiatura CE, la quale viene già utilizzata per regolare la circolazione di molti prodotti, all'interno del mercato europeo. Questo tipo di procedura prevede il controllo a carico del produttore, quindi rende il tutto più agevole e sposta sugli operatori economici la responsabilità di assicurare il rispetto dei requisiti di sicurezza stabiliti dalla normativa. La scelta di questa procedura, presenta però delle eccezioni. Per quanto concerne alcuni sistemi biometrici, i controlli e la procedura di conformità devono essere effettuati da soggetti terzi. Per quanto riguarda questa procedura iniziale di controllo di conformità, bisogna precisare che non è l'unico momento in cui si effettua il controllo dei rischi, poiché la Commissione ha deciso di affiancare alle procedure precedenti all'immissione nel mercato dei sistemi di IA ad alto

rischio, un sistema di monitoraggio *post market*.[27] Questo sistema di monitoraggio ha l'obbiettivo di garantire la conformità del prodotto ai requisiti stabiliti dalla normativa, nel corso dell'intera vita del sistema. Affinché sia possibile effettuare questo controllo sulla conformità, gli Stati membri hanno un compito fondamentale, ovvero quello di nominare le autorità nazionali competenti in materia di sistemi di IA, con lo scopo di garantire l'applicazione e l'attuazione del regolamento. Gli stati devono nominare un'autorità di controllo, che agisce anche come autorità di notifica. Sono proprio gli organismi di notifica che vanno a verificare la conformità dei sistemi prima dell'immissione nel marcato, i quali si dedicano anche alla gestione della sorveglianza post market e che riconoscono precisi obblighi in capo all'utilizzatore e in capo al *provider*[28]. Il provider ha l'obbligo di conservare, per un periodo di tempo adeguato, che deve essere individuato in base alle caratteristiche del sistema di IA preso in considerazione, le registrazioni di funzionamento del sistema di IA, chiamate *automatically generated logs*. Queste registrazioni potranno essere oggetto di accesso da parte delle autorità nazionali competenti per finalità di sorveglianza. Il provider deve inoltre, adottare nell'immediatezza le misure coercitive necessarie in caso di difformità e deve comunicare all'autorità nazionale competente eventuali violazioni riscontrate nel funzionamento del sistema. In tutto questo, l'autorità di notifica deve operare in maniera indipendente rispetto al provider del sistema ad alto rischio che viene sottoposto alla valutazione. Andando avanti con l'analisi della normativa, troviamo che essa va poi a sancire anche i poteri e le misure volte ad assicurare il rispetto degli obblighi previsti da parte dei providers. L'autorità di sorveglianza, in particolare, nel momento in cui viene a conoscenza di una difformità, del sistema di IA, rispetto ai requisiti e gli obblighi fissati dal regolamento, potrà imporre al soggetto interessato l'adozione di misure appropriate per interrompere le possibili violazioni, potrà anche ritirare il sistema di IA dal mercato o richiamarlo per un tempo commisurato alla natura del rischio. Tra le ultime disposizioni, vista la complessità di questi sistemi e visti i rischi di errori e discriminazioni, il regolamento impone il rispetto di altri requisiti. Il primo requisito si riferisce alla qualità dei dati e alla governance dei dati. È istituito un "comitato europeo per l'intelligenza artificiale". Il comitato fornisce consulenza e assistenza alla Commissione allo scopo di

[27]Dopo la sua immissione nel mercato
[28]Fornitore

contribuire alla cooperazione delle autorità nazionali di controllo e della Commissione per quando riguarda le materie trattate nel regolamento; assistere le autorità nazionali di controllo e la Commissione nel garantire l'applicazione uniforme delle norme sancite dal regolamento. Il comitato è composto dalle autorità nazionali di controllo, rappresentate dal capo di tale autorità o da un altro funzionario designato e dal Garante europeo per la protezione dei dati. Esso, se necessario, può formare dei sottogruppi per esaminare questioni specifiche. Il comitato è presieduto dalla Commissione, la quale convoca le eventuali riunioni e prepara l'ordine del giorno. Il comitato può istituire gruppi di esperti e osservatori esterni alle sue riunioni e tenere scambi con terzi. Tale comitato adotta un suo regolamento, il quale contiene gli aspetti operativi relativi all'esecuzione dei compiti del comitato stesso. Per quanto riguarda appunto i compiti del comitato, essi vengono direttamente sanciti dal regolamento. Il comitato ha il compito di raccogliere e condividere conoscenze e pratiche tra gli Stati membri, ha il compito di contribuire all'uniformità delle pratiche amministrative negli Stati membri, deve formulare pareri, raccomandazioni o contributi scritti su questioni relative al regolamento, quali per esempio sulle specifiche tecniche o sulle norme esistenti relative ai requisiti per i sistemi di Intelligenza Artificiale ad alto rischio, e anche per quanto riguarda l'uso delle norme armonizzate o delle specifiche comuni relative alle norme armonizzate e alle specifiche comuni. Il regolamento disciplina anche il tema della banca dati dell'Unione Europea per i sistemi di IA indipendenti ad alto rischio. La Commissione, insieme agli Stati membri, istituisce e mantiene una banca dati dell'UE, contenente le informazioni relative ai sistemi di IA ad alto rischio registrati rispettando i requisiti richiesti dalla normativa. La banca dati contiene i dati personali necessari alla raccolta. Queste informazioni riguardano i nomi e i dati di contatto delle persone fisiche responsabili della registrazione del sistema di IA e aventi l'autorità di presentare il fornitore di tale sistema. I fornitori dovranno inserire nella banca dati dell'UE i dati elencati nella presente normativa. Le informazioni contenute nella banca dati sono accessibili al pubblico e la Commissione è titolare del trattamento delle banche dati dell'UE. Per quanto riguarda la disciplina attinente alle sanzioni, invece, la Commissione lascia ampio spazio ai legislatori dei vari Stati membri, anche se, come sappiamo, le sanzioni dovranno avere natura effettiva, proporzionata e dissuasiva. Va precisato che la proposta lascia ampia libertà agli Stati membri, ma individua diversi regimi sanzionatori a seconda della gravità delle violazioni. Le sanzioni

più alte vengono inflitte nel momento in cui vengono immessi nel mercato sistemi di IA vietati, o viene violata la disciplina relativa ai dati e alla governance dei dati. Poi si passa al livello intermedio per i sistemi che non rispettano gli altri requisiti sanciti dalla normativa. Infine, abbiamo un regime sanzionatorio più leggero, che viene stabilito per le violazioni da parte dei providers degli obblighi informativi. La Commissione ha deciso che la determinazione della sanzione da emettere non dovrebbe essere mai automatica. Infatti, dovrebbero essere presi in considerazione alcuni elementi: la natura, la gravità e la durata della violazione, oltre alle conseguenze che ne derivano. Inoltre, bisogna controllare che la sanzione non sia già stata elargita da un'altra autorità di sorveglianza per la medesima sanzione e lo stesso operatore. Infine, bisogna prendere in considerazione la dimensione del mercato in cui la violazione è stata commessa. È stata prevista altresì una disciplina a parte per quei casi in cui a violare il regolamento sia un'istituzione, un'agenzia o un organismo amministrativo dell'Unione Europea. In questi casi, tra i criteri da prendere in considerazione al fine di determinare la sanzione applicabile, si prevede, oltre agli elementi sopracitati, anche la volontà mostrata dall'autorità di collaborare con il Garante per i dati personali. Ultimo aspetto importante riguarda il richiamo, da parte del regolamento, alle fondamentali garanzie del contraddittorio nei procedimenti sanzionatori. Nel corso del procedimento sono pienamente garantiti i diritti di difesa delle parti interessate.

2.6 I DIRITTI FONDAMENTALI DA TUTELARE

Con il presente regolamento, l'Unione Europea, oltre a voler dettare regole uniformi per quanto concerne la gestione dei sistemi di intelligenza artificiale, pone anche come obbiettivo quello di tutelare i diritti fondamentali dell'uomo. Tali diritti li troviamo nella Carta dei diritti fondamentali dell'Unione Europea. La proposta di regolamento mira proprio ad assicurare un elevato livello di protezione di questi diritti e ad affrontare le varie fonti di possibile rischio. I diritti che la Carta dei diritti fondamentali va a sancire sono molteplici, quali per esempio il diritto alla vita, alla libertà, alla dignità umana. La presente proposta vuole affiancarsi a questa normativa, in modo da migliorare e promuovere il livello di protezione di questi diritti. Il primo diritto che viene tutelato è il diritto alla dignità umana, la quale è inviolabile, deve essere rispettata e tutelata. Altro diritto fondamentali, che riguarda proprio quest'ambito dell'IA è il diritto al rispetto della

vita privata e alla protezione dei dati di carattere personale dell'individuo. Tali diritti sono rispettivamente sanciti dagli articoli 7 e 8 della Carta. L'articolo 7 sancisce proprio il diritto al rispetto della vita privata, ma non solo, l'articolo parla anche di rispetto di vita famigliare, del proprio domicilio e delle proprie comunicazioni. In sintesi, viene sancito il diritto alla riservatezza del soggetto. Viene poi tutelato il diritto alla non discriminazione, in particolare è vietata qualsiasi forma di discriminazione basata sul sesso, la razza, il colore della pelle o l'origine etnica o sociale, le caratteristiche genetiche, la lingua, la religione o le convinzioni personali, le opinioni politiche o di qualsiasi altra natura, l'appartenenza ad una minoranza nazionale, gli handicap e altri fattori. Affianco a questo articolo risulta fondamentale evidenziare la parità di tra uomo e donna, sancita anche questa dalla Carta. La parità di genere deve essere assicurata in tutti i campi, compreso quello in materia di occupazione di lavoro e retribuzione. Questa proposta, inoltre mira a prevenire un effetto dissuasivo sui diritti alla libertà di espressione e alla libertà di riunione. Ogni individuo è libero di esprimersi e questa libertà comprende anche la libertà di opinione, la libertà di ricevere o comunicare informazioni o idee senza che vi possa essere intromissione da parte delle autorità pubbliche. Per quanto riguarda la libertà di riunione invece, ogni individuo ha diritto alla libertà di riunione pacifica e di associazione a tutti i livelli in ambito politico, sindacale e civile. Questa libertà implica il diritto di ogni individuo di fondare sindacati insieme ad altri soggetti e di aderirvi per la difesa dei propri diritti. Il regolamento mira, inoltre ad assicurare la tutela del diritto a un ricorso effettivo e a un giudice imparziale, tutela del diritto riguardante la presunzione di innocenza e dei diritti della difesa, nonché assicurare il principio generale di buona amministrazione. Rilevante per la proposta è anche il diritto a un elevato livello di protezione dell'ambiente e al miglioramento della sua qualità, anche in relazione alla salute e alla sicurezza delle persone. Gli obblighi di verifica dei requisiti e di gestione dei rischi e della sorveglianza umana, renderanno più agevole il rispetto dei diritti fondamentali, riducendo al minimo il rischio di decisioni errate o distorte prese dai sistemi di IA, in settori critici, quali l'istruzione e la formazione, l'occupazione, servizi importanti, le attività di contrasto e i sistemi giudiziari. Nell'eventualità in cui si verifichino violazioni di questi diritti fondamentali, resta ferma la possibilità per il soggetto leso di poter mettere in atto un ricorso efficace, e questo sarà reso possibile assicurando la trasparenza e la tracciabilità dei sistemi di IA e prevedendo rigidi controlli

dei sistemi anche dopo la loro immissione nel marcato unico. La presente normativa, è vero che incentiva l'utilizzo dei sistemi di IA all'interno delle imprese e degli ambienti di lavoro; tuttavia, impone delle restrizioni alla libertà d'impresa. Queste restrizioni vengono imposte sempre al fine di andare a tutelare la salute, la sicurezza, i consumatori e altri diritti fondamentali. Va precisato che tali restrizioni sono proporzionate e limitate al minimo necessario per prevenire ed eventualmente attenuare i possibili rischi e probabili violazioni dovuti all'utilizzo di questi sistemi. Ultima precisazione da fare in merito, riguarda il diritto alla protezione della proprietà intellettuale. Gli obblighi di trasparenza sanciti dalla nuova regolamentazione, non andranno ad incidere in maniera sproporzionata nei confronti di questo diritto, visto che saranno limitati. Qualsiasi divulgazione di informazione sarà sempre effettuata rispettando la legislazione pertinente nel settore, compresa quella di carattere europeo. Nell'eventualità in cui le autorità pubbliche e gli organismi notificati avessero la necessità di entrare in possesso di informazioni riservate o al codice sorgente per esaminarne il rispetto degli obblighi sostanziali, saranno sottoposte a obblighi di riservatezza vincolanti.

2.7 INTELLIGENZA ARTIFICIALE E DIRITTO ALLA PRIVACY

La normativa tra i vari "considerando" ne inserisce proprio uno che riguarda i sistemi di intelligenza artificiale e i lavoratori. Viene precisato che i sistemi di IA utilizzati nel settore dell'occupazione, nella gestione dei lavoratori e nell'accesso al lavoro, con particolare riguardo all'assunzione e la selezione del personale, in materia di promozione e cessazione del rapporto, nonché per l'assegnazione di compiti, per il monitoraggio o la valutazione delle persone nei rapporti di lavoro, dovrebbero essere considerati ad alto rischio, poiché posso avere un elevato impatto sul futuro lavorativo di essi. Infatti, come precedentemente detto, la proposta di regolamento, ha come scopo anche quello di proteggere i diritti fondamentali sanciti dall'Unione Europea. In questo caso, poniamo attenzione ai diritti fondamentali che riguardano gruppi speciali di individui, quali i diritti dei lavoratori. Alcuni diritti dei lavoratori possiamo ravvisarli nella Carta dei diritti fondamentali, primo fra tutti è l'articolo 15. L'articolo dice che ogni individuo ha il diritto di lavorare e di esercitare una professione, scelta o accettata in maniera libera, senza costrizioni. Accanto a questo diritto, si affianca il diritto alla non discriminazione per ragioni di razza, sesso, età, etnia, colore della pelle, nascita, luogo di origine, religione, handicap sia nella fase iniziale della vita lavorativa, sia nella fase intermedia e anche nella

fase di cessazione del rapporto di lavoro. Oltre alla non discriminazione, altro diritto sancito è quello della parità tra uomo e donna. Questa parità viene intesa in tutti campi, compreso l'ambito lavorativo e la retribuzione. È importante ricordare che questo principio di parità non ostacola il mantenimento o l'adozione di misure volte a prevedere dei vantaggi nei confronti del sesso sottorappresentato. Ogni lavoratore, poi ha il diritto ad essere tutelato di fronte ad un licenziamento che viene considerato illegittimo, secondo le normative vigenti. Altro diritto che riguarda i lavoratori e che la normativa promette di tutelare il diritto dei lavoratori a condizioni lavoro giuste ed eque. Questo significa che ogni lavoratore ha diritto a condizioni di lavoro sane, sicure e dignitose, ha diritto al riposo giornaliero e settimanale, a vedersi stabilita una durata massima della durata del lavoro e a ferie annue retribuite. Un diritto importante, che riguarda sempre i lavoratori, è il diritto che a va tutelare il lavoratore nel momento in cui si trova di fronte ad un licenziamento ingiustificato: infatti ogni lavoratore, ha il diritto ad essere tutelato di fronte ad un licenziamento ingiustificato secondo le norme del diritto comunitario e in conformità alle legislazioni nazionali dei singoli Stati membri. Dopo questa elencazione, è importante però riportare la nostra attenzione sull'IA e su come questa può in qualche modo andare a ledere i diritti dei lavoratori, in particolar modo il diritto alla privacy dei lavoratori. A tal proposito, è il regolamento stesso che va a precisare che i sistemi di intelligenza artificiale utilizzati, per monitorare il comportamento delle persone o le loro prestazioni in ambito lavorativo, possono in qualche modo andare a ledere il diritto alla protezione dei dati personali e della vita privata dei soggetti coinvolti. Un esempio concreto riguarda un'azienda americana che di recente, ha lanciato un'applicazione destinata agli operatori di un call center, in grado di analizzare il tono della voce e le parole usate dai lavoratori per conversare con i clienti, al fine di definire il livello di stress degli stessi ed eventualmente correggere l'operatore in modo da farlo essere più empatico con i clienti. Come già visto, l'articolo 8 della Carta tutela la privacy dei lavoratori. L'articolo 8 si intitola proprio *Protezione dei dati di carattere personale* e dice così:" *1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.*" Partiamo dando una definizione di dati di carattere personale. Per dato

personale si intende: *qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*.[29] Oltre a questo, sono dati personali, tutti quelli che permettono di rilevare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. I sistemi di IA stanno sempre più entrando a far parte della quotidianità, compresi gli ambiti di lavoro. Come detto viene incentivato l'utilizzo di questi sistemi anche nelle imprese, per esempio per monitorare i lavoratori e il loro comportamento. Un esempio di utilizzo di sistema di intelligenza artificiale nei luoghi di lavoro, sono i sistemi di riconoscimento. A tal proposito, il riconoscimento facciale è l'elaborazione automatica di immagini digitali di volti e di persone con finalità di identificazione o verificazione. Il sistema di riconoscimento facciale può essere utilizzato per la verifica dell'identità dichiarata dalle persone o per identificare la persona stessa. Questo meccanismo avviene tramite sistemi di intelligenza artificiale, o meglio algoritmi, chiamati *face recognition*. L'utilizzo di tali sistemi è possibile solamente se il soggetto dispone di un'adeguata informativa e di un'adeguata base giuridica, poiché il trattamento dei dati biometrici rientra nei dati personali e quindi nella privacy del soggetto stesso. L'utilizzo di questo sistema negli ambienti di lavoro deve essere accompagnato dal consenso esplicito, informato e libero degli interessati dei quali vengono trattati i dati biometrici. Un altro esempio di sistema di intelligenza artificiale che può andare a ledere il diritto alla protezione dei dati personali dei lavoratori è l'algoritmo reputazionale. È un sistema che attraverso documenti forniti dall'utente va a stilare un profilo personale attraverso cui è possibile valutare l'affidabilità del soggetto, o di un'impresa o di un ente. C'è stata anche un caso già risolto dalla cassazione riguardante proprio questi algoritmi, in particolare un'associazione[30]. In questo caso è

[29]Articolo 4, del REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016

[30]Cassazione Civile, Sez. I, 25 maggio 2021, n. 14381, ord. - Pres. Genovese - Rel. Terrusi - Garante della Privacy c. Ass. Mevaluate Onlus

entrato in gioco anche un provvedimento del Garante della Privacy, il quale ha ritenuto che questo rating reputazionale potesse in qualche modo ripercuotersi sulla vita, anche privata, degli individui, oltre al fatto che la reputazione, risulta estremamente connessa alla dignità degli individui, la quale è un elemento cardine nell'ambito della protezione dei dati personali.

3 INTELLIGENZA ARTIFICIALE E PRIVACY DEI LAVORATORI

3.1 LE NUOVE TECNOLOGIE UTILIZZATE NELL'AMBITO LAVORATIVO

Prima di partire con l'analisi della normativa stessa, è necessario capire come si è evoluto il mondo del lavoro oggi e che strumenti hanno a disposizione i datori di lavoro per andare a valutare e conoscere i lavoratori. Partiamo dal fenomeno della datificazione del lavoro. Se il datore di lavoro da' uno strumento digitale ad un lavoratore per l'esecuzione della prestazione crea questa datificazione, che non si limita solo alla prestazione lavorativa. Oggi, questo fenomeno coinvolge anche tutto quello che un lavoratore compie in un ambiente digitale, ovvero come interagisce con i colleghi, come approfondisce un argomento, come interagisce con i vari programmi utilizzati. Parliamo di tecnologie, che vengono definite abilitanti e che quindi dovrebbero dare al lavoratore delle potenzialità in più. Tra questi strumenti, quello che riguarda ciò di cui stiamo parlando è il fenomeno dei *Big Data*, ovvero nel momento in cui si passa alla digitalizzazione, acquisiamo dei dati e *Big Data* sta a significare proprio grandi volumi di dati. Dati che possono essere definiti personali oppure no e avere a disposizione questo tipo di dati può essere una potenzialità e un valore, ma allo stesso tempo può essere anche un rischio. Nel momento in cui abbiamo questi dati e compiamo una sorta di analisi su di essi, ecco che ci troviamo di fronte ad un processo chiamato proprio *People analytics*. Questo fenomeno consiste nell'analisi di grandi quantità di dati per andare ad identificare modelli o prevedere comportamenti di gruppi e comunità. Questo tipo di fenomeno nell'ambito lavorativo prende il nome di *Workfoce analytics*. Le fonti da cui parte questa analisi sono di vario genere, possono essere le videocamere di sorveglianza, come i socialnetwork. Ci possono essere vari tipi di strumenti utilizzati. Gli strumenti che noi prendiamo in considerazione sono completamente digitali e sono quattro. Il primo si chiama *Human Resouces Information Sistem*, sono grandi banche dati al cui interno troviamo tutti quelli che sono i dati del lavoratore. Questi dati sono di tipo identificativo, sulla persona stessa, sull'attività lavorativa svolta, dati relativi a risposte a sondaggi e questionari e dati di posizione. Poi ci sono i *Cistomer Relationship Management*, sistemi che nascono per creare un rafforzamento del rapporto tra l'azienda e il cliente. Sono grandi banche dati, che hanno come oggetto quello di osservare i clienti e capire se sono soddisfatti oppure no. Il terzo strumento, è quello che viene chiamato *Digital Workplace*, sono software collaborativi, i quali costituiscono dei veri e propri spazi, ai quali i lavoratori possono

accedere per svolgere la prestazione lavorativa, ma attraverso i quali vengono fatte delle vere e proprie analisi sullo stress, il benessere, il malessere del lavoratore. In questo caso il rischio di violazione della privacy è veramente elevato. Nelle aziende più sviluppate poi, vengono utilizzati quegli strumenti che vengono chiamati *Applicant Tracking Sistem*, ovvero quei sistemi che vengono utilizzati per andare a filtrare i curriculum vitae che arrivano alle aziende. Oggi, di fronte a questo fenomeno della *People analytics*, è importante chiedersi allora quali sono le normative che ci tutelano, specialmente nell'ambito della privacy. Le principali criticità della *People analytics* sono da individuare in quattro ambiti: fonti con cui si acquisiscono i dati, tipi di dati acquisiti, tipo di trattamento eseguito e strumenti con cui avviene il trattamento. Le fonti sono gli strumenti di lavoro e di controllo, sui quali grava un dibatto in merito alla loro definizione, anche per la natura di questi strumenti di lavoro digitali. In questo caso il Garante Privacy è intervenuto precisando che gli strumenti di lavoro sono quelli strettamente funzionali alla prestazione lavorativa e che non siano in grado di tracciare e identificare un soggetto, mentre gli strumenti di controllo sono gli hardware e software configurati in modo tale da trattare e conservare dati nel dettaglio in ordine alla risorsa internet. Per quanto riguarda invece il tipo di dati acquisiti, sappiamo che si parla di dati personali e particolari. Per quanto riguarda il trattamento dei dati, ecco che siamo di fronte ad una criticità, poiché il rischio è quello che il trattamento possa risultare viziato. Il vero problema è poi quanto abbiamo una grande quantità di dati acquisiti e questi non sono subito comprensibili, infatti vengono detti non autoevidenti. Quindi devono essere elaborati. In questo caso rischio sta proprio qui: io acquisisco questi dati in forma neutra, ma che una volta che vengono elaborati mi danno come risultato delle informazioni eccedenti a quelli per i quali li ho raccolti, portando così ad un controllo diretto dei dati e quindi ad un vizio. Ultima criticità è il modo con cui si esegue il trattamento. Il possesso di tutto questi dati, porta quindi il titolare, ad avere e poter esercitare un controllo sull'interessato. Ecco perché è necessario capire come potersi tutelare e con quali normative. Bisogna chiarire subito che una normativa specifica non c'è ancora, però possiamo richiamare tutta una serie di fonti che devono essere applicate. In primis abbiamo le fonti che riguardano la tutela dei diritti fondamentali della persona, le norme a tutela dei dati personali, le tutele giuslavoristiche e le normative vigenti in tema di intelligenza artificiale.

3.2 IL REGOLAMENTO 2016/679 E IL NUOVO CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

La seconda normativa, che riguarda l'argomento da noi trattato è proprio il Decreto Legislativo n. 196, del 30 giugno 2003, modificato poi dal decreto legislativo 101 del 2018. Come possiamo notare, è una normativa più recente, integrata da modifiche, che hanno dato attuazione al regolamento europeo. Per capire quali sono le regole che vanno a regolamentare il diritto alla riservatezza all'interno del nostro stato, dobbiamo andare a vedere allora anche il Regolamento UE 2016/679. È necessario, infatti andare ad analizzare le due fonti normative insieme. Tuttavia, non possiamo soffermarci su tutto ciò che è previsto dal regolamento, infatti vorrei soffermarmi sui principi che stanno alla base del trattamento dei dati e il trattamento dei dati alla luce delle nuove tecnologie. Avevamo già accennato in precedenza a questo regolamento, ma ora cerchiamo di capire meglio come viene regolato il trattamento dei dati vero e proprio. I dati personali, devono essere trattati in maniera lecita, corretta e rispettando il principio di trasparenza. Partiamo dando una definizione di trattamento, che troviamo all'interno del regolamento stesso. Viene definito «trattamento»: "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione" I dati devono essere raccolti per determinate finalità, le quali devono essere esplicite e legittime, devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. Cerchiamo di capire subito quand'è che il trattamento dei dati risulta lecito. Il trattamento risulta lecito nel momento in cui ricorre una delle seguenti condizioni: l'interessato ha espresso il consenso al trattamento dei propri dati personali, il trattamento dei dati è necessario all'esecuzione di un contratto di cui l'interessato è parte o il trattamenti è necessario all'esecuzione di misure precontrattuali adottate su richiesta dello stesso, il trattamento è fondamentale per adempiere ad un obbligo legale, il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica, il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici

poteri, ed infine il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi. Definiti i casi di liceità, così come previsti dalla normativa, è necessario prendere in considerazione l'articolo 9. In questo articolo troviamo la salvaguardia di una categoria di dati definita "particolari". Questi dati, sono proprio quei dati più riservati, risultano infatti vietati trattare i dati personali che rilevino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici ed infine i dati biometrici volti ad identificare in modo univoco una persona fisica, i dati riguardanti la salute, la vita sessuale o l'orientamento sessuale di una persona. Possiamo notare come questi dati non possono essere trattati, ma il Regolamento ha previsto delle eccezioni in merito. Dopo aver citato il principio di liceità e l'articolo 9, è fondamentale però soffermarci sul concetto di trasparenza e ciò che ne deriva. Il concetto di trasparenza e le modalità di trattamento. La trasparenza è un concetto fondamentale nell'ambito dei dati personali; infatti, il titolare del trattamento deve fornire all'interessato tutte le informazioni relativi alla sua identità, i suoi contatti, i dati di contatto del responsabile del trattamento dei dati personali, il periodo di conservazione dei dati raccolti. Oltre a ciò, l'interessato viene tutelato attraverso un diritto fondamentale, ovvero il diritto di accesso. Attraverso l'esercizio di questo diritto l'interessato può ottenere dal titolare informazioni in merito al trattamento dei dati, in merito alle finalità del trattamento stesso, le categorie dei dati trattati, i destinatari di tali dati, il periodo di conservazione, ecc. Altro diritto di cui si sente spesso parlare, e che possiamo ravvisare all'interno del regolamento in questione, è il diritto all'oblio, ovvero il diritto alla cancellazione. Un diritto fondamentale per la tutela della privacy, il quale prevede la possibilità per l'interessato di richiedere al titolare del trattamento dei dati, la cancellazione di essi. Il titolare, ovviamente, una volta esercitato tale diritto da parte dell'interessato, ha l'obbligo di cancellare tali dati nel momento in cui ricorrono determinate condizioni. Nel momento in cui, infatti, il titolare revoca il consenso al trattamento dei dati, oppure nel caso in cui i dati siano stati trattati in maniera illecita, oppure il trattamento di tali dati non è più necessario rispetto alle finalità per le quali sono stati raccolti, scatta l'obbligo di cancellazione. Ecco che allora, vediamo come il codice, fornisca una serie di regole precise, che permettono di poter difendere questo diritto alla privacy, di cui ogni cittadino deve godere. La parte della normativa, di maggior interesse per noi però, è il titolo VIII, rubricato "Trattamento nell'ambito del rapporto di

lavoro". Già la sua rubricazione ci fa capire la materia oggetto del titolo e la necessità da parte del legislatore di dedicare una specifica parte della normativa a tale materia. Tale titolo, riprende alcuni articoli del regolamento, i quali si occupano di andare a proteggere la privacy dell'interessato già in fase di assunzione. La normativa va a regolamentare le informazioni ricevuto tramite il curriculum. Essa prevede che il trattamento dei dati ricevuti in fase curricolare, non necessita del consenso nel momento in cui i dati trattati secondo il principio di liceità, ovvero nel momento in cui ricorre uno dei requisiti richiamati già in precedenza. Nella medesima sezione vediamo come il legislatore ha deciso di richiamare in maniera espressa lo Statuto dei Lavoratori, per ciò che concerne le garanzie in materia di controllo a distanza e la raccolta dei dati e la loro pertinenza. Facendo sempre riferimento al regolamento, da cui deriva la normativa italiana in materia di privacy, non possiamo non citare l'articolo 22 del regolamento UE. Il quale tratta proprio del diritto alla privacy e la tecnologia. L'articolo in questione, in particolare, riguarda il processo decisionale automatizzato relativo alle persone fisiche, comprendendo anche la profilazione[31]. Il diritto che viene garantito all'interessato è quello di non essere sottoposto a una decisione basata solamente sul trattamento automatizzato, compresa la profilazione stessa. Parliamo di un processo automatizzato che può produrre effetti giuridici o che potrebbe andare ad incidere direttamente e in maniera significativa sull'interessato stesso. Il rischio che può derivare dall'utilizzo di questo tipo di sistemi è quello di andare ad incidere negativamente su una serie di diritti, libertà fondamentali e sulla dignità dell'individuo. Attraverso i dati raccolti dall'algoritmo di intelligenza artificiale c'è il rischio per l'individuo di essere discriminato. Tuttavia, il legislatore ha deciso di andare a definire delle situazioni nelle quali questo diritto non si applica. La norma, più precisamente, ha definito tre eccezioni, ovvero 3 casi di non applicabilità di tale diritto. Il primo caso di non applicabilità riguarda quella situazione in cui la decisione sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e il titolare del trattamento. Il secondo caso rientra in quelle situazioni in cui la decisione stessa venga autorizzata dal diritto dell'Unione o da uno degli Stato membri

[31]Profilazione: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

a cui è soggetto il titolare del trattamento, anche se deve comunque prevedere misure adeguate alla tutela dei diritti, delle libertà e degli interessi legittimi del soggetto interessato dal trattamento. Il terzo, ed ultimo caso, di non applicabilità, riguarda quelle situazioni in cui si ha il consenso esplicito del diretto interessato. Va precisato però che nel primo e nel terzo caso, il titolare del trattamento deve, in ogni caso, prevede e attuare delle misure che siano adatte a tutelare i diritti, le libertà e i legittimi interessi dell'interessato. L'interessato, infatti, deve avere almeno il diritto di ottenere l'intervento umano del titolare del trattamento, di poter esprimere la propria opinione e di contestare la decisione. Altra precisione riguarda tutti e tre i casi sopracitati. Le decisioni automatizzate, riguardanti i tre casi, non si basano sulle categorie di dati relative a quella categoria di dati, definita "dati particolari", della quale abbiamo già dato definizione in precedenza. È possibile fondare una decisione su dati raccolti attraverso questi sistemi, solo se l'interessato ha prestato il suo consenso in maniera esplicita al trattamento di questa categoria di dati o nel momento in cui sia necessario per motivi di interesse pubblico. Ecco che abbiamo delineato, in maniera sintetica, le norme che stanno alla base del diritto alla privacy.

3.3 LO STATUTO DEI LAVORATORI

Dopo un'analisi relativa alla proposta di regolamento Europeo sull'IA, passiamo ad analizzare le normative italiane riguardanti la privacy, ed in particolare la privacy dei lavoratori. Iniziamo con l'analisi dello Statuto dei Lavoratori, ovvero la legge numero 300, del 20 maggio 1970. Questa normativa, risale ormai al secolo scorso, ma anch'essa, come spesso succede, ha subito successive modifiche ed adattamenti, dato che il lavoro è un ambito in continua evoluzione, anche a causa dell'avvento delle nuove tecnologie. Queste nuove tecnologie, infatti, assumono un aspetto sempre più impregnante e dirompente in vari ambiti della nostra vita, tra cui l'ambito lavorativo. Se ben notiamo, questa legge, viene rubricata: "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro e norme sul collocamento", quindi già la rubricazione stessa, ci indica qual è l'orientamento della normativa. Essa mira proprio a tutelare le libertà dei lavoratori, ovviamente, tenendo conto della necessità di bilanciamento tra le esigenze le esigenze del datore di lavoro e dei lavoratori. Gli articolo di maggior interesse nel nostro caso sono l'articolo 4 e l'articolo 8 dello statuto. L'articolo 4 riguarda proprio i controlli a distanza, dai quali

possono essere raccolte informazioni sensibili, mentre l'articolo 8, riguarda il divieto di indagini nella sfera privata del lavoratore stesso. Partendo dall'analisi dell'articolo 4, la prima cosa da tenere sempre presente, è che i controlli a distanza, devono essere svolti in modo da garantire un corretto bilanciamento tra l'interesse del datore di lavoro e il diritto alla riservatezza di cui il lavoratore deve godere. La prima cosa fondamentale, è che la normativa, riconosce al datore di lavoro, la possibilità di utilizzare questi strumenti di controllo, solamente ed esclusivamente per determinate esigenze. Queste esigenze sono: o per esigenze organizzative e produttive, o per ragioni di sicurezza del lavoro, o per ragioni di tutela del patrimonio aziendale. Quindi, nel momento in cui non ricorra una di tali esigenze l'attività di controllo è vietata. Altro paletto che la norma ha deciso di imporre è quello dell'accordo. Infatti, nell'articolo 4 troviamo proprio un obbligo al quale il datore di lavoro deve sottostare. Quest'obbligo consiste nel fatto che questi strumenti possono essere installati solamente se sono preceduti da un accordo o con le RSU, o con le RSA, o con le Associazioni sindacali comparativamente più rappresentative, presenti sul territorio nazionale, nel caso in cui l'impresa sia articolata in più unità produttive, dislocate in diverse regioni o provincie. Nel caso in cui, non si dovesse raggiungere l'accordo, la legge prevede la possibilità di sopperire a tale mancanza, attraverso l'autorizzazione dell'Ispettorato Nazionale o Territoriale del Lavoro. oltre a questo adempimento, il datore di lavoro deve anche sottostare all'obbligo d'informativa sulla privacy. L'utilizzo di questi sistemi infatti può portare al trattamento di dati personali. Tale trattamento deve essere effettuato rispettando i principi generali, ed in particolare il principio di trasparenza. Questo principio, prevede che gli interessati siano informati del fatto che stanno accedendo ad una zona che è videosorvegliata. Il titolare del trattamento, infatti, ha come obbligo quello di apporre idonei cartelli informativi. Ecco che, entra in gioco un tema sempre più prorompente e fondamentale ai giorni nostri. Tale tema riguarda l'angolo di visuale delle telecamere stesse, il quale oggi rappresenta uno degli adempimenti sempre più disatteso e oggetto di sanzioni. Le Linee Guida del comitato europeo per la protezione dei dati hanno specificato che nel momento in cui è necessario estendere la videosorveglianza alle immediate vicinanze dell'area di proprietà, il titolare del trattamento dovrebbe andare a utilizzare dei mezzi fisici e tecnici che siano in grado, per esempio di oscurare le zone non pertinenti. Il trattamento, perciò, deve essere effettuato utilizzando modalità che permettano di visualizzare solamente l'area da

proteggere. L'eventuale assenza di un'informativa adeguata comporta una condotta illecita. Infine, arriviamo al punto cruciale per la nostra analisi, ovvero come devono essere utilizzati le informazioni raccolte tramite i controlli a distanza e il tempo di conservazione delle immagini. Tali dati possono essere utilizzati, solamente per fini connessi al rapporto di lavoro, a condizione che il lavoratore però, sia stato adeguatamente e preventivamente informato sulla modalità di utilizzo di tali strumenti e sullo svolgimento dell'attività di controllo, la quale deve rispettare sempre le disposizioni in materia di trattamento dei dati personali. In questo caso, è opportuno soffermarci su questo articolo, poiché, come ben sappiamo lo statuto risale agli anni n'70 del secolo scorso; infatti, rispetto a quegli anni il contesto tecnologico è molto cambiato. Il concetto di distanza è mutato e si parla di distanza non più in senso spaziale, ma anche in senso temporale. Oggi la normativa, non può andare a considerare solamente gli impianti audiovisivi, ma dovrà anche riferirsi a qualunque strumento che consenta la ricostruzione, anche ex post, e qui entra in gioco il concetto di distanza temporale, dell'attività lavorativa del soggetto interessato. La giurisprudenza ha confermato la necessità di un'autorizzazione preventiva e di un accordo con le Rsa e le RSU, come già previsto dalla normativa. Il punto critico, riguarda gli strumenti necessari allo svolgimento dell'attività lavorativa, ma che al tempo stesso possono portare ad un controllo a distanza, e gli strumenti di registrazione degli accessi e delle presenze. Qui il punto cruciale sono gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa. Diventa, infatti, ancora più difficile capire quali possano essere gli strumenti da definire "necessari per lo svolgimento della prestazione" da quelli che potrebbero esserlo, ma che poi magari non lo sono. In questo caso, al fine di risultare necessari allo svolgimento della prestazione, occorre che ricorrano determinate caratteristiche. In primo luogo, gli strumenti devono essere messi a disposizione dal datore di lavoro per il concreto svolgimento della prestazione, l'utilizzo di tali strumenti dovrebbe imporre una partecipazione attiva del lavoratore in termini di utilizzo degli stessi, lo strumento deve essere palesemente necessario per la corretta esecuzione della prestazione dedotta nel contratto di lavoro. Altro tema critico è quello della conservazione delle immagini delle immagini raccolte, detto anche *data retention*. Anche qui, come accede sempre nelle normative italiane, ci troviamo di fronte alla necessità di dover ponderare gli interessi in gioco. Da un lato abbiamo l'interesse del titolare del trattamento alla conservazione delle immagini il più a

lungo possibile, dall'altro invece c'è il principio di minimizzazione. Il Garante ha osservato come le immagini non possono essere conservate più a lungo di quanto sia necessario alle finalità per le quali vengono acquisite. In questa cornice, spetta al Titolare del trattamento, secondo il principio di responsabilizzazione, prevedere i tempi di conservazione delle immagini, tenuto conto del contesto, delle finalità e del rischio per i diritti e le libertà delle persone fisiche. Va constato però che, in via generale, gli scopi della videosorveglianza sono, nella maggior parte dei casi, la sicurezza e la protezione del patrimonio. Solitamente, quindi, è possibile andare ad individuare eventuali danni entro uno o due giorni. Tenendo conto di questo e dei principi di minimizzazione e limitazione della conservazione, i dati raccolti dovrebbe essere cancellati dopo pochi giorni, anche facendo ricorso a sistemi di cancellazione automatica. Parlando sempre di controllo, non possiamo non trattare, dei cosiddetti "controlli difensivi[32]". Tali controlli, si fondano sul fatto che essi, oltre ad essere diretti alla tutela del patrimonio aziendale, mirano ad accertare l'esistenza di specifiche condotte illecite realizzate da singoli lavoratori, le quali non sono equiparabili al mero inadempimento della prestazione lavorativa. I controlli difensivi, si differenziano dai controlli a distanza per due ragioni: essi sono eseguiti in concreto *ex post,* ovvero in un momento successivo al venire in essere di un ragionevole sospetto e, partendo da concerti indizi, hanno come scopo quello di accertare specifiche condotte illecite imputabili a determinati lavoratori. Il bisogno, da parte del datore di lavoro, di ricorre a questo tipo di controlli deve emerge quindi da fatti contingenti e imprevedibili, che richiedono quindi un controllo circoscritto a determinati soggetti. Negli anni questi controlli hanno fatto molto discutere la giurisprudenza, a seguito anche di varie sentenze emanate. Sembra, infatti, che negli ultimi anni la giurisprudenza, sia arrivata ad ammettere i controlli difensivi detti "occulti" e i controlli difensivi effettuati tramite telecamere di video sorveglianza nascoste, quindi all'insaputa dei lavoratori. Secondo una sentenza della Grande Camera della Corte Europea, questi controlli risultano ammessi, purché siano giustificati dal fondato sospetto della messa in

[32]Corte di Cassazione, 12 novembre 2021, numero 34092: "In tema di cd. Sistemi difensivi, sono consentiti, anche dopo la modifica dell'art. 4 Stat. lav. ad opera dell'art. 23 D.Lgs. n. 151/ 2015, i controlli anche tecnologici posti in essere dal datore di lavoro finalizzati alla tutela di beni estranei al rapporto di lavoro o ad evitare comportamenti illeciti, in presenza di un fondato sospetto circa la commissione di un illecito, purché sia assicurato un corretto bilanciamento tra le esigenze di protezione di interessi e beni aziendali, correlate alla libertà di iniziativa economica, rispetto alle imprescindibili tutele della dignità e della riservatezza del lavoratore, sempre che il controllo riguardi dati acquisiti successivamente all'insorgere del sospetto".

atto di condotte illecite da parte dei lavoratori, per esempio se si sospetta di furti di merce all'interno dei luoghi di lavoro. A propositi di controlli, voglio portare alla luce un tema che fa molto discutere, ovvero quello del controllo della posta elettronica aziendale. La difficoltà di questo strumento, parte da individuarne la natura stessa di esso. Anche qui, ci vengono in aiuto alcune sentenze, che si contraddistinguono anche per il fatto di essere in disaccordo tra di loro. La prima sentenza è quella della Corte Suprema, la quale prende in esame l'artico 616 del c. p., il quale punisce chiunque venga a conoscenza del contenuto della corrispondenza elettronica di un altro soggetto. Secondo la Corte, il fatto non costituisce reato nel momento in cui è l'azienda stessa a prevedere una policy aziendale, che obbliga il lavoratore a comunicare al datore di lavoro la password del proprio pc. [33] La giurisprudenza però ha precisato che occorre fornire al lavoratore un'informativa adeguata nell'ipotesi di controllo sulla posta elettronica, sempre ai sensi del comma 3, art. 4 dello Statuo in esame.[34] Questo tipo di indirizzo è stato accolto, anche dal Garante Privacy, il quale ha emanato predisposizioni e raccomandazioni relative proprio all'utilizzo della posta elettronica e Internet in azienda. Tuttavia, risulta inoltre, necessario tenere conto di una pronuncia della CEDU, la quale ha ritenuto però, che anche le comunicazioni sul posto di lavoro, rientrino nel concetto di vita privata. Per la Cedu, il diritto alla privacy continua ad esistere anche nell'ambito appena descritto. Procedendo con l'analisi della normativa, il secondo articolo che voglio portare all'attenzione è l'articolo 8 dello Statuto, il quale riguarda il divieto di indagini sulle opinioni dei lavoratori. Parliamo di indagini su fatti che non riguardano strettamente il rapporto di lavoro. Questo divieto è inviolabile sia in fase di assunzione, ma anche in fase di svolgimento del rapporto di lavoro stesso. Attraverso questa norma, il legislatore ha inteso

[33]Tribunale di Roma, 2019:" Mentre le e-mail personali sono inaccessibili, pena la commissione di un reato e la violazione delle regole costituzionali sul segreto della corrispondenza, non così per le e-mail aziendali. Dunque, distinguendo tra account personale ed account aziendale, non c'è dubbio che per il primo il datore di lavoro ha il divieto categorico di accesso, mentre per il secondo il controllo delle e-mail è legittimo. Va altresì precisato che, stante quanto sopra, se è possibile utilizzare per l'accertamento ex post di comportamenti illeciti e la eventuale conseguente contestazione disciplinare, e-mail inviate da e all'indirizzo del dipendente, parallelamente ne è ammessa la loro produzione nel giudizio volto al sindacato della legittimità dell'atto espulsivo che ne è seguito, costituendo queste, presupposto necessari".

[34]Sentenza del Tribunale di Milano, 13 maggio 2019, numero 17778: "Viola la normativa sulla privacy il datore di lavoro che controlla il dipendente disponendone il pedinamento e l'accesso all'account di posta elettronica senza dare atto delle ragioni e delle effettive modalità del controllo. Non può essere configurato come legittimo ai sensi dell'art. 4, comma 2 Stat. lav. il controllo effettuato sull'account e-mail del dipendente in assenza dell'adeguata informazione prevista dall'art. 4, comma 3 Stat. lav. Le predette violazioni comportano l'inammissibilità delle risultanze ottenute dai controlli occulti e, dunque, l'inutilizzabilità delle informazioni acquisite".

circoscrivere il potere del datore di lavoro, imponendo una valutazione sullo stesso basata su criteri rigorosamente attitudinali. Questo divieto, non vieta a trecentosessanta gradi le indagini sui lavoratori, ma fornisce un perimetro entro il quale il datore di lavoro non dovrebbe andare. Il fulcro di questo articolo sono i "fatti rilevanti" ai fini della valutazione. Un esempio di fatto rilevante potrebbe essere ciò che rientra nella sfera giudiziale del soggetto. Questa norma disegna quindi, attorno al lavoratore un'area di riservatezza, ma l'oggetto del divieto, sono quei fatti, quelle opinioni che poi vengono ad esprimersi nella vita pubblica dell'individuo. C'è da chiarire però un aspetto importante, ovvero quello del concetto di indagine, alla base della quale, si presuppone un comportamento attivo, anche se minimo, nella raccolta delle informazioni.

3.4 IL NUOVO DECRETO TRASPARENZA

L'ultima normativa di cui voglio trattare è il decreto legislativo n. 107 del 27 giugno 2022, il quale a sua volta da attuazione alla direttiva 2019/1152 dell'Unione. Viene anche chiamato "Decreto Trasparenza"[35]. Questo decreto riguarda proprio la materia del diritto del lavoro e già nel leggere il primo articolo appare chiara quale sia l'intenzione del legislatore. Il decreto introduce nuovi doveri informativi, infatti oggi il datore di lavoro è tenuto ad informare il lavoratore circa gli elementi essenziali del rapporto di lavoro. Il presente decreto trova applicazione nelle più disparate forme contrattuali di lavoro, previste ovviamente dal diritto del lavoro italiano. Per comprendere l'importanza di questo decreto, sotto il profilo della protezione dei dati, occorre prima fare un passo indietro e soffermarci sul concetto di "trasparenza". Questo concetto ricorre più volte nel regolamento Ue riguardante proprio la protezione dei dati personali, anche se non troviamo al suo interno una definizione vera e propria. Nel diritto europeo questo concetto di trasparenza è divento espressione del principio di correttezza in relazione proprio al trattamento dei dati personali. La trasparenza è un obbligo trasversale, che si esplica attraverso tre elementi fondamentali. Il primo elemento consiste nel fornire agli interessati, le informazioni relative al corretto trattamento dei dati; il secondo elemento riguarda le modalità con cui il titolare comunica ai soggetti interessati i diritti di cui essi

[35]Di questo decreto, messo in relazione con il tema della privacy, come vedremo in questa trattazione, ne tratta Marco Soffientini. (Soffeintini M., "Decreto Trasparenza e nuovi obblighi in materia di privacy", fascicolo "Diritto & Pratica del Lavoro", fascicolo 37/2022, pagine 2219-2224)

godono; terzo elemento riguarda le modalità, utilizzate dal titolare, per agevolare gli interessati all'esercizio dei diritti di cui essi godono. Ecco che allora, il decreto introduce questi nuovi obblighi informativi, ai quali il datore di lavoro deve sottostare. La novità più significativa però la troviamo all'articolo 1 bis del regolamento, il quale è rubricato "Ulteriori obblighi informativi nel caso di utilizzo di sistemi decisionali o di monitoraggio automatizzati". Qui oltre al decreto, è importante citare anche una circolare del dicastero, la quale precisa che per definire meglio l'ambito di applicazione è necessario fare una distinzione tra i due sistemi in questione. Questo perché, il datore di lavoro ha l'obbligo di informare il lavoratore circa l'utilizzo di sistemi automatizzati, nel momento in cui essi siano rilevanti ai fini dell'assunzione o del conferimento dell'incarico, ai fine della gestione o della cessazione del rapporto di lavoro, ai fini dell'assegnazione di compiti o mansioni, e ha lo stesso obbligo nel momento in cui utilizza sistemi di monitoraggio automatizzati che incidano sulla valutazione, la sorveglianza, le prestazioni e sull'adempimento delle obbligazioni contrattuali. Detto questo però, dobbiamo notare subito che il legislatore, ci tieni a precisare che quanto viene disposto dall'articolo 4 dello Statuto dei lavoratori rimane invariato. Va precisato inoltre, che tra questi sistemi, non rientrano gli strumenti attraverso i quali è effettuata la rilevazione delle presenze dei lavoratori, purché questo rilevamento non vada ad innescare l'intervento di un sistema decisionale o di monitoraggio automatizzati che vada ad influire sullo svolgimento dell'attività del lavoratore. L'obbligo però non finisce qui. Infatti, il datore di lavoro, oltre ad informare sull'utilizzo di questi particolari sistemi, deve fornire ulteriore indicazione, le quali riguardano vari aspetti. In primis, deve andare ad indicare gli aspetti del rapporto di lavoro sui quali incide l'utilizzo di questi sistemi. Se per esempio, vi è la presenza all'interno dell'ambiente di lavoro, di un sistema di videosorveglianza, il datore di lavoro dovrà specificare se questo sistema è il frutto della necessità di esigenze organizzati e produttive, o di sicurezza del lavoro oppure di tutela del patrimonio. Secondo informazione da fornire, riguarda gli scopi e le finalità dei sistemi utilizzati. Questo significa che, nel sistema di videosorveglianza, andranno precisati le specifiche finalità per le quali viene utilizzato. Terzo elemento da fornire, riguarda la logica ed il funzionamento dei sistemi. Poi, il datore di lavoro deve fornire informazioni riguardo le categorie di dati e i parametri principali utilizzati per programmare o addestrare i sistemi utilizzati, e deve fornire informazioni riguardo le misure di controllo adottate per le

decisioni automatizzate, i processi di correzione e il responsabile del sistema di gestione. Infine, è necessario fornire informazioni riguardo il livello di accuratezza, robustezza e cybersicurezza dei sistemi utilizzati. Nel caso in cui queste informazioni dovessero mutare, il datore di lavoro è tenuto ad informare il lavoratore, almeno 24 ore prima, attraverso una comunicazione redatta in forma scritta. Questa comunicazione, deve essere data nel momento in cui queste modifiche hanno un impatto effettivo sullo svolgimento delle condizioni di lavoro, altrimenti si ritiene che l'obbligo venga meno. Il legislatore, però non si è limitato a questo. Infatti, il datore di lavoro è chiamato anche a dover fornire ulteriori informazioni, che riguardano proprio il trattamento dei dati personali. Dal testo emerge che il datore di lavoro deve integrare l'informativa con le indicazioni riguardanti la sicurezza dei dati, deve aggiornare il registro dei trattamenti, deve effettuare un'analisi dei rischi e una valutazione di impatto dei trattamenti ed infine procedere eventualmente con la consultazione preventiva dell'Autorità Garante per la protezione dei dati personali. In merito a questi ultimi due punti, pare che il decreto vada ad introdurre un obbligo generalizzato e indiscriminato di conduzione di una valutazione di impatto privacy in presenza di sistemi decisionali o di monitoraggio automatizzati. Uno dei nuovi obblighi è proprio quello di effettuare una valutazione di impatto privacy. Questo tipo di valutazione consiste in una procedura finalizzata a descrivere il trattamento dei dati, valutarne la necessità e la proporzionalità, e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei dati personali. Il titolare ha il dovere di valutare sempre i rischi, specialmente di fronte a trattamenti automatizzati. Se a seguito di una valutazione, il rischio risulta elevato, il titolare dovrà tenere aggiornata la valutazione di impatto privacy. Questa valutazione è un importante strumento di responsabilizzazione, che se fatta nella maniera corretta, può essere di aiuto al titolare stesso se egli dimostra di trattare i dati secondo gli obblighi previsti. Facciamo solo un breve accenno a quelle che sono le sanzioni previste a fronte di condotte illecite da parte del datore di lavoro. Il datore di lavoro che non adempie a questi obblighi, previsti dalla normativa, viene punito con una sanzione amministrativa per ogni lavoratore interessato. Trova applicazione, inoltre, la procedura di diffida in relazione alla tipologia delle informazioni omesse. Poi, si parla di sanzione amministrativa pecuniaria per ciascun mese di riferimento. La sanzione viene applicata, quindi per ciascun mese in cui il lavoratore svolga la propria attività senza che il datore di lavoro abbiamo adempiuto agli

obblighi informativi previsti. Abbiamo poi, la sanzione per fasce, ovvero, se la violazione si riferisce a più di cinque lavoratori la sanzione amministrativa va dai 400 ai 1500 euro, se invece si riferisce a più di dieci lavoratori, la sanzione va dai 1000 ai 5000 euro, senza la possibilità di ricorrere al pagamento in misura ridotta e neanche alla procedura di diffida. Infine, se la comunicazione delle medesime informazioni e dati non viene effettuata anche alle Rappresentanze sindacale unitaria o, in loro assenza, alle sedi territoriali delle associazioni sindacali comparativamente più rappresentative sul piano nazionale, vi è una sanzione amministrativa pecuniaria, che va dai 400 ai 1500 euro per ciascun mese in cui si verifica l'omissione.

3.5 IL FENOMENO DEL BRACCIALETTO ELETTRONICO E LA PEOPLE ANALYTICS

Il caso che ho voluto portare alla luca è si collegato all'intelligenza artificiale e alla privacy, in particolare con riferimento alla *People analytics*. Partiamo dal fatto che stiamo parlando di braccialetti elettronici. Questo tipo di tecnologie rientrano nei cosiddetti "*wearable devices*", i quali simboleggiano in maniera evidente a che punto siamo arrivati e dove arriveremo con il progresso tecnologico. Questo tipo di dispostivi indossabili possono essere definiti anche come una sorta di computer in miniatura che vanno ad integrarsi con chi ne usufruisce e permettono di compiere diverse attività a mani libere e di restare, in costante contatto con l'ambiente circostante e con il dispositivo stesso. Questo tipo di dispositivi si differenziano dal tablet e computer poiché la connessione è una connessione costante con chi li indossa, la quale permette di estrapolare un numero maggiore di informazione sull'individuo, sui suoi spostamenti e su ogni azione che lui compie. Il dispositivo, infatti conosce le coordinate geografiche dell'ambiente in cui si muove l'individuo e sa se il soggetto si sta muovendo all'interno del magazzino, ad esempio, o se si trova al di fuori di esso. Non manca la volontà di alcuni datori di lavoro di ricorrere all'utilizzo di tali strumenti in modo da poter ottimizzare la prestazione di lavoro dei dipendenti. Ha creato stupore ed è stata molto dibattuta la scelta di Amazon di brevettare *l'ultrasonic bracelet and receiver for detecting position.* Questo braccialetto avrebbe la funzione di andare a sostituire il lettore scanner utilizzato dai lavoratori di Amazon. Per capire perché Amazon ha voluto brevettare questi braccialetti, è necessario

innanzitutto fare una precisazione: i magazzini Amazon coprono aree molto vasta, dove le merci vengono stoccate con l'aiuto di questi scanner, i quali registrano e gestiscono l'immagazzinamento della merce. Il modello di business adottato da Amazon si incentra attorno all'intuizione secondo cui i clienti acquistano attraverso ogni ordine da loro effettuato, una serie di prodotti diversi tra loro e non stock di prodotti identici. Da questo, deriva la scelta della società di non disporre le merci in modo ordinato all'interno del magazzino, ma di collocarle in ordine casuale. In questo modo, solamente il sistema informatico aziendale è in grado di poter indicare la collocazione esatta di quel determinato prodotto e di conseguenza il dipendente può svolgere il suo lavoro solo se connesso allo strumento informatico. Per fare questo Amazon utilizza un lettore ottico, ma il prossimo passo dovrebbe essere quello di sostituirlo con questo braccialetto elettronico. Questo braccialetto dovrebbe funzionare principalmente in questo modo: saranno posizionati dei sensori su ogni scaffale, i quali saranno in grado di andare a percepire l'esatta posizione delle mani del lavoratore, in questo modo potranno guidare i movimenti del lavoratore attraverso l'impulso vibrante e, in caso, poterlo anche correggere se sta svolgendo qualcosa in maniera errata. Altra funzione che potrebbe avere il braccialetto è quella di contenere al suo interno un timer, il quale permetterebbe al lavoratore di visualizzare sul dispositivo un conto alla rovescia, in modo da poter prendere visione di quanto tempo resta al dipendente per evadere l'ordine. Infine, questo braccialetto avrebbe anche la funzione di andare a registrare quanto tempo intercorre tra l'arrivo dell'ordine e la battitura del codice a barre. Questo permetterebbe di registrare dati sull'attività lavorativa che possono essere utilizzati anche ai fini disciplinari. Dopo aver presentato il funzionamento di questo braccialetto, è importante metterlo in relazione con le normative vigenti. Al di là dell'articolo 4 dello Statuto dei lavoratori post Jobs Act riguardante i controlli a distanza e gli strumenti utilizzati dal lavoratore per rendere la prestazione, bisogna porre l'attenzione sul trattamento dei dati che possono essere raccolti tramite l'utilizzo del braccialetto elettronico. In primo luogo, bisogna sempre tenere presente che qualsiasi trattamento dei dati personali deve soddisfare finalità legittime, determinate ed esplicite e non può portare all'utilizzo di tali dati per scopi non compatibili con quelli fissati in origini e di cui il lavoratore ha ricevuto l'informativa. Prendiamo il caso ipotetico in cui un datore di lavoro decida di adottare questi dispositivi all'interno della sua azienda e che tramite l'utilizzo di essi riesca a registrare dati sull'adempimento

della prestazione, sulla velocità, sui tempi di esecuzione del lavoro, sulle pause e i riposi dei lavoratori, per poi andarli ad utilizzare per scopi disciplinari. Ci si chiede se questo possa essere legittimo e la risposta risulta negativa, poiché si tratta di un controllo che andrebbe a compromettere la dignità delle persone. Questo valore, infatti, risulterebbe poi compromesso ulteriormente, se la legge arrivasse ad autorizzare un controllo continuo e stressante sulla persona stessa, per finalità connesse all'aumento della produttività del datore di lavoro. Tale questione, vista da questo punto vista, si collega allora alla valutazione delle *performance* del lavoratore e al concetto di *People analytics.* Con la digitalizzazione del lavoro la valutazione delle performance del lavoratore ha portato all'innovazione delle tecniche di controllo e valutazione tramite l'utilizzo dei nuovi output: *i dati che codificano le prestazioni.*[36] Queste valutazioni, si legano al concetto di *People analytics,* poiché essa è: *la raccolta e l'analisi di grandi quantità di dati per identificare modelli di atteggiamento e prevedere comportamenti di gruppi e comunità.* Queste tecniche hanno acquisito grande importanza perché sono strumenti in grado di acquisire, correlare ed interpretare dati dei lavoratori in modo da poter ottenere un'analisi dei singoli e delle loro interazioni con l'organizzazione per il raggiungimento degli obbiettivi prefissati. Questo tipo di tecniche acquisiscono il nome di *HR Analytics*[37] nel momento i cui i dati acquisiti rivestono un ruolo centrale per le strategie nell'ambito della gestione delle risorse umane. L'analisi tramite queste tecniche, inoltre, viene svolta su una grande quantità di dati eterogenei, i quali vengono elaborati attraverso l'utilizzo di sistemi di intelligenza artificiale. Analizzare i dati, tramite questi sistemi e tramite tecniche di People Analytics può portare a nuove criticità in relazione alla valutazione delle performance. Tutto questo può condurre ad un'estensione incontrollata delle prerogative datoriali, esercitate tramite un monitoraggio pervasivo e persistente.[38] Le

[36]Del Giglio, sottolinea come l'uso di piattaforme o l'implementazione negli uffici, genera un'evoluzione destinata a potenziare la connessione e la collaborazione tra i lavoratori (Ilaria Del Giglio, "Valutazione della performance mediante tecniche di People Analytics. Privacy in employment o innovazione", in Journal of Etichics and legal Technologies, volume 3(2), novembre 2021, pagine 103-137).

[37]Del Giglio, specifica, inoltre, che nel momento in cui i dati acquisiti riguardano anche le caratteristiche personali dei soggetti, come le attitudini o le percezioni, siamo di fronte al concetto di "*Sentiment Analysis*". (Ilaria Del Giglio, "Valutazione della performance mediante tecniche di People Analytics. Privacy in employment o innovazione", in Journal of Etichics and Legal Technologies, volume 3(2), novembre 2021, pagine 103-137).

[38]Il poter andrebbe a risultare in questo modo svincolato da una reale supervisione umana e potrebbe portare quindi ad una sorta di "dittatura del calcolo" (Ilaria Del Giglio, "Valutazione della performance mediante tecniche di People Analytics. Privacy in employment o innovazione", in Journal of Etichics and Legal Technologies, volume 3(2), novembre 2021, pagine 103-137).

principali criticità che si possono contestare all'utilizzo delle tecniche di People Analytics[39] sono: le fonti con cui si acquisiscono i dati, tipi di dati che vengono acquisiti, tipo di trattamento eseguito e strumento con cui viene eseguito il trattamento. Di tutte queste criticità abbiamo già parlato nel primo paragrafo di questo capitolo, ma è importante cercare di metterle in relazione con il caso dei braccialetti elettronici. Per ciò che concerne le fonti, il discorso ovviamente non può prescindere dall'articolo 4 dello Statuto dei lavoratori, il quale regolamenta il controllo dei lavoratori. Questo poi deve essere messo in relazione con le fonti che vanno a regolare l'utilizzo dei dati acquisiti. La possibilità di acquisire informazioni sui lavoratori per tutti i fini connessi al rapporto di lavoro, dipende dalla natura attribuita allo strumento utilizzato. Ovvero se questo strumento è strettamente necessario a rendere la prestazione oppure no. Anche in questo caso però bisogna fare una precisazione, poiché ci troviamo di fronte a due scuole di pensiero differenti: la prima ci dice che è da considerarsi strumento di lavoro solamente il dispositivo o software[40] indispensabile allo svolgimento delle mansioni del lavoratore. La seconda ci dice che è da considerarsi strumento di lavoro anche quello che solamente facilita, ottimizza e semplifica il lavoro. Questa norma non basta però, bisogna anche fare riferimento alla norma sulla privacy; quindi, nel caso in cui il braccialetto rientrasse negli strumenti di lavoro, non vuol dire che il lavoratore possa controllare costantemente il comportamento dei suoi lavoratori e utilizzare i dati raccolti a suo piacimento. Seconda questione, riguarda la tipologia di dati acquisiti, infatti come ben sappiamo bisogna sempre porre attenzione ai dati personali e particolari dei lavoratori. Questa eventualità si può verificare nel momento in cui si utilizzano dispostivi dotati di servizio IOT, ovvero

[39]Del Giglio, specifica come l'analisi fatta mediante queste tecniche di people analytics consenta di ridurre i limiti quantitativi dell'operato umano, poiché esse si svolgono su una grande quantità di dati che sfruttano appunto i sistemi di Intelligenza Artificiale (Ilaria Del Giglio, "Valutazione della performance mediante tecniche di People Analytics. Privacy in employment o innovazione", in Journal of Etichics and Legal Technologies, volume 3(2), novembre 2021, pagine 103-137).

[40]In questo caso Del Giglio specifica come a proposito di software, bisogna precisare anche i cosiddetti file di log e BYOD. I file di log sono file che effettuano una registrazione sequenziale e cronologica delle operazioni compiute da un sistema informatico (come i server). I dispositivi BYOD sono dispositivi di proprietà del dipendente in cui viene installato un applicativo, di cui il titolare è il datore di lavoro, i quali consentono il collegamento tra il dipendente e la rete aziendale per rendere la prestazione lavorativa. Il BYOD, a causa della sua natura risulta potenzialmente in grado di acquisire dati e informazioni personali di chi lo utilizza, tanto che già nel 2015 il Garante Europeo per la Protezione dei Dati ha provveduto a pubblicare delle Linee guida in materia di dati personali e *mobile devices* (Ilaria Del Giglio, "Valutazione della performance mediante tecniche di People Analytics. Privacy in employment o innovazione", in Journal of Etichics and legal Technologies, volume 3(2), novembre 2021, pagine 103-137).

Internt of things. Il termine IOT viene utilizzato per indicare oggetti, i quali interagiscono fra loro mediante connessione di rete. Interazioni che possono essere con pc e smartphone, ma anche con i dispositivi indossabili, quali i *wearable device.* Le potenzialità di un servizio IOT si possono apprezzare soprattutto se messe in relazione con i dispositivi appena citati. Ecco che, definitivo questo quadro ci rendiamo conto di come l'utilizzo di questi braccialetti, collegati ad un servizio IOT, rende sempre più concreta la possibilità di acquisire e processare dati personali e particolari dei lavoratori. Penultima questione riguarda il trattamento di tali dati. Il datore di lavoro non può andare a utilizzare il braccialetto elettronico per avere una ricostruzione del comportamento del lavoratore. Questa argomentazione è supportata da varie ragioni. Innanzitutto, l'interesse legittimo del datore di lavoro nell'utilizzare tale dispositivo dovrebbe essere quello secondo cui il datore di lavoro consegna il braccialetto al lavoratore poiché tale strumento è utile alla produzione. Quindi il trattamento trova la sua base giuridica nell'esigenza di aumentare la produttività e non nell'esigenza di sottoporre il lavoratore ad un controllo costante. Un controllo di questo genere, infatti, porterebbe solamente a mettere sotto "pressione" la persona e questo non è compatibile con la protezione della sua dignità. Se venisse applicato un simile trattamento i dati raccolti sarebbero inutilizzabili. Infine, il datore di lavoro deve sempre conformare il trattamento dei dati alle regole di trasparenza, correttezza, limitazione delle finalità e minimizzazione. Ultima questione, riguarda gli strumenti utilizzati per il trattamento. Le criticità in questo caso, sta nel fatto che questi utilizzano tecniche di IA di *machine learning* e *deep learning,* definibili anche *black box.* Ultimo tema che voglio affrontare riguarda un tema affrontato da Claudio Sarra, ovvero le procedure di reclutamento al lavoro mediante strumenti di Intelligenza Artificiale. Per prima cosa la "biometria" è stata definita come "l'insieme delle tecniche di identificazione o di 'misurazione' dell'essere umano attraverso la rilevazione di determinate caratteristiche fisiche o comportamentali che vengono tradotte in sequenze matematiche e conservate in banche dati elettroniche" nota. Nella realtà attuale le misurazioni biometriche sono diventate sempre più agevoli, grazie alla grande quantità di immagini presenti nel web. In questo modo si è andati oltre l'identificazione di "prima generazione" e quindi oltre l'identificazione univoca, ma si sfruttano queste immagini per andare a ricavare nuovi dati fisici e comportamentali dell'essere umano. Inoltre, se si va

a mettere insieme la grande quantità di dati raccolti, con le tecniche di *data mining*[41], si può dare vita ad un modello, ad un ideal-tipo di soggetto che fungerebbe da referente statistico al fine di includere o escludere alcuni soggetti, a seconda del loro grado di corrispondenza con il modello appena citato. Se prendiamo per esempio il mondo del lavoro, questo tipo di modello potrebbe essere preso come riferimento per per-selezionare i candidati o classificare le loro richieste in vista di una seconda fare di selezione, sia che sia automatizzata o basata su decisioni umane. Nell'ambito lavorativo però, le regole sono molto restrittive per quanto riguarda il processamento dei dati personali dei lavoratori o dei candidati per un posto di lavoro ed in più possono richiedere la necessità di avere alla base una giustificazione rigorosa. Questa giustificazione riguarda la relazione tra l'uso dei dati biometrici e le competenze e abilità richieste per un determinato impiego. Nella realtà attuale, le società di reclutamento al lavoro utilizzano strumenti di *big data analitycs* nell'organizzazione delle procedure di selezione che vadano a coinvolgere una grande quantità di candidati. In questi casi, la questione relativa alla privacy è molto delicata, poiché è nell'interesse delle società poter conoscere almeno un minimo il candidato, ma dall'altro tecniche di *data mining* e profilazione possono andare a rivelare molto di più di quello che un datore di lavoro ha il diritto di sapere sul candidato. Ecco perché molte legislazioni adottano un approccio restrittivo nei confronti dell'utilizzo di questi tipi di tecniche. In questo contesto, il GDPR ci fornisce un quadro generale, in cui vediamo come l'articolo 88 della normativa stessa da ampio potere agli stati membri di poter emanare norme più precise al fine di assicurare le libertà fondamentali. Prima di questo però, già l'articolo 4 ci parla di dati biometrici e dice che sono "dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici". Da qui già vediamo come la recente proposta di regolamento risulta in linea con questa definizione di dato biometrico fornita dal GDPR. Proseguendo poi, l'articolo 9 del GDPR va a proibire il processamento dei dati genetici e biometrici, poiché essi risultano volti ad

[41]"Estrazione dati, cioè l'attività di selezione, esplorazione e modellizzazione di grandi quantità di dati, attraverso tecniche statistiche, al fine di individuare regolarità o relazioni non note a priori e traducibili in informazioni chiare e rilevanti. Il d. m. inizia con la traduzione delle esigenze in una problematica da analizzare e la raccolta, preparazione e pulizia della base dati necessaria all'analisi. (Enciclopedia Treccani, anno 2012)".

identificare in modo univoco una persona. Da questo si possono ricavare due riflessioni importanti in merito al quadro europeo sui dati biometrici: per prima cosa se non sono oggettivamente idonei a conoscere o confermare l'identità di una persona in maniera univo o se anche lo sono, ma non vengono usati con questo scopo, il loro trattamento non richiede particolare legittimazione. Da questo emerge come non tutte le misurazioni fisiche o comportamentali offrono dati biometrici. La seconda riflessione è che se i dati vengono considerati biometrici e vengono usati con l'intenzione di procedere all'identificazione di una persona in maniera univoca, il *data controller* dovrà ricordarsi che l'articolo 9 del GDPR proibisce l'uso dei dati biometrici con tale scopo. Resta da tenere presente però, che il reclutamento non per forza deve o può comprendere il trattamento di dati biometrici e che l'articolo 88 del GDPR lascio spazio alle normative dei paesi membri. Per quanto concerne l'ordinamento italiano il trattamento dei dati biometrici è soggetto a misure più restrittive e questo approccio è utilizzato anche nell'ambito del reclutamento. L'articolo 8, dello Statuto dei lavoratori vieta al datore di lavoro qualsiasi indagine, schedatura, classificazione negli ambiti che riguardano le opinioni politiche, religiose o sindacali e su fatti non rilevanti ai fini del rapporto di lavoro. Il medesimo divieto viene applicato anche alle agenzie per il lavoro e agli altri soggetti pubblici o privati autorizzati o accreditati alla preselezione di lavoratori, anche nel caso in cui vi sia il consenso del datore di lavoro, sempre che tali dati non incidano sullo svolgimento dell'attività lavorativa o che costituiscano un requisito essenziale e determinante ai fini dello svolgimento dell'attività lavorativa. Ecco che, anche se non si parla esplicitamente di biometria, molti dei dati indicati sono tratti da caratteristiche fisiche o comportamentali. Tali divieti, dovrebbero implicare l'impossibilità di utilizzare tecniche di data mining idonee a raccogliere dati indirettamente utilizzabili a partire da dati non utilizzabili. La liceità dei dati utilizzati quindi deve essere valutata alla luce di due requisiti: nessun dato del candidato può essere trattato a meno che non sia strettamente correlato alle sue attitudini professionali e a meno che non sia necessario per il suo inserimento nell'ambito lavorativo. Lo spazio quindi, per l'uso di strumenti di Intelligenza Artificiale con finalità di *recruiting* è alquanto ristretto e, nel caso vengano utilizzati, deve esserci alla base una giustificazione e spiegazione di alto livello circa le modalità di utilizzo dei dati dei candidati. In questo contesto così delineato, si colloca la proposta di regolamento, la quale anch'essa tratta di dati biometrici. Il quadro normativo

europeo appare quindi in questo modo: “ a) i dati che derivino da misurazioni fisiche o comportamentali possono essere trattati purché ricorrano le condizioni di legittimità stabilite in generale nonché siano adempiuti tutti gli altri adempimenti previsti in generale; b) essi possono essere, utilizzati, in questo contesto, anche per il controllo e la correzione dei *bias* di sistema; c) i dati biometrici che non siano usati col fine di identificare univocamente la persona fisica seguono le medesime regole; d) il trattamento dei dati biometrici che siano, invece, usati a tale scopo, incontrerà la proibizione generale di cui all’art. 9 del GDPR”. A tale articolo si aggiunge la deroga contenuta nella Proposta di regolamento di IA, la quale consente l’utilizzo di tali dati per il monitoraggio e la correzione dei *bias* di sistema. Quindi, nel caso della normativa italiana, per quel che concerne l’utilizzo dei sistemi di reclutamento tramite l’utilizzo di sistemi di Intelligenza Artificiale, rimane invariato anche nel caso in cui dovesse essere approvata del tutto l’Artificial Intelligence Act.

CONCLUSIONE

Dopo aver trattato le varie normative e portato l'esempio di un caso quasi concreto, passiamo a chiudere questa trattazione. Da questa trattazione credo che si comprenda a pieno la necessità di emanare una nuova normativa, la quale non sia solo una proposta, ma sia a tutti gli effetti un atto normativo che possa darci delle definizioni e dei limiti di movimento all'interno di questo spazio in continua evoluzione, quale l'Intelligenza Artificiale. Tali tecnologie nuove, come abbiamo visto, ormai hanno acquistato e stanno acquistando sempre più importanza, infatti tanti di questi nuovi strumenti, risultano ormai essenziali al giorno d'oggi. Attualmente il tema dell'Intelligenza artificiale, associato al lavoro è un tema che recentemente ha iniziato ad interessare anche la giurisprudenza, questo perché come sappiamo le norme cambiano, in base all'evoluzione della società. Nuovi fenomeni richiedono che rischiano di mettere in pericolo i nostri diritti, portano alla necessità di emanazione di nuove norme, o di modificare le norme precedenti. In questo contesto credo che la proposta di regolamento europeo, ovvero l'Artificial Intelligence act, rappresenti già una presa di conoscenza della necessità di andare a delimitare quello che questi nuovi sistemi possono fare. Il fatto poi di classificare i sistemi in base al rischio, credo sia stata una scelta corretta, perché appunto quello che a noi deve interessare, a mio avviso, sono i rischi a cui va incontro una persona nel momento in cui decide di utilizzare questi strumenti. Il punto centrale per il legislatore nell'emanazione di una nuova norma è sempre stato quello di andare a tutela la parte più debole, quella più esposta al rischio di vedersi lesi i propri interessi e i propri obbiettivi. In questo caso la parte più debole, siamo noi utilizzatori, perché data la complessità di questi sistemi, non sempre siamo in grado di capire, o abbiamo degli studi alla base che ci permettano di capire come funzionano questi sistemi. Ecco perché ritengo che la scelta di classificare i sistemi in base al livello di rischio, sia la scelta più appropriata. Mi auguro fortemente che questa proposta di regolamento venga approvata, in modo da poter essere applicato in tutti i paesi membri. Questo perché il trattamento dei dati personali è un problema serio, che molto spesso, a mio avviso, viene anche sottovalutato anche dall'utilizzatore stesso. Credo che ci sia capitato molte volte di dare il consenso o accettare molte cose all'interno dei siti internet senza neanche minimante leggere cose ci stessero chiedendo o cosa prevedessero. Questo già dimostra come noi stessi, in molte situazioni, sottovalutiamo il problema e magari ci rendiamo conto di quelli che abbiamo fatto solamente a posteriori,

quando ormai forse è troppo tardi e tante delle nostre informazioni, dei nostri dati, sono già stati acquisiti. Altro problema, è sempre la trasparenza, anche questa da noi viene sottovalutata. Questo perché molto spesso noi utilizzatori la pretendiamo questa trasparenza, ma poi neanche ci informiamo in maniera attiva su chi andrà a trattare i nostri dati. Ora però cerco di spostare la mia attenzione sul tema centrale della nostra trattazione, ovvero questi nuovi sistemi di intelligenza artificiale in rapporto alla privacy del lavoratore. Di per sé già la privacy del lavoratore è un tema centrale quado si parla di tutela del lavoratore stesso, il quale come sappiamo è la parte debole del rapporto di lavoro. Come è giusto che sia il mio datore di lavoro non è tenuto a dover sapere tutto quello che faccio al di fuori dell'ambito lavorativo, quello in cui credo, con chi mi frequento, ecc. Tutto ciò che non è strettamente legato al rapporto di lavoro, rientra in quella sfera di riservatezza che deve essere garantita al lavoratore. Questa riservatezza però, come abbiamo visto, rischia di essere compromessa con queste nuove tecnologie, le quali sono molto invasive e in grado di raccogliere una grandissima quantità di dati in poco tempo. Anche in questo senso, credo che le norme attuali, quali il Codice Privacy e lo Statuto dei Lavoratori, non bastino più, forse è necessario una normativa che regolamenti questo fenomeno o che comunque preveda delle regole specifiche che si aggiungono a quelle già emanate e che aiutino alla tutela della privacy. Già parlando di smartphone e di social network, vediamo come è più facile venire a sapere quello che il lavoratore fa al di fuori dell'ambiente di lavoro e al di fuori del suo orario di lavoro. questo problema però, abbiamo visto che può crearsi anche all'interno dell'ambiente di lavoro, tramite l'utilizzo di alcuni dispositivi nuovi, che sono stati brevettati da poco, i quali possono condurre, se utilizzati nella maniera sbagliata, ad un controllo costante del lavoratore, il quale piò portare ad uno stress elevato. Oltre alla privacy quindi, si può parlare anche di salute nei luoghi di lavoro. Credo che anche questo debba essere un tema da prendere in considerazione. Tornando però al centro della nostra trattazione, ciò che mi ha molto colpito è come il mondo del lavoro stia cambiando ad una velocità strabiliante, ma che allo stesso fa quasi paura, perché mi chiedo se noi, in particolare dal punto di vista normativo, saremo in grado di stare dietro a questa evoluzione e se le norme attuali basteranno e per quanto ancora andranno bene. Al fronte di questo è sempre necessario e importante fare dei bilanciamenti. Parlando, per esempio, del fenomeno della People analytics, bisogna sempre fare un bilanciamento tra la valutazione delle

performance e il controllo sul lavoratore. Il datore di lavoro è dotato appunto tra tutti i poteri, del poter di controllo, ma non deve mai dimenticarsi che la persona da controllare ha una dignità, che in nessun modo deve essere calpestata. Parlando però di dati e privacy nel lavoro, molte volte la difficoltà sta nell'andare a decifrare i dati stessi che vengono raccolti, questo per poter andare a interpretare i comportamenti digitali dei lavoratori e capire quali dati possono essere utilizzati e quali no ai fini del lavoro. Questo è uno dei principali problemi derivanti dalla raccolta di dati. Quindi è necessario compiere una "significazione" dei dati che vengono raccolti, poiché non tutti per forza ci possono portare ad avere informazioni utili per il nostro scopo. Quello che sarebbe auspicabile per la Del Gilio, è quello di andare a coinvolgere anche i dispendenti in questo processo. Interpretare i dati e l'intellegibilità dei sistemi di IA dovrebbe andare a fornire un modello di organizzazione che integri queste People Analytics, attraverso un processo partecipativo inclusivo dei dipendenti stessi appunto. Questa collaborazione può essere accolta come un'opportunità in grado di modificare i vari modelli organizzativi, dandoci la possibilità di avere modelli che ci permettano di avere una progettazione del lavoro più ergonomica. Il coinvolgimento dei dipendenti allora, sembra la strategia più adatta perché più i dipendenti saranno coinvolti nel processo valutativo, maggiore sarà l'identificazione con l'organizzazione e l'evoluzione di comportamenti innovativi. In sintesi credo sia necessario, comprendere l'importanza dello sviluppo di questi sistemi senza andare a vietare l'utilizzo di questi o senza creare troppo timore nella società nei confronti dell'utilizzo di tali sistemi. Questo perché tali sistemi, come già analizzato, possono portare dei benefici alla società, l'importante è semplicemente mettere dei limiti all'interno dei quali questi strumenti possono essere sviluppati e utilizzati, senza andare a creare aree grigie, non regolamento in cui rischiano di svilupparsi sistemi che vadano a violare i nostri diritti fondamentali. credo, inoltre, che ormai non si possa più tornare avanti con lo sviluppo tecnologico e che soprattutto questo non sia conveniente per nessuno, in termini di costi, fatica e benefici, la cosa importante è prendere atto che questi sistemi esistono, che fanno parte della nostra e imparare a conviverci. Per fare questo è importante che gli sviluppatori rispettino le regole di trasparenza e chili utilizza rispetti le regole riguardanti l'informativa. In questo modo se io so come un sistema di Intelligenza Artificiale funzione e con quale scopo i miei dati vengono raccolti, posso anche capire come tutelarmi al meglio e come evitare violazioni di miei diritti e interessi.

Per fare questo, è inoltre importante iniziare a dare alle persone la possibilità di formarsi, almeno in maniera base su come funzionino questi sistemi. Non dobbiamo diventare tutti esperti o studiosi di questa materia, ma almeno essere curiosi, informarci oppure inserire delle iniziative apposite a disposizioni di tutti, in modo da poter apprendere al meglio questo nuovo mondo in continua evoluzione.

BIBLIOGRAFIA

Aimo Mariapaola, “Dalle schedature dei lavoratori alla profilazione tramite algoritmi: serve ancora l’art. 8 dello Statuto dei lavoratori?”, in *Lavoro e diritto*, fasc. 3-4, estate-autunno 2021, pagg. 585-600.

Amidei Andrea, “La governance dell’Intelligenza Artificiale: profili e prospettive di diritto dell’Unione Europea”, in Ugo Ruffolo (a cura di), in *Intelligenza artificiale. Il diritto, i diritti, l’etica*, Giuffrè, 2020, pagg. 571-588.

Barbieri Luca, Bevante Rosamaria e Mamprin Aurora, “Sistemi decisionali o di monitoraggio automatizzati e controlli a distanza”, in *Diritto & Pratica del lavoro*, fasc. 15/2023, pagg. 923-937.

Carmelo Romeo, ”Le nuove regole del diritto del lavoro tra algoritmi e incertezza delle tutele”, in *Il Lavoro nella giurisprudenza*, fasc. 2/2021, pagg. 129-141.

Casonato Carlo, Marchetti Barbara, “Prime osservazioni sulla proposta di regolamento dell’Unione Europea in materia di intelligenza artificiale”, in *BioLaw Journal – Rivista di BioDiritto*, fasc. 3/2021, pagg. 415-437.

Costantini Federico,”Il Regolamento (UE) 679/2016 sulla protezione dei dati personali”, in *Il Lavoro nella giurisprudenza*, fasc. 6/2018, pagg. 545-555.

D’Avack Lorenzo, “La rivoluzione tecnologica e la nuova era digitale: problemi etici”, in Ugo Ruffolo (a cura di), in *Intelligenza artificiale. Il diritto, i diritti, l’etica*, Giuffrè, 2020, pagg. 3-27.

Del Giglio Ilaria, “Valutazione della performance mediante tecniche di People Analitics. Privacy in employement, controllo o innovazione?”, in *Journal of Ethics and Legal Technologies*, Volume 3(2) – November 2021, pagg. 103-137.

Finocchiaro Giusella, “Riflessioni su intelligenza artificiale e protezione dei dati personali”, in Ugo Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l’etica*, Giuffrè, 2020, pagine 237-247.

Floridi Luciano, “Etica dell’intelligenza artificiale. Sviluppi, opportunità, sfide”, Raffaello Cortina Editore, 2022.

Maurelli Roberto, “Sistemi decisionali e di monitoraggio automatizzati: obbligo informativo”, in *Guida alle paghe*, 5/2023, pagg. 314-318.

Moro Paolo, “Macchine come noi. Natura e limiti della soggettività robotica”, in Ugo Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l’etica*, Giuffrè, 2020, pagg. 45-61.

Moro Paolo, “Intelligenza artificiale e tecnodiritto. Fondamenti etici ed innovazione legislativa”, in Paolo Moro (a cura di), E*tica, diritto e tecnologia. Percorsi dell’informatica giuridica contemporanea*, Franco Angeli, 2021, pagg. 7-24.

Natali Luca Christian, Piselli Sabrina, “Intelligenza artificiale e protezione dei dati personali dei lavoratori”, in *Diritto & Pratica del Lavoro*, fasc. 26/2021, pagg. 1673-1686.

Natali Luca Christian, “Intelligenza artificiale e impatto sul lavoro”, in *Diritto e pratica del lavoro*, fasc. 23/2023, pagg. 1446-1456.

Natali Luca Christian, “Tutela del patrimonio aziendale e dei lavoratori”, in *Diritto & Pratica del lavoro*, fasc. 2/2023, pagg. 117-124.

Pagallo Ugo, “Etica e diritto dell’intelligenza Artificiale nella governance del digitale: il Middle-out Approach”, in Ugo Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l’etica*, Giuffrè, 2020, pagg. 29-44.

Peruzzi Marco, “Intelligenza artificiale e tecniche di tutela”, in *Lavoro e Diritto*, fasc. 3, estate 2022, pagg. 541-559.

Pizzetti Franco, “La proposta di Regolamento sull’IA della Commissione Europea presentata il 21.4.2021 (COM(2021) 206 final) tra Mercato Unico e competizione digitale globale”, in *Diritto di Internet*, fasc. 4/2021, pagg. 590-599.

Quintarelli Stefano, Corea Francesco, Fossa Fabio, Loreggia Andrea, Sapienza Salvatore, “AI: profili etici Una prospettiva etica sull'intelligenza artificiale: princìpi, diritti e raccomandazioni”, in *Biolaw Journal*, fasc. 3/2019, pagg. 183-204.

Renzi Samuele, “Decisioni automatizzate, analisi predittive e tutela della privacy dei lavoratori”, in *Lavoro e diritto*, fasc. 3, estate 2022, pagg. 583-603.

Rotondi Francesco, "Controllo della posta del lavoratore", in *Guida alle paghe*, fasc. 9/2022, pagg. 559-562.

Sarra Claudio, “Business Intelligence ed esigenze di tutela: criticità del c.d. Data Mining”, Paolo Moro, Claudio Sarra (a cura di), *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, Franco Angeli, 2017, pagg. 41-63.

Sarra Claudio, “L’uso di dati biometrici nelle procedure di reclutamento al lavoro mediante strumenti di Intelligenza Artificiale. Difficoltà normative multilivello.”, in *Journal of Ethics and Legal Technologies,* Volume (4)2, Novembre 2022, pagg. 27-49.

Sartor Giovanni e Lagioia Francesca, “Le decisioni algoritmiche tra etica e diritto”, in Ugo Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l’etica*, Giuffrè, 2020, pagg. 63-92.

Soffientini Marco, “Sistemi di videosorveglianza in azienda: progettazione e errori comuni da evitare”, in *Diritto & Pratica del Lavoro*, fasc. 5/2023, pagg. 322-326.

Soffientini Marco, “Sicurezza dei dati personali dei lavoratori”, in *Diritto & Pratica del Lavoro*, fasc. 27/2022, pagg. 1727-1731.

Soffientini Marco, “Decreto Trasparenza e nuovi obblighi in materia di privacy”, fascicolo *Diritto & Pratica del Lavoro*, fasc. 37/2022, pagg. 2219-2224.

Soffientini Marco,“Intelligenza artificiale e riconoscimento facciale negli ambienti di lavoro”, *Diritto & Pratica del Lavoro*, fasc. 17/2021, pagg. 1035-1040.

Zanuzzi Anna Chiara, “Internet of things e privacy. Sicurezza e autodeterminazione informativa”, in Paolo Moro, Claudio Sarra (a cura di), *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, Franco Angeli, 2017, pagg. 99-120.