Digitalizzazione del mercato del lavoro

Modulo di formazione sviluppato nell'ambito del progetto

Avvio di attività per l'attuazione dell'Accordo quadro delle parti sociali europee sulla digitalizzazione

co-finanziato dall'Unione europea

Cofinanziato dall'Unione europea

Giugno 2023

Autrici:

Blanka Wawrzyniak

Marta Musidłowska

Supporto scientifico:

Hanna Sakowicz-Daszczyńska

Ettore Innocenti *(per il quadro giuridico italiano)*

Responsabile editoriale:

Julia Zaleska

Pubblicazione gratuita, finanziata dall'Unione europea nell'ambito del progetto n. 101051759 **"Avvio di attività per l'attuazione dell'Accordo quadro delle parti sociali europee sulla digitalizzazione (EFAD)".** Titolo originale: **"**Initiating activities to implement the European Social Partners Framework Agreement on Digitalisation (EFAD)".

Nota introduttiva

Questa pubblicazione è stata realizzata nell'ambito del progetto "Avvio delle attività di attuazione dell'accordo quadro delle parti sociali europee sulla digitalizzazione". Si tratta di un manuale che verrà utilizzato sia durante che dopo la formazione di progetto. Il modulo di formazione mira a preparare le parti sociali ai dinamici cambiamenti che avvengono nel mercato del lavoro a causa della trasformazione digitale. Si tratta di cambiamenti che riguardano, tra le altre cose, l'automazione della produzione, i nuovi modelli di business, lo smart working e i metodi di gestione innovativi nelle aziende. La pubblicazione comprende anche una discussione sui diritti dei dipendenti nell'era digitale. L'obiettivo è fornire ai dipendenti gli strumenti per staccare la spina e mantenere l'equilibrio tra vita professionale e vita privata.

Indice

Introduzione

Sebbene l'intelligenza artificiale (AI) sia un termine ampio che comprende un gruppo di algoritmi in grado di modificare i propri parametri e creare nuovi risultati, nei suoi termini più semplici può essere descritta come la capacità delle macchine di comprendere, apprendere, pianificare e dimostrare creatività.

Per molti esperti, il ritmo di sviluppo dell'intelligenza artificiale e il suo impatto sul mondo che ci circonda sembrano preoccupanti. Ciò è influenzato, tra le altre cose, dal fatto che i sistemi di IA vengono sviluppati dalle più grandi aziende tecnologiche statunitensi e cinesi, che in cima alle loro priorità mettono i propri profitti commerciali. La stessa industria tecnologica ha messo in guardia dai pericoli di uno sviluppo illimitato dell'IA. Una lettera aperta che chiede di fermare gli esperimenti sui sistemi di intelligenza artificiale e sui sistemi più potenti della Chat GPT-4 è stata firmata, tra gli altri, da Elon Musk (CEO di SpaceX, Tesla e Twitter), Steve Wozniak (co-fondatore di Apple) e Yuval Noah Harari (futurista, professore all'Università Ebraica di Gerusalemme).

Controllare lo sviluppo dell'IA è essenziale per garantire che i sistemi di IA siano sicuri e che tengano conto dell'impatto sul benessere umano. Tuttavia, nell'ampio flusso di informazioni sull'IA, emergono le visioni più allarmistiche, non necessariamente fondate sulla realtà. Questo, a sua volta, porta a opinioni scettiche sulle nuove tecnologie, alla paura di una disoccupazione di massa e alla riluttanza a utilizzare gli strumenti digitali. Tuttavia è importante ricordare che le tecnologie digitali sono ormai parte integrante della vita quotidiana. Non sono solo fonte di intrattenimento, ma anche strumenti che facilitano lo svolgimento dei compiti domestici e professionali. Pertanto, la familiarizzazione con soluzioni innovative e l'educazione del pubblico a un uso corretto delle tecnologie digitali sono estremamente importanti.

Le attività di sensibilizzazione dovrebbero riguardare anche (o soprattutto) gli strumenti digitali utilizzati sul posto di lavoro. Come verrà sottolineato più avanti nel manuale, le nuove tecnologie sono utilizzate in molti settori e in diverse fasi dell'impiego (dall'assunzione alla valutazione dei dipendenti). Esse facilitano sia i processi di gestione aziendale che il lavoro quotidiano di molte persone (sia operai che impiegati). L'esempio migliore è la diffusione di traduttori automatici come Google Translator o Deepl, che migliorano la comunicazione transfrontaliera tra aziende o consentono di tradurre testi professionali senza dover ricorrere a un traduttore professionista.

Crescono anche le speranze di semplificare il lavoro con l'intelligenza artificiale generativa. Applicazioni come chat-GPT o DALL-E vengono già utilizzate per compiti creativi, come la scrittura di e-mail o l'analisi di dati. Ad esempio, con l'aiuto dell'intelligenza artificiale

generativa è possibile analizzare più rapidamente il contenuto di un articolo o redigere il verbale di una riunione in un attimo. Dopo aver impartito un comando appropriato (ad esempio, "esponi le principali conclusioni della discussione") e aver inserito i parametri di base nel sistema, si può prevedere che vengano generati i risultati attesi (conclusioni).

Allo stesso tempo, è importante tenere presente che i modelli *linguistici di grandi dimensioni* (LLM) come Chat GPT, pur producendo contenuti che sembrano naturali, li generano in modo automatico e non riflessivo. Questo, a sua volta, può portare a testi prodotti dagli algoritmi che, sebbene molto affidabili, contengono molti errori. È per questo che è così importante sviluppare negli utenti capacità di pensiero critico, la capacità di analizzare l'ambiente reale e di discernere ciò che non è vero (ad esempio, le *fake news*). Inoltre, nel lavoro nell'era digitale, oltre a preparare i dipendenti dei vari settori all'automazionee a dotarli di nuove competenze, è necessario insegnare ai dipendenti la convivenza con la tecnologia e la capacità di "staccare la spina". Questi sono i prerequisiti per un giusto equilibrio tra lavoro e vita privata.

Il presente elaborato è stato creato nel 2022/2023. Dato lo sviluppo dinamico dell'innovazione e, in particolare, degli strumenti di intelligenza artificiale (AI), le autricii del manuale desiderano sottolineare che alcuni contenuti potrebbero diventare obsoleti nei prossimi mesi e anni a causa dei progressi tecnologici.

Glossario

AI ACT / Legge sull'intelligenza artificiale

Regolamento dell'UE che stabilisce norme armonizzate sull'intelligenza artificiale.

Algoritmo

Un insieme di istruzioni (formule computazionali) che prendono autonomamente decisioni basate su modelli statistici o regole decisionali senza l'intervento esplicito dell'uomo.

Anonimizzazione

Il processo di trasformazione dei dati personali in modo tale che non possano essere attribuiti a una persona fisica identificata o identificabile.

Autoapprendimento (ML; machine learning)

Un'area dell'intelligenza artificiale dedicata agli algoritmi che migliorano continuamente le loro prestazioni attraverso l'esperienza o l'esposizione ai dati. Gli algoritmi di apprendimento automatico costruiscono un modello matematico a partire da dati campione (chiamati set di apprendimento) per fare previsioni o prendere decisioni senza la necessità di programmare un essere umano.

Automazione

L'uso della tecnologia per controllare la produzione e creare prodotti e servizi utilizzando strumenti digitali.

Blockchain

La cosiddetta "catena di blocchi", una tecnologia per il trasferimento e l'archiviazione di informazioni sulle transazioni online; un registro di dati decentralizzato che viene condiviso in modo sicuro. La tecnologia blockchain consente a un gruppo di partecipanti selezionati di condividere dati.

Bring you own device (BYOD) / Porta il tuo dispositivo

La tendenza a utilizzare dispositivi privati come laptop, smartphone e tablet per svolgere le proprie mansioni professionali.

Chat GPT

Uno strumento che utilizza l'intelligenza artificiale (chatbot) e che, in un formato simile al dialogo, consente di rispondere a domande poste in un linguaggio naturale dall'utente.

Competenze del futuro

Competenze specifiche per intraprendere e svolgere compiti in un ambiente di lavoro fondamentalmente flessibile, geograficamente disperso, soggetto a frequenti e rapidi cambiamenti e che comporta la necessità di utilizzare tecnologie digitali e collaborare con sistemi automatizzati e macchine che utilizzano l'intelligenza artificiale.

Crittografia dei dati

Un insieme di tecniche di codifica di informazioni sensibili o personali per garantirne la riservatezza.

Dati personali

Qualsiasi informazione relativa a una persona fisica vivente identificata o identificabile (costituiscono dati personali anche le singole informazioni che, se considerate nel loro insieme, possono portare all'identificazione di una persona costituiscono anch'esse dati personali).

Deep Fake / Falso *profondo*

Da due espressioni inglesi: *deep learning (apprendimento profondo)* e *fake (bufala, falso)*. Si tratta dell'elaborazione di suoni e immagini per creare un messaggio falso utilizzando tecniche di intelligenza artificiale. In questo modo è possibile produrre materiale che è difficile o impossibile da distinguere da filmati o fotografie creati con mezzi tradizionali e con persone reali.

Diritto alla disconnessione

Il diritto di non impegnarsi in compiti legati al lavoro al di fuori dell'orario di lavoro e di non partecipare alla comunicazione attraverso strumenti digitali.

Equilibrio tra *lavoro e vita privata*

Mantenere un equilibrio tra lavoro (sia retribuito che non), vita familiare e tempo libero.

Economia della condivisione/su richiesta (sharing economy; on-demand economy)

Un insieme di modelli di business basati sull'intermediazione di piattaforme collaborative, che creano un mercato ad accesso aperto per l'utilizzo temporaneo di beni o servizi spesso forniti da privati.

Fake news / *Notizie false*

Informazioni false o parzialmente false di natura sensazionale che inducono deliberatamente in errore il destinatario.

GDPR

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito: il Regolamento GDPR).

Intelligenza artificiale (AI)

La capacità delle macchine di comprendere, apprendere, pianificare e dimostrare creatività. Secondo la definizione proposta dalla bozza di legge sull'intelligenza artificiale, per sistema di intelligenza artificiale si intende un software sviluppato utilizzando una o più delle tecniche e degli approcci descritti nel regolamento, in grado di generare, per un determinato insieme di scopi definiti dall'uomo, output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagisce. Questa definizione è molto ampia e vaga, ma è comprensibile nel contesto di una tecnologia in rapido sviluppo come l'intelligenza artificiale.

Lavoro assistito

Lavoro in cui alcune attività possono essere sostituite da robot, mentre altre richiedono l'intervento umano.

Lavoro tramite piattaforma

Una forma di impiego in cui un dipendente utilizza una piattaforma digitale per accedere ad altre organizzazioni o individui per fornire servizi specifici e in cambio di un compenso. Tra i compiti svolti a pagamento attraverso le piattaforme digitali vi sono i servizi di taxi e di corriere, le consegne, i servizi di riparazione a domicilio, nonché i lavori impiegatizi come il copywriting e la contabilità.

Mobbing

Azioni o comportamenti diretti a un lavoratore che consistono in molestie o intimidazioni persistenti e prolungate.

Modelli linguistici di grandi dimensioni (LLM, Large Language Models)

Modelli di apprendimento automatico in grado di eseguire una serie di compiti di elaborazione del linguaggio naturale. L'addestramento di un sistema di questo tipo consiste nel fornirgli grandi quantità di dati (ad esempio libri, articoli, siti web) in modo che possa apprendere modelli e connessioni tra le parole per generare nuovi contenuti in futuro. Un esempio di LLM è Chat GPT, sviluppato da OpenAI e disponibile al pubblico dal novembre 2022. Questo modello è in grado di elaborare informazioni e generare testi simili a quelli umani in risposta alle richieste dell'utente.

Processo decisionale automatizzato

Un'attività basata su calcoli avanzati e su mezzi esclusivamente tecnici di elaborazione delle informazioni. L'emissione di decisioni da parte di un computer senza il coinvolgimento dell'elemento umano.

Profilazione

Qualsiasi forma di trattamento automatizzato dei dati personali che comporti l'utilizzo degli stessi per valutare determinati fattori personali di un individuo. In particolare, la profilazione viene utilizzata per analizzare o prevedere le prestazioni di tale persona, la sua situazione

economica, la sua salute, le sue preferenze personali, i suoi interessi, la sua affidabilità, il suo comportamento, la sua ubicazione o i suoi spostamenti.

Pseudonimizzazione

Trattare i dati personali in modo tale che non sia possibile identificare a chi appartengono senza accedere ad altre informazioni conservate in modo sicuro altrove.

Robot collaborativi (co-bot)

Attrezzatura progettata per ridurre il carico di lavoro dei lavoratori in fabbrica, svolgendo parte delle loro mansioni.

Spoofing

Un tipo di attacco in cui i criminali si fingono banche, istituzioni e uffici governativi, aziende o addirittura individui per estorcere dati o denaro alle loro vittime.

Start-up

Un'azienda di nuova costituzione o un'organizzazione temporanea alla ricerca di un modello di business per crescere in modo redditizio.

Wearables / Dispositivi indossabili

Dispositivi elettronici "indossabili", cioè indossati vicino alla pelle. Possono monitorare e analizzare i parametri di salute o il comportamento di chi li indossa. I dispositivi più diffusi di questo tipo sono attualmente gli smartwatch, le fasce sportive (le cosiddette smartband) e gli orologi sportivi.

1. Impatto della digitalizzazione sui processi lavorativi

1.1 Accordo quadro delle parti sociali europee sulla digitalizzazione - osservazioni generali

La trasformazione digitale dell'economia ha un enorme impatto sui datori di lavoro, sui lavoratori e sul corso stesso del lavoro. Per facilitare l'integrazione delle tecnologie digitali nei luoghi di lavoro, nel giugno 2020 è stato concluso l'Accordo quadro autonomo delle parti sociali europee (EFAD). Il suo obiettivo è prevenire e ridurre al minimo i rischi che i lavoratori e i datori di lavoro possono correre. L'accordo riguarda tutte le persone impiegate o che impiegano lavoratori nel settore pubblico e privato e in tutti i tipi di attività economica.

L'accordo EFAD è un'iniziativa autonoma ed è il risultato dei negoziati tra le parti sociali europee nell'ambito del Sesto programma di lavoro pluriennale 2019-2021. Alla luce dell'art. 155 del Trattato sul funzionamento dell'Unione europea (TFUE), questo accordo quadro europeo autonomo impegna i membri di BusinessEurope, SMEunited, CEEP e CES (e il comitato di collegamento EUROCADRES/CEC) a promuovere e attuare strumenti e misure (se necessario a livello nazionale, settoriale o aziendale) secondo le procedure e le prassi proprie delle parti sociali negli Stati membri e nei paesi dello Spazio economico europeo.

Esempi di altri accordi autonomi conclusi negli ultimi anni sono l'accordo quadro autonomo delle parti sociali europee sull'invecchiamento attivo e gli approcci intergenerazionali o l'accordo quadro europeo sullo stress legato al lavoro.

I. Principali obiettivi dell'accordo EFAD

1. Aumentare la consapevolezza e la comprensione tra i datori di lavoro, i lavoratori e i loro rappresentanti delle opportunità e delle sfide sul lavoro che derivano dalla trasformazione digitale.
2. Fornire assistenza ai lavoratori e ai loro rappresentanti e ai datori di lavoro nello sviluppo di misure e azioni per sfruttare le nuove opportunità digitali e quindi affrontare le sfide, tenendo conto delle iniziative, delle pratiche e dei contratti collettivi esistenti.
3. Incoraggiare un approccio di partenariato tra datori di lavoro e sindacati.

II. Fasi di creazione di partnership per facilitare il processo di trasformazione digitale in azienda

Ai rappresentanti dei lavoratori saranno fornite le strutture e le informazioni necessarie per un coinvolgimento efficace nelle varie fasi del processo.

Fase 1.

"Esplorazione/preparazione/sostegno congiunto", che si occupano di sensibilizzazione e di creare le condizioni e l'atmosfera di sostegno e fiducia. Queste attività mirano a consentire una discussione aperta sulle opportunità e sulle sfide/minacce della digitalizzazione e sul loro impatto sul luogo di lavoro, nonché a discutere di possibili azioni e soluzioni.

Fase 2.

La "mappatura/valutazione/analisi regolare congiunta" è un esercizio di mappatura delle aree tematiche in termini di benefici e opportunità, nonché di sfide e rischi che l'integrazione efficace delle tecnologie digitali può portare ai dipendenti e all'azienda.

Fase 3.

"Revisione congiunta della situazione e adozione di una strategia di trasformazione digitale", che è il risultato delle prime due fasi. Si tratta di una comprensione di base delle opportunità
e delle sfide/rischi, dei diversi elementi che compongono la digitalizzazione dell'azienda e delle loro interrelazioni, e del concordare strategie digitali che fissino gli obiettivi dell'azienda per il futuro.

Fase 4.

"Adozione di misure/azioni appropriate" sulla base di un esame congiunto della situazione. Essa comprende: la possibilità di testare e pilotare le soluzioni previste, la definizione delle priorità, l'attuazione delle azioni in fasi temporali successive, il chiarimento e la definizione dei ruoli e delle responsabilità della direzione e del personale e dei loro rappresentanti, nonché le risorse e le misure di accompagnamento (ad esempio, supporto di esperti, monitoraggio).

Fase 5.

Il "regolare monitoraggio/follow-up, apprendimento, valutazione congiunti" è una valutazione congiunta dell'efficacia delle azioni e una discussione sulla necessità di ulteriori analisi, sensibilizzazione, supporto o altre azioni.

III. L'ambito di applicazione dell'accordo comprende:

1. Competenze digitali e occupazione

Le parti sociali dovrebbero essere interessate a facilitare l'accesso a una formazione di qualità e allo sviluppo delle competenze dei dipendenti. Una sfida fondamentale sarà quella di identificare le competenze digitali e i cambiamenti processuali da implementare in una determinata azienda.

Le misure da considerare includono:

- Impegno delle parti alla riqualificazione.
- Accesso e organizzazione della formazione, alta qualità ed efficacia della formazione, introduzione di opportunità part-time e assegnazione di tempo di lavoro specifico per la formazione.
- Condizioni di partecipazione chiaramente definite, tra cui: durata, aspetti finanziari, coinvolgimento dei dipendenti e compensazione se la formazione si svolge al di fuori dell'orario di lavoro.

2. Modalità di connessione e disconnessione

È dovere del datore di lavoro garantire la sicurezza e la salute dei lavoratori sotto ogni aspetto legato al lavoro. Pertanto, il diritto alla disconnessione è uno degli aspetti principali di questo manuale. Chiediamo ai sindacalisti di fare ragionevole chiarezza sulle aspettative del datore di lavoro nei confronti del lavoratore quanto all'uso dei dispositivi digitali anche con il sostegno della contrattazione collettiva ai livelli appropriati

Introdurre nuovi dispositivi digitali può assicurare flessibilità nell'organizzazione del lavoro con benefici sia per i lavoratori che i datori di lavoro. Al contempo questa può comportare un grave rischio legato ad una difficile separazione tra lavoro e vita privata. Per questo è opportuno concentrarsi sull'evitare fenomeni negativi che impattino la salute e la sicurezza dei lavoratori. Per far ciò è necessario definire bene i diritti, gli obblighi e le mansioni, nei quali il principio di precauzione è la più alta priorità.

Le misure da prendere in considerazione sono:

- Formazioni e altre attività di sensibilizzazione dei lavoratori.
- Creare una nuova cultura del lavoro tra i dirigenti che eviti il contatto con il dipendente al di fuori dell'orario di lavoro.

- Fornire una guida chiara sulla legislazione esistente in materia di orario di lavoro, telelavoro e lavoro mobile.
- Organizzazione efficiente del lavoro, compresa la garanzia che il numero di dipendenti non costringa a lavorare oltre l'orario di lavoro.
- Compenso adeguato per il tempo di lavoro supplementare.
- Procedure di allerta e sostegno che permettano di scollegarsi e che tutelino da sanzioni per la mancanza di contatto con il lavoratore dopo l'orario di lavoro.
- Prevenire l'isolamento sul lavoro.

3. Intelligenza artificiale e garanzia del principio del controllo umano

Non c'è dubbio che l'IA avrà un impatto crescente sul lavoro umano. Pertanto l'Accordo europeo autonomo stabilisce alcuni principi e indicazioni per la sua introduzione nel mercato del lavoro. Un elemento importante che dovrebbe essere garantito in ogni luogo di lavoro è il controllo umano sull'IA, che è la base per l'uso della robotica e delle applicazioni basate sull'IA. Il sistema dovrebbe essere legale ed equo e rispettare standard etici compatibili con i diritti umani. Da un punto di vista tecnico e sociale, invece, dovrebbe essere sicuro e trasparente.

4. Rispetto della dignità umana e della sorveglianza

A causa della significativa ingerenza delle moderne tecnologie nel processo lavorativo, sussiste il rischio di violare i valori fondamentali dell'essere umano che lavora (ad esempio, raccogliendo dati sensibili - si pensi all'accesso a locali o documenti attraverso un'impronta digitale o una scansione della pupilla o un chip impiantato). Tali tecnologie aumentano il rischio di violazione della dignità umana, soprattutto nel caso del monitoraggio personale. Ciò può portare a un deterioramento delle condizioni di lavoro.

La minimizzazione e la trasparenza dei dati personali, insieme a regole chiare per il loro trattamento, riducono il rischio di un monitoraggio invasivo e di un uso improprio dei dati. Nel contesto lavorativo, le regole sul trattamento dei dati personali dei dipendenti sono stabilite dal regolamento GDPR. Inoltre, le parti sociali dell'accordo EFAD ricordano che l'articolo 88 del GDPR fa riferimento alla possibilità di stabilire, attraverso contratti collettivi, regole più dettagliate per la conservazione dei dati personali dei dipendenti. Ciò al fine di garantire la tutela dei diritti e delle libertà dei lavoratori in relazione al trattamento dei loro dati personali nell'ambito del rapporto di lavoro.

Le misure da considerare includono:

- Consentire ai rappresentanti dei dipendenti di risolvere le questioni relative a dati, consenso, privacy e sorveglianza.
- Raccogliere dati per uno scopo specifico e trasparente. I dati non devono essere raccolti o conservati semplicemente perché è possibile o per uno scopo non definito.
- Informare i dipendenti che possono non acconsentire al trattamento di un particolare gruppo di dati personali o che possono revocare in qualsiasi momento il consenso precedentemente dato.
- Fornire ai rappresentanti del personale strutture e strumenti (digitali), ad esempio bacheche digitali, per svolgere i loro compiti.

5. Attuazione e follow-up

Le organizzazioni aderenti riferiranno al comitato di dialogo sociale in merito all'attuazione dell'accordo. Entro i primi tre anni dalla firma dell'accordo, il comitato di dialogo sociale è tenuto a preparare e adottare un pacchetto annuale che riassuma lo stato di attuazione in corso dell'accordo. Una relazione completa sulle attività di attuazione intraprese sarà preparata dal comitato e adottata dalle parti sociali europee negli anni successivi. L'accordo non pregiudica il diritto delle parti sociali di concludere accordi di adattamento e/o complementari in modo da tenere conto delle esigenze specifiche delle parti sociali interessate.

1.2 Le nuove tecnologie sul posto di lavoro - lavoro assistito dalle macchine e completamente automatizzato

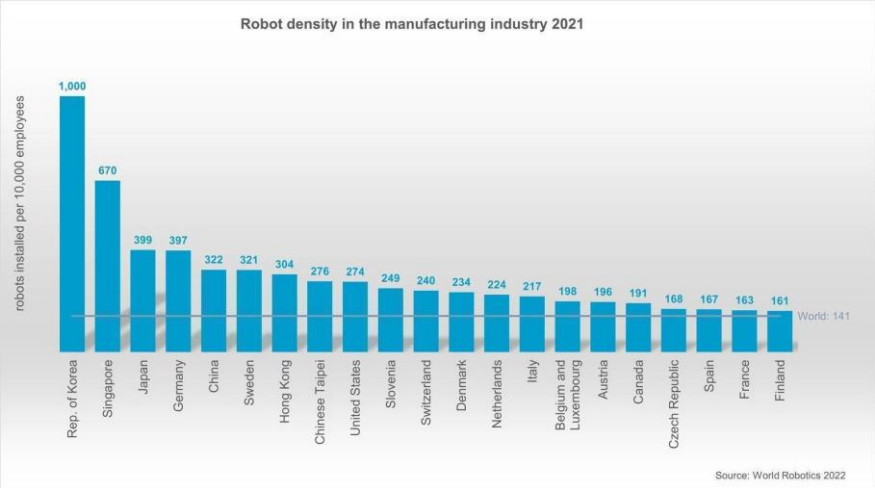
L'atteggiamento nei confronti della robotizzazione sta cambiando sia dal punto di vista delle imprese che dei lavoratori stessi. Il robot non rimane più solo un'immaginazione, ma appare come uno strumento di produzione che può alleggerire il peso dell'uomo e aiutarlo a risolvere problemi specifici. A seconda del settore e della fase di produzione, tuttavia, l'automazione può essere introdotta in diversa misura. Oltre a seconda del livello di coinvolgimento nelle varie mansioni, i robot possono essere suddivisi in quelli che svolgono un lavoro prevalentemente intellettuale (ad esempio tutti gli strumenti di intelligenza artificiale) e quelli che sollevano l'uomo da compiti ripetitivi (ad esempio nell'imballaggio dei prodotti).

Che cos'è un sistema di produzione automatizzato?

Per automazione della produzione si intende quella direzione di sviluppo delle aziende che comporti una significativa riduzione o la completa sostituzione del lavoro umano fisico e mentale con il lavoro delle macchine. Le origini di questo fenomeno possono essere fatte risalire al XX secolo, quando, nel 1913, Henry Ford cambiò per sempre il mondo con una catena di montaggio mobile gestita da operai specializzati. La premessa di questo lavoro era quella di aumentare la scala della produzione, abbassando al contempo il prezzo del prodotto finale.

Siamo ora di fronte alla prossima fase dell'evoluzione della produzione: la semplificazione dell'automazione attraverso la digitalizzazione. Grazie a tecnologie come i moduli di programmazione intuitivi, la creazione di istruzioni dettagliate per i robot sta diventando più semplice. I sensori avanzati consentono alle macchine di comprendere l'ambiente circostante e di essere più reattive. Secondo la Federazione Internazionale di Robotica, dal 2015 al 2020 la densità di robot[1] è quasi raddoppiata a livello mondiale, passando da 66 unità nel 2015 a 126 unità nel 2020.

Paesi con la produzione più automatizzata (2021)



Fonte: Federazione Internazionale di Robotica (*The Robot Report*, 2021).

[1] Una metrica utilizzata dalla Federazione Internazionale di Robotica che misura il numero di robot per 10.000 lavoratori in un settore.

Lavoro supportato

Per lavoro assistito si intendono quei casi in cui alcune attività della produzione possono essere sostituite da robot, mentre altre richiedono l'intervento umano. I *robot collaborativi* (i cosiddetti "co-bot") sono più spesso utilizzati per supportare i processi produttivi, con il compito di sgravare gli operai di una parte del carico di lavoro. Una caratteristica importante che distingue i cosiddetti co-bot dai sistemi industriali standard (che di solito sono separati dall'uomo) è che, nel caso della robotica collaborativa, i sistemi robotici controllati condividono lo stesso spazio di lavoro con gli esseri umani.

Modi in cui i robot interagiscono con gli esseri umani:

1. **Interazione umana limitata -** il robot si ferma completamente quando un uomo appare nell'area designata e riprende a funzionare in modo indipendente dopo che il lavoratore ha lasciato l'area.
2. **Collaborazione umana -** grazie ai sensori integrati, il co-bot rallenta le operazioni o interrompe il lavoro quando qualcuno si trova nelle sue vicinanze, consentendo un'interazione sicura tra uomo e macchina.
3. **Guida manuale** - il co-bot è sempre controllato dall'operatore. Ad esempio, il dispositivo trattiene il carico mentre un uomo ne guida il braccio.

Lavoro completamente automatizzato

L'automazione nell'industria è intesa come l'uso della tecnologia per controllare la produzione e creare prodotti e servizi utilizzando strumenti digitali. Nel caso dell'automazione completa, le persone e le macchine cessano di svolgere compiti complementari e iniziano a operare negli stessi ambiti. A causa della robotizzazione la partecipazione dei lavoratori ai processi produttivi diminuisce significativamente o scompare del tutto. Tutti i processi produttivi diventano completamente automatizzati e l'intervento umano si fa superfluo in ogni fase della creazione del prodotto.

Nonostante il diffuso timore causato dalla crescente automazione dei processi industriali, l'introduzione di questo tipo di tecnologia può portare benefici a vari livelli legati ai processi produttivi - anche quando il lavoro è rischioso per la vita e la salute umana.

Discussione - Il lavoro dei robot dovrebbe essere tassato?

Con la diminuzione dei costi di automazione dei processi produttivi, la scala della robotizzazione industriale sta aumentando. Le conseguenze previste comprendono sia aspetti positivi, come la crescita economica o l'aumento della produttività, sia aspetti negativi, come la riduzione dell'occupazione in vari comparti del settore manifatturiero.

La trasformazione dei modelli di business tradizionali sta suscitando molte polemiche e ci sono nuove sfide per i legislatori in quei paesi in cui l'automazione si è già sviluppata a un ritmo sorprendente.

Con la significativa riduzione del costo del lavoro e dei profitti causata dall'uso dei robot nell'industria, la **questione delle tasse imposte sul lavoro robotizzato** è diventata una delle questioni difficili da risolvere. Tuttavia, quando si tratta di acquistare nuovi macchinari e attrezzature, i singoli governi stanno utilizzando incentivi fiscali per incoraggiare la trasformazione digitale e la modernizzazione del settore industriale.

In Polonia, ad esempio, a partire dal 2022, gli imprenditori potranno detrarre fino al 150% del costo di acquisto di macchinari e attrezzature funzionalmente correlati per la sicurezza sul lavoro nelle postazioni in cui si verifica l'interazione uomo-robot.

Conseguenze positive e negative della robotizzazione

1. **Economia**

   a) **Positive:**

      i) Capacità di migliorare i prodotti e di immetterli sul mercato più rapidamente.

      ii) Sviluppo più rapido di nuove tecnologie.

      iii) Miglioramento della competitività delle aziende.

   b) **Negative:**

      i) Aumento della disoccupazione - secondo le stime degli autori del rapporto 2023 *Future of Jobs* (World Economic Forum), nel prossimo futuro le macchine svolgeranno una percentuale maggiore di compiti rispetto agli esseri umani. Se nel 2018, in media, il 71% del tempo di lavoro consisteva in compiti che coinvolgevano il fattore umano, questa proporzione è destinata a cambiare significativamente nel 2025. Gli esseri umani saranno responsabili di circa il 48% delle attività, mentre il restante 52% sarà completamente automatizzato.

ii) Aumento del consumo di energia e contributo all'aumento dell'inquinamento ambientale.

2. Datore di lavoro

a) Positive:

i) Riduzione dei costi di produzione.

ii) Riduzione del rischio di errori.

iii) Capacità di registrare meglio le prestazioni.

iv) Individuazione più rapida dei colli di bottiglia, che facilita l'ottimizzazione del lavoro.

v) In alcuni paesi (ad esempio la Polonia) - è possibile detrarre i costi di acquisto di robot industriali con uno scopo specifico.

b) Negative:

i) Elevati costi iniziali di installazione delle apparecchiature.

ii) Necessità di inventario ed elevato costo di riparazione.

iii) Se i processi sono altamente automatizzati, i guasti alle apparecchiature causano interruzioni della produzione.

iv) Ridotta flessibilità di risposta a problemi o errori imprevisti rispetto alla risposta dei dipendenti.

v) Necessità di rispettare le normative più esigenti.

vi) Alti costi di consumo energetico.

3. Dipendente

a) Positive:

i) Semplificazione del processo produttivo.

ii) Supporto nelle attività più difficili o ripetitive.

iii) Maggiore efficienza produttiva con un minore coinvolgimento dei dipendenti.

iv) Possibilità di dedicare tempo ad altre attività di sviluppo grazie alla cessione di quelle ripetitive a strumenti automatizzati.

v) L'emergere di nuovi posti di lavoro legati alla creazione, al funzionamento o alla riparazione di macchinari.

b) Negative:

i) Potenziale perdita di posti di lavoro dovuta all'automazione del processo

ii) Maggiore probabilità di burnout lavorativo innescato dalla paura di perdere il lavoro

iii) Se i macchinari si rompono o non sono utilizzati correttamente - esposizione al deterioramento delle condizioni di salute/di pericolo di vita.

1.3 Come evitare un controllo sul luogo di lavoro sproporzionato ed eccessivo

La supervisione sul posto di lavoro - opportunità e rischi

Le aziende del settore tecnologico sono desiderose di rispondere alla crescente domanda da parte dei datori di lavoro in termini di nuove tecnologie. Al contrario, il trend riscontrabile negli strumenti di IA sta creando opportunità per mettere i dipendenti sotto pieno controllo, indipendentemente dalla loro conoscenza o dal loro consenso. Esiste anche una forte tendenza ad accettare il nuovo stato di cose come una conseguenza "naturale" dello sviluppo delle aziende.

Opportunità:

- Il monitoraggio utilizzato in situazioni di pericolo e in caso di incidente sul lavoro può andare a vantaggio del dipendente (ad esempio, quando è necessario dimostrare che il luogo di lavoro non era sufficientemente sicuro)
- in alcuni settori il monitoraggio è necessario per garantire la conformità (ad esempio, nel settore bancario può essere utilizzato per prevenire l'*insider trading*)
- la sorveglianza utilizzata durante la formazione dei dipendenti può accelerare i processi di inserimento (ad esempio, nel settore edile, i *wearable* sono caschi intelligenti con sensori di vibrazione che avvertono i lavoratori della presenza di oggetti potenzialmente pericolosi nell'ambiente).

Esempio di Stellate

Stellate, una start-up di analisi dei dati con sede a San Francisco, ha un team di dipendenti sparsi in tutto il mondo. Oltre agli strumenti utilizzati per collaborare in remoto, l'azienda controlla lo sviluppo dei propri dipendenti attraverso programmi di formazione e mentoring. Piuttosto che sanzioni per prestazioni inadeguate o altri comportamenti scorretti, l'obiettivo principale di queste iniziative è promuovere tra i dipendenti dell'azienda strumenti per migliorare l'efficienza del loro lavoro.

Minacce:

- l'uso eccessivo o scorretto delle tecnologie digitali può portare a violazioni della privacy e dei diritti di tutela dei dati dei dipendenti,
- rischi per la salute mentale e fisica dei lavoratori a causa dello stress dovuto all'eccessiva supervisione e agli standard di lavoro imposti,
- forme associative di dipendenti ostacolate- il monitoraggio dei dipendenti e l'identificazione del sentimento aziendale consentono di cogliere i movimenti a favore dell'associazione (ad esempio, nei grandi luoghi di lavoro, accade che i dati dei dipendenti vengano utilizzati per identificare gli atteggiamenti dei dipendenti nei confronti del datore di lavoro e determinare dove è più probabile che i dipendenti si oppongano alle politiche aziendali).

Principi fondamentali del monitoraggio del luogo di lavoro

È riconosciuto che i datori di lavoro devono essere in grado di sorvegliare i luoghi di lavoro e di valutare le prestazioni dei propri dipendenti per garantire una migliore gestione dell'azienda e per proteggere i segreti aziendali, imporre il rispetto della legge e prevenire la criminalità dei dipendenti. Allo stesso tempo, l'Unione europea e i singoli Stati membri attribuiscono grande importanza alla privacy dei dipendenti e al rispetto della loro vita privata.

Il monitoraggio del luogo di lavoro è legale, ma...[2]

- le finalità del trattamento delle informazioni (ad esempio, per garantire la sicurezza dei dipendenti) devono essere esplicitate in dettaglio prima di utilizzare la videosorveglianza,
- il datore di lavoro deve informare le persone potenzialmente soggette a monitoraggio che il monitoraggio è in atto e quale area è coperta.

Inoltre è importante che gli obiettivi, la portata e il metodo di applicazione del monitoraggio siano stabiliti in un contratto collettivo o in un regolamento di lavoro, ad

[2] Norme sul monitoraggio dei luoghi di lavoro previste dal diritto comunitario (articolo 8 della Convenzione europea dei diritti dell'uomo, regolamento GDPR), decisioni di tribunali e corti, codici del lavoro dei singoli Stati membri.

esempio nell'ambito della contrattazione collettiva. Nelle situazioni in cui il datore di lavoro non è coperto da un contratto collettivo o non è obbligato a stabilire un regolamento di lavoro, le regole vanno sancite in un avviso.

La videosorveglianza occulta è consentita solo in misura limitata quando vi è il ragionevole sospetto che sia stato commesso un grave illecito o un reato penale che abbia causato un danno significativo al datore di lavoro.

Inoltre, il datore di lavoro può utilizzare altri tipi di monitoraggio. Ad esempio:

- GPS montato su un'auto aziendale,
- monitoraggio di Internet e della messaggistica istantanea utilizzata sulle apparecchiature aziendali,
- geolocalizzazione di un telefono cellulare o di un computer portatile aziendale.

Le disposizioni sulla videosorveglianza si applicano *mutatis mutandis* a tutte le forme di monitoraggio (ad esempio, un datore di lavoro può monitorare la posta elettronica di un dipendente solo dopo averne dato notifica preventiva al dipendente stesso).

Monitoraggio sul lavoro e legge - esempi dai paesi partner

Polonia

Secondo il Codice del lavoro polacco, il monitoraggio è una forma specificia di sorveglianza dei locali di un luogo di lavoro o dell'area circostante un luogo di lavoro, sotto forma di mezzi tecnici che consentono la registrazione di immagini.

Il monitoraggio in Polonia è consentito se è necessario per:

- garantire la sicurezza dei lavoratori,
- proteggere la proprietà o esercitare controllo sulla produzione,
- mantenere riservate le informazioni la cui divulgazione potrebbe esporre il datore di lavoro a danni
- il monitoraggio della posta elettronica (articolo 223 del Codice del lavoro) è consentito nella misura in cui questo si rende necessario per garantire un'organizzazione del lavoro che consenta il pieno utilizzo dell'orario di lavoro e il corretto uso degli strumenti di lavoro forniti al dipendente; il monitoraggio della posta elettronica non deve violare la segretezza della corrispondenza e altri diritti personali del dipendente.

Le registrazioni video possono essere utilizzate dal datore di lavoro solo allo scopo per cui sono state raccolte e conservate, per un periodo non superiore a tre mesi dalla data di registrazione.

Italia

La base giuridica in materia di controlli a distanza è l'articolo 4 della legge n. 300 del 1970 (c.d. Statuto dei lavoratori).

Tale norma riconosce al datore di lavoro il potere di installare impianti audiovisivi ed altri strumenti dai quali derivi anche la possibilità di controllare a distanza l'attività dei lavoratori esclusivamente per esigenze organizzative e produttive, la sicurezza sul lavoro e la tutela del patrimonio aziendale.

Inoltre, ad eccezione degli strumenti di lavoro nonché di quelli di registrazione degli accessi e delle presenze, l'installazione di strumenti di controllo a distanza è subordinata alla stipulazione preventiva di un accordo sindacale di livello aziendale oppure, in mancanza, all'autorizzazione dell'Ispettorato del Lavoro territorialmente competente.

Le informazioni raccolte tramite strumenti di controllo a distanza sono utilizzabili a tutti i fini connessi al rapporto di lavoro, previo adempimento da parte del datore dell'obbligo di informare adeguatamente i lavoratori circa le modalità d'uso degli strumenti e di effettuazione dei controlli nonché nel rispetto della normativa sulla privacy.

Come condurre il monitoraggio in modo lecito? Procedura in sei fasi

Per condurre un monitoraggio legittimo, il datore di lavoro deve valutare l'impatto che le sue azioni possono avere sui dipendenti. Le fasi seguenti indicano su quali domande dovrebbe basarsi tale analisi.

Passi	Domanda	Azione
Fase 1	Se il monitoraggio è già stato introdotto, in cosa consiste in questo preciso momento?	Condurre un audit per determinare quali tipi di monitoraggio sono utilizzati sul posto di lavoro e chi, all'interno dell'organizzazione, ha l'autorità di monitorare i dipendenti.
Fase 2	Perché si fa o si dovrebbe fare monitoraggio?	• Comprendere lo scopo del monitoraggio dei dipendenti.

		• Definire precisamente la funzione del monitoraggio (i dati raccolti da un monitoraggio specifico possono essere utilizzati solo allo scopo per cui sono stati raccolti). **Eccezione**: se, nel corso del monitoraggio, un'organizzazione viene in possesso di informazioni su attività che non possono essere ignorate (ad esempio, potenziali attività criminali, bullismo), i dati raccolti possono essere utilizzati stabilire le responsabilità.
Fase 3	È possibile raggiungere questo obiettivo senza monitoraggio?	Una volta individuato il motivo dell'introduzione del monitoraggio, è importante stabilire se lo stesso obiettivo può essere raggiunto senza il monitoraggio dei dipendenti. **Esempio:** l'introduzione del monitoraggio dei siti visitati dai dipendenti può essere sostituita dal blocco dei siti inappropriati o dalla possibilità per i dipendenti di caricare file solo da account specifici ed entro una certa dimensione.
Fase 4	Se un determinato obiettivo non può essere raggiunto senza monitoraggio, esiste un mezzo di controllo meno invasivo di quello attualmente in esame?	**Ad esempio,** il controllo che i dipendenti non violino la politica di riservatezza dell'azienda può essere effettuato sia controllando il contenuto delle e-mail inviate dai dipendenti, sia attraverso un monitoraggio automatico, come il controllo degli indirizzi e degli oggetti delle e-mail o il blocco delle e-mail con allegati di una certa dimensione.
Fase 5	Che effetto avrà il monitoraggio sui dipendenti?	È necessario rispondere alle seguenti domande: • Il monitoraggio può essere considerato svalutante o ingiusto? • Il monitoraggio influirà sulla fiducia reciproca tra datore di lavoro e dipendenti? • Le informazioni riservate o sensibili possono essere condivise con persone che non hanno necessità di conoscerle? **Esempio:** al team contabile può essere comunicato che una persona è stata assente dal lavoro per malattia (per consentire il pagamento dell'indennità di malattia), ma solo il responsabile

		delle risorse umane deve conoscere i motivi medici dell'assenza.
Fase 6	L'introduzione del monitoraggio è giustificata?	Decidere se l'introduzione del monitoraggio è giustificata (un monitoraggio meno intrusivo è più facile da giustificare, di cui i dipendenti sono informati). Il personale può essere consultato prima dell'introduzione del monitoraggio, sviluppare congiuntamente una logica per il monitoraggio

Supervisione dei dipendenti e lavoro a distanza

La sorveglianza dei lavoratori dipendenti può avvenire tramite l'installazione di applicazioni di controllo sui computer dei dipendenti, che spesso non vengono comunicate ai dipendenti stessi. Il cosiddetto *bossware*[3] può registrare i tasti premuti, fare screenshot e persino attivare le webcam dei dipendenti che lavorano in remoto.

Vale la pena notare che il timore costante di essere osservati da un datore di lavoro può portare a un deterioramento dello stato mentale dei dipendenti. Secondo le ricerche, ben il 56% degli intervistati si sente stressato e ansioso per il fatto che il proprio datore di lavoro controlli le sue comunicazioni elettroniche, il 41% si chiede costantemente se sia osservato e il 32% è meno propenso a fare pause sul lavoro per questo motivo.

Come controllare efficacemente il lavoro senza compromettere il benessere dei dipendenti?

Suggerimenti per il datore di lavoro:

- informare il dipendente sugli strumenti di sorveglianza utilizzati,
- chiarire le regole sull'uso del monitoraggio e stabilirne i limiti (ad esempio sul tipo di dati trattati),
- invece di un'eccessiva supervisione e di un approfondimento delle attività quotidiane del dipendente, introdurre un sistema di responsabilità per i risultati (ad esempio, revisione e valutazione settimanale dei compiti),

[3] Il nome deriva dalle parole inglesi *boss* e *software* e significa software per il datore di lavoro.

- utilizzare applicazioni per monitorare e gestire i flussi di lavoro (ad esempio Connecteam) e migliorare la comunicazione inter-team a distanza e la pianificazione congiunta.

1.4 Differenza tra lavoro a distanza e telelavoro - effetto sulle relazioni di lavoro

Secondo una ricerca della Commissione europea, nell'anno precedente allo scoppio della pandemia COVID-19, solo il 5,4% degli occupati nell'UE-27 lavorava da casa, una percentuale che non è cambiata dal 2009. A seguito della pandemia, questa percentuale è più che raddoppiata, raggiungendo il 12,3%. In alcuni Stati membri, questa cifra ha superato fino a un quarto degli occupati, indipendentemente dall'industria o dal settore economico.

Nonostante le iniziali difficoltà di adattamento alla nuova realtà (causate soprattutto dalla mancanza di infrastrutture TIC adeguate o di formazione alla digitalizzazione dei processi lavorativi), i dipendenti oggi non riescono a immaginare un ritorno al modo in cui lavoravano prima della pandemia. Apprezzano la maggiore flessibilità sul lavoro, l'opportunità di trascorrere del tempo con le proprie famiglie e l'aumento dell'efficienza lavorativa.

Tuttavia, nonostante la popolarità del lavoro ibrido, sono ancora molti i datori di lavoro e i dipendenti che scelgono di tornare in ufficio, motivando questa decisione con il miglioramento dei rapporti di lavoro e della collaborazione, nonché con la possibilità di creare un ambiente favorevole all'innovazione collettiva e a una migliore produttività, separando nettamente la vita privata da quella professionale.

Lavoro a distanza - concetti di base

La crescente popolarità del lavoro con gli strumenti digitali e la moltitudine di possibilità che essi offrono ha reso necessario l'uso di una serie di nuovi termini. Per facilitare l'orientamento nel labirinto delle definizioni, è stata creata una tabella che mostra le differenze tra le varie modalità di lavoro.

Tipo di lavoro che utilizza strumenti digitali	Definizione

Lavoro a distanza	Per lavoro a distanza si intende qualsiasi attività svolta fuori dalla sede del datore di lavoro, indipendentemente dalla tecnologia utilizzata. Secondo gli emendamenti al Codice del Lavoro polacco si tratta di: lavoro svolto interamente o parzialmente in un luogo indicato dal lavoratore e concordato con il datore di lavoro di volta in volta **In Italia si distingue tra telelavoro e lavoro agile. Il telelavoro è una modalità di svolgimento del rapporto di lavoro caratterizzata dalla regolarità dell'attività esterna ai locali aziendali e dal ricorso alla strumentazione tecnologica. Il lavoro agile si configura come una modalità esecutiva del rapporto di lavoro subordinato, di cui gli elementi essenziali sono l'alternanza tra l'attività interna ed esterna ai locali aziendali, l'assenza di una postazione fissa e la flessibilità oraria (nei limiti della durata massima giornaliera e settimanale). Sia al telelavoro che al lavoro agile si accede mediante un accordo individuale tra datore di lavoro e lavoratore.**
Telelavoro	Il telelavoro è qualsiasi forma di organizzazione e/o esecuzione del lavoro che utilizza le tecnologie dell'informazione, nel contesto di un contratto/rapporto di lavoro in cui il lavoro, che può anche essere svolto nei locali del datore di lavoro, viene regolarmente svolto fuori da tali locali.
Telelavoro a tempo parziale	Questa modalità di lavoro combina giorni di lavoro a distanza con giorni in ufficio ed è stata messa in pratica per la prima volta da Jack Nilles all'inizio degli anni '70 negli Stati Uniti.
Telelavoro e lavoro mobile basati sulle TIC (TICTM)	Il termine TICTM si riferisce all'uso di tecnologie dell'informazione e della comunicazione come smartphone, tablet, computer portatili e desktop per lavorare fuori dalla sede del datore di lavoro. Copre tutte le forme di telelavoro, ma cerca di distinguere tra il lavoro da casa o da una postazione fissa (telelavoro) e il lavoro mobile basato sulle TIC. Quest'ultimo termine è utilizzato in Germania per distinguere il telelavoro svolto a casa da una forma di lavoro più mobile.

Smart working/lavoro agile	Lo smart working si riferisce a un sistema di lavoro flessibile che consente ai dipendenti di lavorare in modo comodo ed efficiente senza vincoli di tempo e di spazio (sempre e ovunque) utilizzando le TIC in rete. Un termine simile ("lavoro agile") viene utilizzato in Italia.
Condizioni di lavoro flessibili	Gli accordi di lavoro flessibile sono opzioni di lavoro alternative che consentono di svolgere il lavoro al di fuori dei tradizionali confini temporali e/o spaziali della giornata lavorativa standard.
Lavoro virtuale	Il lavoro virtuale è un lavoro retribuito o non retribuito che viene svolto utilizzando una combinazione di tecnologie digitali e di telecomunicazioni o che produce contenuti per i media digitali
Lavoro ibrido	Si tratta di un accordo in cui il lavoro può essere svolto in parte presso la sede del datore di lavoro e in parte a casa o in altri luoghi.

Lavoro a distanza e telelavoro: cosa dice la legge?

Regolamenti a livello UE

Al momento manca una legislazione vincolante sul telelavoro, anche se diverse direttive e regolamenti affrontano questioni volte a garantire buone condizioni di lavoro per i telelavoratori. Esiste tuttavia l'*Accordo quadro europeo sul telelavoro* (2002). Questo documento è un accordo autonomo tra le parti sociali europee (CES, UNICE, UEAPME e CEEP) e obbliga le organizzazioni nazionali affiliate ad attuarlo secondo le "procedure e le pratiche" specifiche di ogni Stato membro.

Lavoro a distanza/ telelavoro e legge - l'esempio della Polonia

La legge del 1° dicembre 2022 che modifica la legge sul codice del lavoro e alcuni altri atti ha introdotto il concetto di lavoro a distanza nel diritto del lavoro polacco, abrogando le disposizioni sul telelavoro. Secondo questa modifica, il lavoro a distanza **è un lavoro svolto in tutto o in parte in un luogo indicato dal dipendente e in ogni caso concordato con il datore di lavoro,** compreso l'indirizzo di casa del dipendente, tra l'altro utilizzando mezzi di comunicazione diretta a distanza.

Il telelavoro, invece, è una qualsiasi forma di organizzazione e/o esecuzione del lavoro con l'ausilio di tecnologie informatiche, nel contesto di un contratto/rapporto di lavoro, in cui il lavoro **che potrebbe essere svolto anche presso i locali del datore di lavoro viene regolarmente svolto fuori da tali locali**. Mentre il lavoro a distanza può essere temporaneo, il telelavoro si basa in linea di principio sullo svolgimento permanente delle mansioni da casa.

Le regole per il lavoro a distanza devono essere stabilite con l'accordo dei sindacati nel regolamento di lavoro o in un accordo individuale con il dipendente. Inoltre, il datore di lavoro non può rifiutare il lavoro a distanza ai genitori che allevano un bambino di età inferiore ai quattro anni, ai genitori o agli assistenti di persone con disabilità o alle donne in gravidanza (a meno che la natura delle mansioni svolte non lo consenta). Il datore di lavoro deve inoltre dotare il lavoratore delle attrezzature e degli strumenti necessari per svolgere il lavoro a distanza compensare, tra l'altro, i costi dell'elettricità o del consumo di Internet.

Il lavoro a distanza può essere effettuato su richiesta del dipendente o per ordine del datore di lavoro. Il datore di lavoro può anche ordinare il lavoro a distanza in caso di stato di emergenza, stato di minaccia epidemica o epidemia conclamata e per cause di forza maggiore, come la distruzione del luogo di lavoro a causa di incendi o inondazioni.

La riforma del Codice del Lavoro include anche una proposta per il cosiddetto lavoro a distanza occasionale, in base alla quale, su richiesta del dipendente, questi potrà svolgere lavoro a distanza per un periodo fino a 24 giorni per anno solare. La richiesta di lavoro a distanza occasionale da parte del lavoratore non è tuttavia vincolante e il datore di lavoro può rifiutarsi di accoglierla.

È importante notare che al datore di lavoro è vietato discriminare un dipendente per lo svolgimento di un lavoro a distanza, così come per il rifiuto di svolgere tale lavoro. Inoltre, il datore di lavoro è tenuto a consentire al dipendente che svolge lavoro a distanza di trovarsi nei locali del luogo di lavoro, di comunicare con gli altri dipendenti e di utilizzare i locali e le strutture del datore di lavoro, le strutture sociali dell'azienda e le attività sociali - alle stesse condizioni degli altri dipendenti.

Telelavoro/lavoro agile in Italia

Nell'ordinamento italiano il lavoro da remoto si articola nelle modalità del telelavoro e del lavoro agile, alle quali si accede mediante la stipulazione di un accordo individuale tra datore di lavoro e lavoratore.

Il telelavoro è una forma di organizzazione del lavoro caratterizzata dalla regolarità dell'attività lavorativa esterna ai locali dell'impresa o della pubblica amministrazione, che trova regolazione per il pubblico impiego nel decreto del Presidente della Repubblica n. 70 del 1999 e per il settore privato nell'accordo interconfederale del 9 giugno 2004.

Il lavoro agile è una modalità esecutiva del rapporto di lavoro subordinato contraddistinta dall'alternanza tra l'attività interna ed esterna ai locali aziendali nonché dalla flessibilità di orario e di luogo di lavoro. La base giuridica è la legge n. 81 del 2017, che si applica nei limiti di compatibilità anche al pubblico impiego. Inoltre, il lavoro agile è oggetto di contrattazione collettiva in conformità alle linee guida stabilite per il settore privato dal Protocollo nazionale sul lavoro in modalità agile del 7 dicembre 2021.

Per quanto concerne gli strumenti di lavoro, ferma restando l'opportunità di una formazione specifica sia per i telelavoratori che per i lavoratori agili, il datore di lavoro come nel telelavoro di norma provvede alla compensazione o copertura dei costi direttamente derivanti dal lavoro, così nel lavoro agile si fa di norma carico delle spese di manutenzione e di sostituzione della strumentazione fornita.

Fatta salva la facoltà del telelavoratore di chiedere ispezioni, il datore di lavoro, le rappresentanze dei lavoratori e/o le autorità competenti hanno accesso al luogo di svolgimento della prestazione lavorativa, nei limiti fissati dalla normativa sulla salute e sicurezza sul lavoro nonché dalla contrattazione collettiva. In caso di domicilio, l'accesso è subordinato all'obbligo di preavviso ed al consenso del telelavoratore.

Quanto al lavoro agile, l'onere di ispezionare i luoghi di svolgimento dell'attività esterna si ricava implicitamente dalla configurazione legale del datore di lavoro come responsabile della sicurezza. Tuttavia, nella prassi applicativa il giudizio di idoneità di tali luoghi sotto i profili della sicurezza e della riservatezza è spesso rimesso alla responsabilità del lavoratore agile.

Fermo restando l'obbligo di cooperazione a carico sia del telelavoratore che del lavoratore agile, il datore di lavoro deve informare il telelavoratore delle politiche aziendali in materia di salute e sicurezza sul lavoro ed il lavoratore agile, il/i rappresentante/i dei lavoratori per la sicurezza dei rischi generali e specifici connessi alla particolare modalità esecutiva del rapporto di lavoro.

Infine, al fine di prevenire il rischio di isolamento, sono da sottolineare da un lato l'obbligo per il datore di lavoro di fornire l'opportunità al telelavoratore di incontrarsi regolarmente con i colleghi e di accedere alle informazioni dell'azienda nonché, dall'altro, la configurazione della formazione per i lavoratori agili come momento di interazione e di scambio in presenza.

1.5 Algoritmi e discriminazione sul posto di lavoro

In un mondo guidato dalle informazioni, sentiamo sempre più spesso parlare di *intelligenza artificiale* (IA), le cui applicazioni si trovano praticamente ovunque. Si può prevedere che sarà sempre più utilizzata anche in ambito lavorativo. Secondo uno studio di

Forbes, circa quattro aziende su cinque considerano l'IA una priorità assoluta nella loro strategia aziendale. Tuttavia, le speranze di ottimizzazione dei costi e di maggiore efficienza nella produzione sono accompagnate dal timore dei dipendenti di perdere il posto di lavoro: secondo il rapporto Future of Jobs Forecast di Forrester, il numero di posti di lavoro persi per l'automazione raggiungerà 12 milioni solo in Europa entro il 2040.

Nonostante questa nuova tecnologia accenda gli animi, nel dibattito pubblico manca ancora una solida spiegazione di come funziona l'intelligenza artificiale e se qualsiasi tipo di automazione possa essere sicuramente classificata come IA. Per una piena comprensione del problema, è necessario anche considerare qual è la differenza tra un sistema di intelligenza artificiale e gli algoritmi, dato che questi termini sono spesso usati in modo intercambiabile.

AI è un termine estremamente ampio che comprende un gruppo di algoritmi in grado di modificare i propri parametri e creare nuovi algoritmi in risposta agli input appresi. Questa capacità di cambiare, adattarsi e crescere sulla base di nuovi dati è ciò che viene definito "intelligenza".

In termini più semplici, l'intelligenza artificiale può quindi essere definita come la **capacità delle macchine di comprendere, apprendere, pianificare e dimostrare creatività. Secondo la** definizione proposta dalla proposta di Regolamento sull'Intelligenza Artificiale (AI Act), invece, per sistema di intelligenza artificiale si intende un software sviluppato utilizzando una o più delle tecniche e degli approcci elencati nel regolamento[4] , in grado - per un determinato insieme di scopi definiti dall'uomo - di generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagisce.

Un algoritmo è un insieme di istruzioni, o più precisamente una formula computazionale, che prende autonomamente decisioni basate su modelli statistici o regole decisionali senza un esplicito intervento umano. Rappresenta una sequenza di istruzioni che indicano al computer cosa fare all'interno di un insieme di passi e regole precisamente definiti per

[4] Tecniche e approcci di intelligenza artificiale elencati nella normativa:

(a) meccanismi di apprendimento automatico, tra cui l'apprendimento supervisionato, l'apprendimento automatico non supervisionato e l'apprendimento per rinforzo, utilizzando un'ampia gamma di metodi, tra cui l'apprendimento profondo;

(b) metodi logici e basati sulla conoscenza, tra cui la rappresentazione della conoscenza, la programmazione induttiva (logica), le basi di conoscenza, i motori di inferenza e deduzione, il ragionamento (simbolico) e i sistemi esperti;

(c) approcci statistici, stima bayesiana, metodi di ricerca e ottimizzazione.

eseguire un compito. Si tratta quindi di un corso d'azione predeterminato, rigido e codificato che si attiva quando si incontra un elemento specifico.

Un tema legato al campo dell'intelligenza artificiale è l'*autoapprendimento* (*machine learning*, ML). Il suo obiettivo principale è quello di creare un sistema operativo automatico che sia in grado di migliorarsi sulla base dell'esperienza sotto forma di dati e di acquisire nuove conoscenze su questa base. Il processo si basa sulla ricerca di uno schema nei dati forniti per rispondere a una domanda su un insieme sconosciuto. Si tratta quindi di una sorta di previsione del futuro che utilizza la probabilità e la statistica.

Non tutta l'intelligenza artificiale presenta capacità di autoapprendimento. Infatti, a volte un algoritmo può essere scritto in modo tale che il programma in cui è incorporato esegua i comandi senza apprendere da nuovi dati (come nel caso del ML).

Un esempio di algoritmo già correttamente programmato è quello del famoso supercomputer IBM Deep Blue. Questa macchina è diventata famosa dopo essere riuscita a vincere a scacchi contro il campione Garry Kasparov, 25 anni fa. Questo perché Deep Blue aveva memorizzato tutte le mosse possibili, a seconda del posizionamento dei pezzi sulla scacchiera e della strategia dell'avversario. Grazie a questo e alla sua elevata potenza di calcolo, poteva agire efficacemente in qualsiasi situazione.

L'opposto dell'algoritmo implementato in Deep Blue di IBM è stato il programma AlphaGo di DeepMind. Utilizzando meccanismi di autoapprendimento, questo sistema ha imparato a giocare a GO (un antico gioco da tavolo cinese in cui l'obiettivo è circondare il maggior numero possibile di territori con le proprie pietre su una scacchiera inizialmente vuota) e ha persino battuto un giocatore considerato il migliore al mondo.

L'intelligenza artificiale generale, invece, è un sistema autocosciente e dotato di conoscenze o capacità cognitive complete, in grado di pensare ed eseguire compiti in modo autonomo.

La creazione dell'originalità tecnologica è stata per anni oggetto di molte controversie, ci si è soprattutto chiesto innanzitutto se sia possibile. Secondo uno dei principali critici dell'ascesa dell'intelligenza artificiale generale, il filosofo Hubert Dreyfus, i computer che non hanno un corpo, non attraversano l'infanzia e l'adolescenza e non partecipano a esperienze culturali, non possono assolutamente acquisire un'intelligenza in senso umano. Una delle argomentazioni principali di Dreyfus era che lo sviluppo dell'intelligenza umana avviene in parte in modo inconscio e quindi non può essere articolato e incorporato in un programma informatico.

Algoritmi al lavoro

1. **Analisi del CV del candidato mediante un algoritmo prima dell'instaurazione del rapporto di lavoro**

L'assunzione algoritmica prevede l'utilizzo di sistemi di intelligenza artificiale e di *machine learning* per individuare i candidati, reclutare, fare colloqui e assumere per coprire dei posti di lavoro. Questa tecnica utilizza una serie di criteri per valutare un candidato, tra cui l'esperienza e la formazione, e spesso filtra i CV ricevuti utilizzando parole chiave. Gli algoritmi possono anche aiutare a valutare le competenze più *soft*, come la propensione del candidato ad apprendere rapidamente e a lavorare in team.

Utilizzando diversi strumenti di intelligenza artificiale durante il reclutamento, le aziende vogliono garantire che il processo sia condotto in modo equo. Questo perché, in teoria, non c'è spazio per il fattore umano e per eventuali discriminazioni nella prima valutazione automatizzata. Tuttavia, questi sistemi sono spesso criticati perché riflettono i pregiudizi delle persone che li hanno programmati.

È importante notare che gli algoritmi non prendono la decisione finale di assunzione. Il loro scopo principale è quello di restringere il campo dei candidati.

Metodi di analisi dei CV per algoritmo:

- **Punteggio del CV** - un algoritmo assegna punti in base a criteri predeterminati dal selezionatore,
- **Ranking** - ordinamento dei CV in base alla presenza di parole chiave,
- **Corrispondenza** - identificare le parole chiave che corrispondono a quelle dell'annuncio di lavoro,
- **Analisi** - l'algoritmo analizza la semantica del CV, estrae le informazioni principali e le suddivide in diverse categorie: esperienza, competenze, contatti.

2. **Caratteristiche e aree di utilizzo degli algoritmi sul posto di lavoro**

Tipi di algoritmi:

- **Descrittivi** - utilizzati per registrare eventi passati e analizzarne l'impatto sugli eventi presenti, come ad esempio gli algoritmi di valutazione delle prestazioni progettati per raccogliere vari tipi di dati relativi alle prestazioni dei dipendenti e indicare una valutazione complessiva.
- **Predittivi** - mirano a prevedere il comportamento futuro o a stimare la probabilità che un evento si verifichi (ad esempio, prevedere un aumento della domanda di nuovi dipendenti).

- **Prescrittivo/raccomandativo**: il loro compito è selezionare lo scenario migliore tra varie possibilità e raccomandare un'azione specifica o semplicemente attuarla (ad esempio, decidere le risorse umane, l'assegnazione dei compiti o il calendario).

L'uso degli algoritmi nel mondo del lavoro comporta la cosiddetta **gestione algoritmica,** ovvero "un sistema di controllo in cui agli algoritmi viene affidata la responsabilità di prendere ed eseguire decisioni di prendere ed eseguire decisioni che riguardano il lavoro, riducendo così la partecipazione umana e la supervisione del processo di lavoro".

Sei funzioni chiave di gestione del flusso di lavoro per le quali sono stati utilizzati algoritmi:

1. monitoraggio/controllo dei dipendenti
2. definizione degli obiettivi
3. gestione delle prestazioni
4. programmazione

5 retribuzione

6. cessazione del rapporto di lavoro

Aumentare il controllo del datore di lavoro sui dipendenti con gli algoritmi

- **Raccomandazione algoritmica** - i datori di lavoro utilizzano algoritmi per valutare una determinata situazione e dare suggerimenti per far sì che il dipendente compia l'azione indicata dall'algoritmo.
- **Restrizione algoritmica** - l'uso di algoritmi per visualizzare solo determinate informazioni e consentire determinati comportamenti impedendone altri.

L'uso di algoritmi può aumentare la frustrazione dei dipendenti che, dovendo attenersi a raccomandazioni incomprensibili, possono sentire sminuita la loro voce in capitolo.

Algoritmi utilizzati per valutare il lavoro

- Registrazione **algoritmica** - l'uso di procedure computazionali per monitorare, aggregare e riportare, spesso in tempo reale, un'ampia gamma di dati selezionati con precisione da fonti interne ed esterne.
- **Tecnologie computazionali** - utilizzate per raccogliere valutazioni e classifiche per calcolare una qualche misura delle prestazioni dei dipendenti; anche analisi predittive per prevedere le loro prestazioni future.

La valutazione del lavoro tramite algoritmi può sollevare problemi specifici, non solo legati alla discriminazione, ma anche alla perdita del senso di privacy dei dipendenti, alla sicurezza delle informazioni, ecc.

Algoritmi utilizzati per la remunerazione

La remunerazione algoritmica può fornire premi in tempo reale per i comportamenti che seguono linee guida predefinite. Può anche utilizzare i principi della *gamification* per rendere l'esperienza lavorativa più positiva e divertente per i dipendenti.

Disciplina sul posto di lavoro

La sostituzione algoritmica consiste nel licenziamento rapido o addirittura automatico di dipendenti con scarse prestazioni dall'organizzazione e nella loro sostituzione con dipendenti più efficienti.

Processo decisionale automatizzato e profilazione

L'articolo 22 del GDPR stabilisce che l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente su un trattamento automatizzato, compresa la profilazione, che produca effetti giuridici o incida in modo analogo significativamente sulla persona.
Il diritto di una persona di contestare una decisione automatizzata riguardante la sua persona si basa sui due motivi della profilazione qualificata: il trattamento automatizzato e gli effetti giuridici o i fattori che incidono significativamente sulla persona.

Che cos'è il processo decisionale automatizzato?

Grazie alla conoscenza codificata e all'analisi precisa delle condizioni ambientali, un computer può impartire istruzioni senza l'intervento dell'uomo. Questa azione si basa su calcoli avanzati e su mezzi di elaborazione esclusivamente tecnici. In questo modo, il coinvolgimento umano nei processi decisionali è ridotto al minimo e i risultati vengono forniti in modo automatizzato.

Tuttavia, affinché il trattamento dei dati sia considerato completamente automatizzato, non deve esserci alcun intervento umano nel processo decisionale. Va notato che un apparente coinvolgimento umano nel processo decisionale, consistente, ad esempio, nella mera approvazione di un verdetto indicato da un algoritmo, non costituirà un motivo di esclusione dall'ambito di applicazione del divieto di cui all'articolo 22 del GDPR. Tuttavia, se una persona, con il potere e l'autorità di cambiare il verdetto, agisse per modificare il verdetto, il processo decisionale automatizzato non avrebbe luogo.

Per quanto riguarda il catalogo delle situazioni coperte dall'articolo 22 del GDPR, questo è ampio e copre sia le situazioni in cui la decisione produce effetti giuridici (cioè incide sui diritti di un individuo ai sensi della legge; ad esempio, il diritto all'indennità di disoccupazione) sia quelle che hanno un "effetto altrettanto significativo" (ad esempio, relativo alla situazione finanziaria o alla salute del soggetto).

Che cos'è il profiling?

L'articolo 22 del GDPR comprende anche una categoria specifica di processo decisionale automatizzato, ossia quello basato sulla profilazione. Il termine "profilazione" (articolo 4 del GDPR) si riferisce a qualsiasi forma di trattamento automatizzato di dati personali che preveda l'uso di dati personali per valutare determinati fattori personali di una persona fisica. In particolare, si tratta dell'analisi o della previsione di aspetti relativi al **rendimento lavorativo**, alla situazione economica, alla salute, alle preferenze personali, agli interessi, all'affidabilità, al comportamento, all'ubicazione o agli spostamenti **di tale persona**[5] .

Esempi pratici di profilazione:

- **marketing** - creazione di profili di consumatori raccogliendo informazioni sulle preferenze di acquisto e facendo in modo che il sistema suggerisca prodotti personalizzati per il cliente,
- **prestiti e crediti** - profilando i candidati e prendendo una decisione di credito positiva subordinata all'analisi dei dati personali forniti all'algoritmo,
- **prestazioni di assistenza sociale** - utilizzo del profiling per allocare in modo equo le risorse dell'assistenza pubblica,
- **reclutamento e risorse umane** - i processi di reclutamento di massa sono spesso condotti utilizzando sistemi che analizzano i CV e altri dati dei candidati in modo indipendente e, sulla base di tale analisi, decidono se rifiutare o accettare il candidato (ad esempio, dopo aver cercato i CV per parole chiave). Nel campo delle risorse umane, la profilazione viene utilizzata anche per la valutazione delle offerte di lavoro.

Rischi associati alla profilazione

- **Ingerenza nella privacy e mancanza di trasparenza** - mentre molte persone sono consapevoli che alcuni tipi di dati (ad esempio quelli medici) sono particolarmente

[5] Va notato che, nonostante le somiglianze, la profilazione e il processo decisionale automatizzato sono due attività diverse che possono essere o meno collegate.

sensibili e dovrebbero essere protetti, una parte del pubblico non è consapevole di quante informazioni personali possano essere ricavate dai dati comportamentali utilizzati per una profilazione indesiderata. Inoltre, lo stesso processo di profilazione può essere spesso non trasparente e incomprensibile per le persone interessate.

- **Discriminazione** - gli algoritmi progettati dall'uomo possono portare con sé i pregiudizi dei loro creatori. Pertanto, il sistema potrebbe trattare in modo meno favorevole, ad esempio, persone con opinioni religiose, orientamento sessuale o colore della pelle diversi.
- **Riduzione della diversità** - la profilazione è progettata per valutare, caratterizzare e segmentare il pubblico di un determinato contenuto, al fine di adattare il materiale in base agli interessi o alle convinzioni (ad esempio, politiche) degli individui interessati. In questo modo, semplifica il catalogo delle informazioni fornite all'utente, limitando la diversità dei contenuti e creando le cosiddette bolle informative, restringendo l'orizzonte virtuale del destinatario.

Profilazione nel processo di lavoro - un *case study*

Dal 2020 il Centro per l'impiego austriaco (AMS) utilizza una profilazione algoritmica delle persone in cerca di lavoro per aumentare l'efficienza del processo di consulenza e adeguare i programmi attuali alle esigenze del mercato del lavoro. Il sistema mira a classificare le persone in cerca di lavoro in tre categorie:

- Gruppo A. Buone prospettive di trovare lavoro nel prossimo periodo.

- Gruppo B. Prospettive medie.

- Gruppo C. Basse prospettive a lungo termine.

Poi, a seconda della categoria assegnata, un algoritmo adatta il programma di assistenza alle esigenze del singolo.

Domanda di discussione: La profilazione algoritmica dei disoccupati per adattare i programmi di sostegno alle loro esigenze è giustificata?

Un esempio: a New York è stata annunciata una legge che limita l'uso di strumenti di intelligenza artificiale nei processi di assunzione. Come indicato, il problema principale che si verificava con le valutazioni realizzate dall'intelligenza artificiale era l'esclusione dal processo di gruppi che non rientravano nella chiave pre-programmata. Ad esempio, la squalifica delle persone con un difetto di pronuncia durante un colloquio video valutato dal computer, o il

rifiuto di candidati con artrite o altre condizioni che limitano la loro idoneità fisica (per i test a tempo).

Domanda di discussione: Dovrebbero essere vietati tutti i tipi di valutazione algoritmica nel processo di assunzione?

Un esempio: un imprenditore stava lavorando allo sviluppo e all'implementazione di uno strumento di intelligenza artificiale nella sua azienda per aiutare ad assumere persone adatte al lavoro. Il lavoro è stato interrotto quando l'azienda si è resa conto che il sistema discriminava le donne. Il motivo del rifiuto più frequente dei profili femminili era che l'intelligenza artificiale si basava sui dati dei CV delle persone che avevano lavorato per l'azienda negli ultimi 10 anni (per lo più uomini). Di conseguenza, il computer ha valutato che avrebbe dovuto dare priorità agli uomini, riducendo automaticamente le possibilità di candidature con caratteristiche femminili.

Domanda di discussione: Potete identificare altri esempi di discriminazione che potrebbero verificarsi durante il reclutamento utilizzando algoritmi di profilazione?

Rischi e benefici dell'uso di algoritmi contro i dipendenti

Minacce:

- maggiore controllo da parte del datore di lavoro a scapito della privacy del dipendente (mancanza di un consenso adeguato da parte del dipendente)
- erosione dell'autonomia umana attraverso la sostituzione del contatto diretto tra i manager e i loro subordinati, ovvero la "disumanizzazione" dei sistemi di gestione
- pregiudizio e discriminazione algoritmica.

Vantaggi:

- aumento della produttività grazie al risparmio di tempo e a un processo decisionale più efficiente,
- pianificazione dei turni e un'assegnazione delle responsabilità più efficaci,
- possibilità di un reclutamento più rapido,
- comprensione dei problemi che sorgono sul posto di lavoro grazie a una migliore conoscenza dell'ambiente di lavoro,
- meno frequenti favoritismi dei dipendenti e l'eliminazione dei pregiudizi che possono esistere nei rapporti diretti con i dipendenti,

- un processo decisionale automatizzato limita la possibilità di interferire con le decisioni della dirigenza in materia di retribuzione, approvazione delle ferie o assegnazione dei turni.

Algoritmizzazione del rapporto dipendente-datore di lavoro

L'algoritmizzazione dei processi lavorativi è già una realtà in molte aziende. Tuttavia, spesso si scontra con i dipendenti su questioni quali:

- **Licenziamento automatico dei dipendenti** (questione da discutere durante il workshop).
- **Liquidazione algoritmica dei salari:**
    - L'algoritmo dell'app per *rider* ordinava agli autisti di evadere gli ordini indipendentemente dalla distanza dal punto di ritiro. Gli autisti non venivano pagati per la distanza dal punto di ritiro. L'imprenditore copriva solo il costo del tragitto più breve, con il risultato che, dedotti i costi del carburante e l'ammortamento dell'auto, gli autisti non ricavavano alcun profitto.
    - L'azienda ha sostenuto che i guadagni dipendono dal numero di chilometri percorsi e che esiste una tariffa fissa per ogni ordine, chiamata "tariffa base", che può variare da città a città.
    - Tuttavia, anche l'incertezza dei lavoratori sulla tariffa oraria ha rappresentato un problema: durante il periodo della pandemia, i corrieri sono stati informati nel giro di un giorno che la tariffa era cambiata, con la conseguenza che spesso erano costretti a rimetterci piuttosto che guadagnare per il lavoro svolto.
    - In seguito allo sciopero, ai corrieri sono stati promessi diversi cambiamenti, tra cui la possibilità di rifiutare un ordine tre volte al giorno, anziché una sola. In questo modo, in caso di variazione sfavorevole del tasso di base, i corrieri hanno la possibilità di rifiutare un ordine. Tuttavia, non è stata dichiarata una maggiore stabilizzazione dei tassi.
- **Identificazione algoritmica dei dipendenti**
    - Le app di taxi utilizzano un software per verificare l'identità dei loro conducenti in base ai selfie che caricano. Nel 2018, questo tipo di software, utilizzato da un'azienda, si è rivelato incline a commettere errori quando si tratta di persone con la pelle scura (vale la pena notare che la stragrande

maggioranza dei conducenti che utilizzano le app per i taxi è di sesso maschile e molti provengono da ambienti BAME *(afroamericani, asiatici e di minoranze etniche)*.

- In relazione alla verifica dell'identità, più di una dozzina di corrieri hanno riferito che, a causa di problemi con l'algoritmo, sono stati minacciati di licenziamento, hanno subito il blocco dell'account o sono stati licenziati definitivamente dopo che un selfie scattato non ha superato il *Real Time ID Check*. Alcuni sono stati licenziati dopo che la funzione selfie si è rifiutata di funzionare. Questo processo non prevedeva il diritto di appello.

- **Valutazione algoritmica dei dipendenti (di performance e non)** (argomento che verrà discusso nel corso del workshop).

Algoritmizzazione e protezione dei dati

Come già detto, un algoritmo è una serie di istruzioni su come trasformare un insieme di fatti sul mondo in informazioni utili. Per dirla in modo ancora più semplice, i fatti sono trattati come dati, mentre le informazioni sono conoscenze che possono essere ulteriormente utilizzate dall'uomo o da altre macchine.

I dati sul posto di lavoro e la loro protezione

Per evitare conflitti in materia di privacy, i datori di lavoro devono attuare misure adeguate per proteggere i dati personali, in particolare quando tali dati vengono utilizzati per processi decisionali automatizzati con un impatto diretto sul dipendente. È quindi necessario bilanciare in modo appropriato l'interesse del datore di lavoro a implementare tecnologie basate sui dati e il benessere della persona interessata, agendo in conformità con i principi fondamentali della GDPR.

- **I datori di lavoro devono raccogliere dati sui dipendenti solo quando è necessario per la gestione del posto di lavoro e delle prestazioni dei dipendenti.**

Stando al principio della minimizzazione dei dati, i datori di lavoro dovrebbero limitare la raccolta dei dati dei dipendenti, ossia qualsiasi informazione relativa alla loro identità, salute e biometria, dati relativi alle attività sul posto di lavoro (ad esempio sulla produttività), ma anche informazioni derivanti dalle attività dei dipendenti sui social media. La raccolta di dati senza limiti espone inutilmente i dipendenti a rischi quali, ad esempio, l'uso improprio dei dati personali da parte dei datori di lavoro o la fuga incontrollata di notizie.

- **I dipendenti devono avere il diritto di ispezionare, correggere e recuperare i propri dati**

I dipendenti dovrebbero essere in grado di ricevere tutte le informazioni pertinenti sui loro dati, tra cui il motivo e il modo in cui i dati sono stati raccolti, cosa è stato dedotto sul dipendente dai dati e se i dati sono stati utilizzati per prendere una decisione relativa al loro impiego. I datori di lavoro dovrebbero invece essere responsabili di correggere eventuali dati inesatti.

- **I dati dei dipendenti devono essere protetti da un uso improprio**

In nessun caso un datore di lavoro dovrebbe consentire la vendita o la concessione in licenza dei dati dei dipendenti a terzi, senza questa riserva la promessa di profitto derivante dalla monetizzazione dei dati dei dipendenti creerebbe un rischio troppo grande di sfruttamento speculativo dei dati da parte dei datori di lavoro.

- **Consenso al trattamento dei dati personali**

Nei rapporti di lavoro, il consenso al trattamento dei dati personali è molto controverso perché, a causa dello squilibrio delle parti, è facile mettere in dubbio la facoltatività del consenso dato dal dipendente. Va notato che un datore di lavoro potrebbe facilmente costringere un dipendente a soddisfare le sue aspettative con la minaccia di conseguenze negative sul lavoro. Tuttavia, ai sensi dell'articolo 155 del GDPR, gli Stati membri possono introdurre norme specifiche relative al trattamento dei dati personali dei dipendenti nel contesto del lavoro e, in particolare, alle condizioni in cui i dati personali possono essere trattati con il consenso del dipendente.

Ad esempio, in Polonia, il datore di lavoro può raccogliere i dati personali elencati nel Codice del Lavoro se il dipendente è d'accordo. Tuttavia, va notato che il consenso deve essere dato volontariamente e quindi non sarà efficace se il dipendente non ha la possibilità di rifiutarlo per paura di subire conseguenze negative. Inoltre, può essere revocato in qualsiasi momento.

In Italia, fermo restando il rispetto della normativa sulla *privacy*, acquista particolare rilievo – a prescindere dalla necessità o meno di raccogliere il consenso del lavoratore interessato dal trattamento dei dati personali – il divieto per il datore di lavoro «di effettuare indagini [...] sulle opinioni politiche, religiose o sindacali del lavoratore nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale» (art. 8 l. n. 300/1970).

Tipi di dati utilizzati nelle diverse fasi di lavoro

Fase I. Ricerca di lavoro

Cosa può aspettarsi un datore di lavoro?

Il datore di lavoro può aspettarsi che il candidato gli fornisca i dati di base necessari per procedere alla stipula del contratto. Questi dati possono includere:

- identificazione (nome, cognome, data di nascita),
- contatto indicato da tale persona;
- istruzione, competenze, esperienza lavorativa (titoli scolastici e universitari, formazione e corsi frequentati, precedenti datori di lavoro, posizioni ricoperte e responsabilità professionali).

È importante notare che in caso di partecipazione al processo di reclutamento, nonostante l'invio di dati, non è necessario che alla fine si concluda un contratto.

Cosa può aspettarsi un candidato?

Già nella prima fase del processo di assunzione, un potenziale datore di lavoro che raccoglie dati dai candidati è obbligato a informarli:

- il nome completo e l'indirizzo legale dell'azienda,
- i dati di contatto del Responsabile della protezione dei dati (se nominato),
- la finalità del trattamento e la base giuridica del trattamento, i destinatari (intesi in senso lato) o le categorie di destinatari a lui noti al momento della raccolta,
- l'intenzione di un trattamento transfrontaliero dei dati (se presente),
- il periodo per il quale i dati saranno trattati o i criteri per determinare tale periodo,
- il diritto del candidato di richiedere l'accesso ai dati, compresa una copia degli stessi, nonché la rettifica, la cancellazione o la limitazione del trattamento,
- il diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento effettuato sulla base del consenso prima della sua revoca (se i dati sono raccolti sulla base del consenso),
- il diritto di presentare un reclamo al Garante per la protezione dei dati
- la volontarietà o l'obbligo di fornire i dati e le conseguenze del mancato conferimento.

Fase II. Processo di reclutamento

Durante il colloquio, il selezionatore può fare molte domande dettagliate sulle informazioni che il candidato ha inserito nel suo CV. È importante, tuttavia, che queste si riferiscano solo a questioni relative alla posizione per la quale il candidato si sta candidando. Sono inaccettabili le domande che possono mettere in imbarazzo il candidato, violare il suo diritto alla privacy o i suoi interessi personali (per es. diritto alla privacy o interessi personali o riguardanti la vita privata, la religione, l'orientamento sessuale, le opinioni politiche, ecc.)

Tempo di archiviazione dei dati

Il periodo di conservazione dei dati del candidato deve essere conforme alle regole di trattamento dei dati predeterminate dal responsabile del trattamento. Come regola generale, il datore di lavoro dovrebbe quindi cancellare definitivamente i dati personali di un candidato con il quale ha deciso di non concludere un contratto di lavoro subito dopo la conclusione del processo di assunzione, ossia dopo aver firmato un contratto di lavoro con il dipendente appena assunto (ad esempio, cancellando o restituendo i dati).

Fase III. Periodo di occupazione

Con l'instaurazione di un rapporto di lavoro, sorgono alcuni diritti e obblighi sia per il datore di lavoro che per il dipendente. L'attuazione di questi comporta chiaramente il trattamento dei dati personali del dipendente. La gestione dei dati personali, sebbene in linea di principio regolata dal GDPR, è ulteriormente chiarita nel caso del lavoro dalla legislazione nazionale.

Ad esempio, in Polonia, ai sensi dell'articolo 221, paragrafi 2 e 4, del Codice del Lavoro, un datore di lavoro ha il diritto di richiedere a un dipendente che ha deciso di assumere, di fornire (in aggiunta ai dati personali che può aver ottenuto da lui/lei nel corso dell'assunzione) anche i dati personali:

- indirizzo di residenza,
- numero PESEL[6]

[6] In Polonia è il numero d'identità anagrafica, simile per uso al Codice Fiscale italiano.

- altri dati personali, compresi, tra l'altro, i nomi e le date di nascita dei figli, se il conferimento di tali dati è necessario per l'esercizio di prerogative speciali ai sensi del diritto del lavoro,
- istruzione e storia lavorativa precedente, se non c'erano i presupposti per richiederli al candidato all'assunzione,
- il numero di conto corrente per il pagamento se il dipendente non ha richiesto il pagamento in contanti

In Italia l'articolo 8 della legge n. 300 del 1970 (c.d. Statuto dei lavoratori) vieta al datore di lavoro di indagare – sia in sede di assunzione che durante lo svolgimento del rapporto lavorativo – le opinioni politiche, religiose o sindacali del lavoratore/candidato nonché fatti non rilevanti ai fini dell'attitudine professionale. I dati personali diversi da quelli richiamati sono trattati nel rispetto della normativa sulla *privacy*, che trova regolazione a livello comunitario nel regolamento dell'UE n. 679 del 2016 (*GDPR*) e a livello interno nel decreto legislativo n. 196/2003 (c.d. Codice *privacy*) come modificato dal decreto legislativo n. 101 del 2018.

Obblighi di informazione del datore di lavoro nei confronti del lavoratore

Poiché il datore di lavoro tratterà i dati del dipendente per una finalità diversa da quella del candidato, il dipendente deve essere informato a questo proposito. Tale finalità può essere soddisfatta includendo tali informazioni nella clausola informativa fornita ai candidati nel corso del processo di assunzione, integrandola con informazioni sulle finalità del trattamento e indicando i destinatari dei dati in caso di assunzione del candidato, oppure integrando tali informazioni poco dopo l'assunzione del dipendente.

Controllo degli algoritmi utilizzati nel lavoro (trasparenza degli algoritmi)

Gli esempi di utilizzo dell'intelligenza artificiale sul posto di lavoro citati di seguito dimostrano
che l'uso incontrollato di strumenti di IA da parte delle aziende può portare a una maggiore insicurezza del lavoro e quindi avere un impatto negativo sulla vita dei dipendenti. Allo stesso tempo, secondo le stime del McKinsey Global Institute, entro il 2030 fino al 70% delle aziende avrà implementato una qualche forma di sistemi di intelligenza artificiale. Ecco perché è così importante valutare criticamente le nuove tecnologie e consentire alle autorità di regolamentazione e alle organizzazioni indipendenti di verificare l'IA.

- Nel Regno Unito, il software Horizon utilizzato dal National Post Office ha erroneamente sospettato singoli dipendenti di aver sottratto decine di migliaia di sterline. A causa dell'errore dell'intelligenza artificiale, ben 736 impiegati postali sono stati perseguiti e alcuni sono stati accusati e condannati.
- Nei Paesi Bassi, i conducenti di un'app per taxi hanno citato in giudizio la società dopo che un algoritmo aveva bloccato i loro account per presunte frodi. Il tribunale ha respinto le loro richieste perché ha ritenuto che le violazioni non rientrassero nella definizione di processo decisionale completamente automatizzato ai sensi del GDPR. Di conseguenza, i dipendenti sono rimasti senza alcuna tutela legale.
- In Italia, un tribunale ha ordinato a un'azienda di consegne di cibo a domicilio di rendere noto l'algoritmo dell'app e di eliminare gli elementi che, non avendo affrontato questioni regolamentate dal diritto del lavoro (come i congedi per malattia o il diritto di sciopero), la rendevano discriminatoria.

Algoritmo e segreto aziendale

Ai sensi della normativa europea, le informazioni sulla tecnologia o su qualsiasi altro aspetto di un'azienda possono essere protette come segreto aziendale. Tuttavia, devono soddisfare le seguenti condizioni:

- le informazioni sull'algoritmo non sono note al grande pubblico o agli esperti del settore,
- le informazioni sull'algoritmo hanno un valore commerciale,
- sono state adottate misure per garantire la riservatezza delle informazioni, ad esempio sono conservate in un luogo sicuro e tutti coloro che vi hanno accesso o che le condividono hanno firmato un accordo di riservatezza.

Nel caso delle nuove tecnologie utilizzate nei processi di lavoro, soddisfare questa logica non è difficile. Le aziende citano spesso i segreti commerciali, evidenziando le loro preoccupazioni per la perdita di competitività derivante dall'esposizione dei loro sistemi interni. Pertanto, la comprensione degli algoritmi e la verifica degli strumenti di IA nel settore privato sono particolarmente problematici. Inoltre, ulteriori forme di tutela legale sotto forma di clausole di riservatezza impediscono agli *insider* (dipendenti attuali o ex) di condividere informazioni sui meccanismi che coordinano il loro lavoro.

Legge sull'intelligenza artificiale (AI Act)

Le ripetute accuse all'intelligenza artificiale di replicare pregiudizi, imprecisioni o discriminazioni da parte degli algoritmi hanno fatto sì che la Commissione europea si assumesse la responsabilità di introdurre una regolamentazione per controllare gli strumenti di intelligenza artificiale e prevenire gli effetti negativi del loro utilizzo.

12 aprile 2021 la Commissione europea ha presentato una bozza di regolamento UE sull'intelligenza artificiale, il primo atto legislativo completo sugli strumenti di intelligenza artificiale. L'obiettivo del regolamento è fornire un ambiente adatto allo sviluppo dell'intelligenza artificiale nell'Unione europea, tenendo conto dei rischi associati allo sviluppo delle tecnologie più recenti. Soprattutto, l'AI Act mira a rendere gli algoritmi utilizzati nell'UE sicuri, trasparenti, etici, imparziali e controllati dall'uomo.

Approccio basato sul rischio

L'obiettivo principale della legge è quello di identificare i rischi posti da un particolare sistema di IA e di porre come condizione gli obblighi e i requisiti normativi a cui saranno soggetti gli sviluppatori e gli implementatori di IA.

- **Rischi inaccettabili**: vietare l'IA

Divieto di applicazioni particolarmente dannose dell'intelligenza artificiale (IA), contrarie ai valori dell'UE, che rischiano di violare i diritti fondamentali dell'individuo, ad esempio: esecuzione di valutazioni dei cittadini (il cosiddetto *social scoring*), sfruttamento della vulnerabilità di un gruppo specifico di persone a causa dell'età, della disabilità motoria o di un disturbo mentale, uso di tecniche subliminali, uso dell'identificazione biometrica negli spazi pubblici e a fini di applicazione della legge (con alcune eccezioni).

- **Rischio elevato** - IA accettabile, ma a determinate condizioni.

Sono stati classificati come ad alto rischio gli strumenti che hanno un impatto negativo sulla sicurezza o sui diritti fondamentali delle persone, ovvero i sistemi che si trovano nelle seguenti aree:

  - identificazione biometrica e categorizzazione degli individui,
  - gestione delle infrastrutture critiche,
  - istruzione o formazione professionale - la capacità di decidere l'accesso di un individuo all'istruzione e alla formazione professionale (ad esempio, la correzione degli esami),
  - sicurezza dei prodotti (ad esempio, l'uso dell'intelligenza artificiale nella chirurgia assistita da robot),

- assunzione, gestione dei dipendenti e accesso al lavoro autonomo (ad esempio, software di analisi dei CV per le procedure di assunzione),
- servizi pubblici e privati di base (ad esempio, valutazione del credito, credit scoring),
- applicazione della legge - interferenza con i diritti fondamentali delle persone (ad esempio, verifica dell'autenticità dei documenti),
- gestione della migrazione, dell'asilo e del controllo delle frontiere (ad esempio, valutazione delle domande di asilo),
- amministrazione della giustizia e dei processi democratici (ad esempio, suggerendo il tipo di sanzioni e il livello di pena per una persona condannata per un reato).

Esempi di requisiti specifici per i sistemi ad alto rischio:

- **Requisiti di trasparenza** - il funzionamento dei sistemi di IA ad alto rischio deve essere sufficientemente trasparente da consentire agli utenti di interpretare i risultati che li riguardano. Per i sistemi di IA ad alto rischio devono essere sviluppate istruzioni per l'uso.
- **Supervisione umana obbligatoria** dei **sistemi ad alto rischio** - necessaria per fornire agli esseri umani una supervisione efficace delle IA ad alto rischio, compresa la comprensione delle capacità e dei limiti di un determinato sistema di IA. Le misure di supervisione appropriate possono includere la decisione di non utilizzare il sistema di IA in una determinata situazione, ignorare una decisione presa dal sistema di IA o interrompere il sistema con un pulsante di STOP.

Problemi di lavoro sollevati dalla legge sull'intelligenza artificiale

I sistemi ad alto rischio con un impatto sul mercato del lavoro e soggetti a sorveglianza specifica sono elencati nell'allegato III della proposta di legge sull'IA. Si tratta di sistemi di IA:

1. Utilizzati nel processo di reclutamento o di selezione di persone specifiche e, in particolare, quelli utilizzati per pubblicare offerte di lavoro, per pre-selezionare o filtrare le candidature, per valutare i candidati durante i colloqui o i test.
2. Decidere la promozione o il licenziamento di qualcuno, determinare la distribuzione dei compiti e monitorare le prestazioni e il comportamento dei dipendenti.
3. Decidere l'accesso alla formazione professionale o valutare i tirocinanti.

Come detto, i suddetti sistemi di intelligenza artificiale possono avere un impatto significativo sulle prospettive di lavoro delle persone di cui trattano i dati, incidendo così sul loro sostentamento e sul loro reddito. La Commissione europea ha anche sottolineato che i sistemi mal progettati e utilizzati possono perpetuare modelli discriminatori (ad esempio nei confronti di donne, anziani, persone con disabilità, orientamento razziale, etnico o sessuale). Inoltre, i sistemi di intelligenza artificiale utilizzati per verificare le prestazioni (in particolare quelli basati sulla biometria) possono avere un impatto sulla protezione dei dati personali e sul diritto alla privacy. Pertanto, dovrebbero essere soggetti a requisiti particolarmente severi e i dipendenti dovrebbero sempre avere una possibilità di ricorso contro le decisioni degli algoritmi.

Critiche alla legge sull'IA

Anche l'applicazione della legge sull'IA alle questioni occupazionali è stata oggetto di numerose critiche. Secondo gli esperti, il regolamento presta troppa poca attenzione alle questioni lavorative e il controllo della trasparenza degli algoritmi si riduce ai requisiti generali di trasparenza elencati nell'articolo 52 della bozza di regolamento. Inoltre, non è certo che il regolamento entrerà in vigore prima del 2025.

Paura di perdere il lavoro a causa dell'algoritmizzazione/robotizzazione

Secondo le stime di McKinsey, entro il 2030 l'automazione nei vari settori porterà alla necessità di riqualificare ben 375 milioni di lavoratori. Una previsione leggermente diversa, anche se altrettanto preoccupante, è stata fatta dal World Economic Forum nel suo rapporto, che ha indicato nella sua pubblicazione *Future of Jobs* che i progressi nelle aree dell'algoritmizzazione e delle tecniche di calcolo potrebbero portare le macchine a sostituire 75 milioni di posti di lavoro in tutto il mondo nei prossimi anni.

Per quanto riguarda gli effetti della robotizzazione, si può ipotizzare che i lavori manuali, soprattutto quelli basati su sequenze prevedibili, saranno i più colpiti. Tuttavia, anche alcuni professionisti potrebbero essere colpiti negativamente dall'automazione. Secondo il già citato rapporto *Future of Jobs,* tra le professioni soppiantate dall'IA, come il meccanico, il magazziniere e il direttore di produzione, ci sono anche avvocati e analisti finanziari. Inoltre, gli effetti dell'automazione saranno avvertiti da coloro le cui professioni consistono nel raccogliere e trattare dati, ossia mansioni realizzate in modo decisamente più rapido e preciso dalle macchine.

Ben il 60% dei dipendenti vede automatizzato un terzo dei compiti del proprio lavoro. Non deve sorprendere, quindi, che gli occupati siano preoccupati per il loro attuale lavoro. Secondo il rapporto *Pandemic Automates Poland?* della Procontent Communication, quasi

un intervistato su cinque (18,7%) teme l'automatizzazione del proprio lavoro, seguita dalla perdita del posto di lavoro. Tuttavia, gli esperti stemperano i timori: guardando a livello globale, solo il 5% dei posti di lavoro rischia di scomparire completamente. Inoltre, anche se molti lavori saranno soppiantati dalle macchine, si può prevedere che al loro posto emergeranno nuove professioni grazie all'aumento della domanda di competenze trasversali che richiedono creatività, intelligenza emotiva e pensiero critico.

Inoltre, lo sviluppo della tecnologia contribuirà alla continua creazione di nuovi posti di lavoro ad alta remunerazione nel settore IT - a livello globale, si potrebbe arrivare a 50 milioni di posti di lavoro entro la fine del decennio. Questo approccio ottimistico sembra essere confermato dal già citato studio del World Economic Forum, che indica che con l'aumento dell'automazione verranno creati fino a 133 milioni di posti di lavoro. Sebbene sia difficile determinare con precisione la forma dei futuri livelli occupazionali a causa del dinamismo dei cambiamenti apportati dalla digitalizzazione, secondo le valutazioni degli esperti non è certo che nel prossimo futuro si verifichi una disoccupazione tecnologica strutturale.

La tecnologia al servizio dell'inclusività

La digitalizzazione dei posti di lavoro contribuisce a una più efficace integrazione nel mercato del lavoro di quei gruppi sociali che in precedenza ne erano temporaneamente o permanentemente esclusi.

Per le **persone con disabilità si** possono osservare i seguenti vantaggi:

- l'assenza delle difficoltà di trasporto verso il luogo di lavoro che in passato dovevano affrontare le persone con determinate limitazioni fisiche,
- una minore esposizione agli stimoli e una modalità di lavoro a distanza più tranquilla favoriscono un lavoro più efficace per le persone con disabilità intellettive, iperattività o difficoltà di concentrazione e apprendimento,
- l'uso di mezzi di telecomunicazione elettronici (e-mail, messaggistica istantanea) consente la partecipazione attiva alle discussioni da parte di persone con disturbi del linguaggio.

Esempi di vantaggi per i **genitori**:

- l'opportunità di trascorrere più tempo con i bambini,
- riduzione dell'esposizione di tutta la famiglia alle malattie infettive comuni (influenza, raffreddore, COVID-19),
- la possibilità per i giovani genitori di conciliare efficacemente vita privata e professionale.

Il lavoro a distanza ha anche un forte impatto sulla permanenza delle giovani madri nel mercato del lavoro (ben il 49% delle madri lavoratrici ammette di conoscere almeno una persona che ha lasciato il proprio lavoro o sta pensando di farlo a causa dell'obbligo di tornare in ufficio).

Esempi dei vantaggi dell'utilizzo delle **app per taxi**:

- lavorare per l'uguaglianza di genere (nella maggior parte delle città americane, le donne rappresentano finora meno del 5% dei tassisti, mentre nel caso delle applicazioni di sharing economy sono già circa il 20-30%), lavorare per l'uguaglianza di genere. 20-30%),
- facilitare l'ingresso degli immigrati (ad esempio dall'Ucraina) nel mercato del lavoro,
- offrire corse a prezzi più accessibili: ad esempio, a Los Angeles l'applicazione Uber è disponibile in 21 quartieri a basso reddito, dove offre corse significativamente più economiche rispetto alle compagnie di taxi tradizionali.

1.6 Effetto delle nuove tecnologie sulle relazioni contrattuali: una discussione sugli *smart contracts* e la loro futura applicazione nelle relazioni datore-lavoratore

La digitalizzazione si è ormai diffusa in quasi tutti gli ambiti della nostra vita quotidiana e privata. Ciò vale anche per i rapporti contrattuali precedentemente conclusi verbalmente o per iscritto, che ora vengono spesso rafforzati o integrati con strumenti digitali. Data la grande quantità di informazioni presenti sul web e la crescente conclusione di obbligazioni reciproche con un elemento digitale, gli strumenti basati sulla blockchain, come i *contratti intelligenti,* avranno sicuramente il maggiore impatto sui rapporti contrattuali nel prossimo futuro.

Che cos'è la blockchain?

La blockchain (*catena di blocchi*) è una tecnologia per il trasferimento e l'archiviazione di informazioni sulle transazioni effettuate su Internet. Le singole informazioni sono organizzate in blocchi successivi di dati. Una volta che un blocco è saturo di un certo numero di transazioni, le informazioni sulle transazioni vengono memorizzate nel blocco successivo. Grazie al riferimento al blocco precedente e al concatenamento delle informazioni in essi contenute, diventa impossibile modificare o cancellare la registrazione di una transazione

senza che tale modifica venga registrata in tutti gli altri blocchi. Questa soluzione favorisce la trasparenza delle transazioni effettuate e contrasta la manipolazione fraudolenta delle informazioni.

Cosa sono i *contratti intelligenti*?

Uno smart contract è un programma "autoesecutivo" basato sulla logica *if-then (se...allora)*. È scritto interamente in un linguaggio di programmazione e può essere eseguito utilizzando la tecnologia DLT (distributed ledger technology, tecnologia del registro diffuso) o la blockchain. In quest'ultimo caso, il programma è memorizzato sulla blockchain e viene eseguito quando determinate condizioni innescano un'altra azione - ad esempio, può attivare un pagamento o fornire un determinato servizio. Si tratta quindi di una **fusione tra la realtà creata da un determinato contratto e il mondo reale attraverso la tecnologia.** Ciò rende il contratto più trasparente e affidabile, fornendo alle parti la fiducia nell'esecuzione dei suoi termini quando si verifica una determinata situazione.

Esempi di utilizzo dei contratti intelligenti:

- Acquisto di un immobile - grazie agli smart contract, il processo, solitamente molto complesso e che richiede il coinvolgimento di numerosi intermediari (notaio, agente immobiliare, consulente legale, istituto di credito), viene notevolmente semplificato e non richiede il coinvolgimento dei suddetti attori, rendendo possibile l'acquisizione del titolo di proprietà per via elettronica.
- Acquisti online - in questo caso, i contratti intelligenti garantiscono che il pagamento venga effettuato immediatamente e che quindi il prodotto venga inviato all'acquirente più rapidamente.
- Trattamento dei dati personali - poiché i dati personali e le ID digitali sono memorizzati sulla blockchain, il rischio di furto di identità è notevolmente ridotto.
- Registrazione dei risultati di elezioni o referendum - per ridurre al minimo il rischio di brogli elettorali. L'uso di smart contract a questo scopo può già essere osservato in pratica in Estonia, tra gli altri.
- Pagamento di compensazioni e premi - liquidazione automatica dei sinistri, calcolo dei premi.

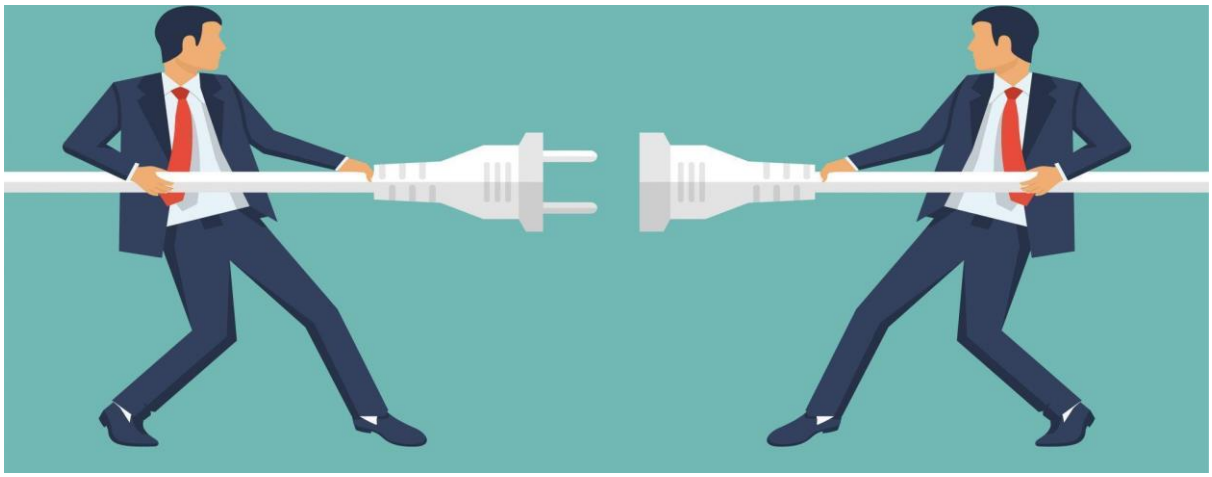
2. Effetti della digitalizzazione sulla vita privata dei lavoratori

2.1 Protezione del tempo di lavoro dei lavoratori nel lavoro a distanza. Lavoro a distanza e work-life balance

Secondo una ricerca di Eurofound, un terzo dei dipendenti dell'Unione Europea ha iniziato a lavorare da casa durante la pandemia e come risultato del passaggio al lavoro a distanza, fino al 27% ha dichiarato di svolgere le proprie mansioni lavorative nel tempo libero. Durante il lock-down, il confine tra vita privata e professionale ha iniziato a sfumare. I dipendenti hanno acquisito la capacità di organizzare il proprio tempo, ma sono stati anche esposti al rischio di essere sempre reperibili e di non potersi staccare completamente dai media elettronici al di fuori dell'orario di lavoro.

È importante notare che nella modalità basata sulle mansioni (non basata su orari di lavoro rigidi) si applicano le stesse regole del sistema tradizionale, ovvero il dipendente deve svolgere le proprie mansioni per 8 ore al giorno nell'arco di una settimana lavorativa di cinque giorni. I compiti svolti al di fuori di questo quadro dovrebbero essere considerati come straordinari. Tuttavia, sebbene l'orario di lavoro flessibile sia indubbiamente vantaggioso per i dipendenti, questi ultimi spesso credono erroneamente che, non essendo in ufficio a orari fissi, debbano dimostrare di essere disponibili in ogni momento della giornata.

2.1.1. Diritto alla disconnessione



Fonte: Shutterstock.

Come sancito dall'articolo 24 della Dichiarazione universale dei diritti dell'uomo, ogni individuo ha diritto al riposo e allo svago, compresa una ragionevole limitazione dell'orario di lavoro e ferie periodiche retribuite. Inoltre, secondo l'articolo 31 della Carta dei diritti fondamentali, ogni lavoratore ha diritto a condizioni di lavoro che rispettino la sua salute, la sua sicurezza e la sua dignità e ha diritto a periodi di riposo giornaliero e settimanale, a ferie annuali retribuite e, soprattutto, alla limitazione dell'orario di lavoro massimo.

La nuova realtà post-pandemica, in cui il confine tra vita privata e professionale è spesso labile, ha evidenziato la necessità di implementare una normativa che dia ai dipendenti la sicurezza di disconnettersi dal lavoro e di non rispondere alle e-mail dei superiori dopo l'orario di lavoro senza conseguenze negative. Per questo motivo, nel 2021, il Parlamento europeo ha adottato una risoluzione a favore del diritto alla disconnessione, invitando la Commissione europea a studiare l'elaborazione di una direttiva sul diritto a essere *offline*.

Vale la pena notare che le risoluzioni del Parlamento europeo non hanno carattere vincolante. Pertanto, la Commissione europea non è obbligata ad agire per l'attuazione della direttiva proposta dal Parlamento. Tuttavia, data la sostanza della questione, si può prevedere che la Commissione cercherà di regolamentare il diritto allo scollegarsi e di garantire un livello di protezione uniforme per i lavoratori in tutta l'Unione europea.

Come proposto dal Parlamento europeo, la direttiva sul diritto alla disconnessione intende garantire:

1) regole minime che garantiscano ai dipendenti che utilizzano mezzi di comunicazione a distanza nel loro lavoro quotidiano il diritto di essere *offline*,
2) Il divieto di discriminazione o di trattamento meno favorevole dei dipendenti (compresa la risoluzione dei contratti di lavoro) che esercitano il diritto alla disconnessione,
3) la parità di trattamento di tutti i dipendenti, sia del settore pubblico che di quello privato, dei dipendenti di livello inferiore o dei dirigenti (anche se in quest'ultimo caso può essere difficile, a causa delle normative specifiche per i dirigenti),
4) una procedura giudiziaria efficiente e la possibilità di chiedere riparazione per le violazioni dei diritti concessi (accesso alla protezione giudiziaria dalle ripercussioni).

Obblighi dei datori di lavoro in relazione al diritto dei dipendenti di essere *offline*

I nuovi diritti dei dipendenti comportano anche ulteriori obblighi da parte dei datori di lavoro. Tra questi, la necessità di dotarsi di un sistema interno che consenta di misurare con precisione l'orario di lavoro giornaliero del dipendente (nel rispetto del diritto alla privacy e alla protezione dei dati personali). Inoltre, è importante sostenere i dipendenti nell'essere

offline - comunicando chiaramente la nuova legge nelle politiche aziendali, conducendo campagne di formazione e informazione in questo settore.

Tuttavia, in termini di sensibilizzazione, l'obbligo di informare per iscritto ciascun dipendente dei propri diritti sembra il più rilevante e promettente.

Inoltre i datori di lavoro dovrebbero evitare di promuovere una cultura di disponibilità continua e di premiare i dipendenti che non esercitano il diritto alla disconnessione. Anche la valutazione della salute e della sicurezza in relazione al diritto alla disconnessione (ad esempio in termini di rischi psicosociali) dovrebbe essere una considerazione importante.

2.1.2. Equilibrio tra la vita privata e professionale: il ruolo dello Stato

Fonte: Technology Headlines.

Lo Stato e le sue politiche del lavoro hanno un ruolo importante nel plasmare il rapporto tra lavoratore e datore di lavoro. In termini di equilibrio tra lavoro e vita privata, alcuni Paesi stanno adottando iniziative per promuovere buone prassi occupazionali. Da un lato ciò riguarda l'attuazione delle normative nazionali, dall'altro, gli strumenti legislativi che non hanno forza vincolante ma cercano di dare forma a determinati comportamenti.

Tali misure "soft" potrebbero consistere, ad esempio, nell'attuazione di codici di buona condotta o nel dare il buon esempio agli altri datori di lavoro promuovendo un approccio favorevole ai lavoratori all'interno delle strutture governative. Questa strada è stata scelta da Malta, che nel 2020 ha pubblicato un *Manuale sulle misure volte all'equilibrio tra lavoro e vita privata*. Questa pubblicazione raccoglie e descrive in dettaglio i diritti dei dipendenti,

con istruzioni su come lavorare correttamente nell'era della digitalizzazione (ad esempio, come organizzare il proprio lavoro quando si svolgono mansioni a distanza). Tuttavia l'utilità del manuale non sta solo nella sua capacità di far conoscere meglio le prerogative dei dipendenti o nel campo della digitalizzazione. Tali codici di buone prassi, applicabili sul posto di lavoro (o in un determinato settore), possono anche essere una sorta di merce di scambio nelle trattative con il datore di lavoro.

Nel caso del manuale maltese, i promotori del progetto hanno dichiarato che il loro obiettivo principale era quello di garantire un equilibrio tra lavoro e vita privata per gli impiegati del settore pubblico, sensibilizzando i dipendenti. Vale la pena notare, tuttavia, che il manuale non amplia in alcun modo il catalogo dei diritti dei lavoratori, ma si limita a richiamare l'attenzione sulle corrette pratiche di impiego e a sensibilizzare i lavoratori sulla possibilità di negoziare le condizioni di lavoro in linea con le disposizioni del documento.

Esempi di promozione del diritto alla disconnessione nei paesi dell'UE

Sebbene al momento non esista ancora un quadro giuridico paneuropeo che disciplini il diritto alla disconnessione, esistono già alcuni esempi di azione legislativa in questo ambito nell'UE. A ciò si aggiunge la promozione del diritto alla disconnessione attraverso i contratti collettivi di lavoro. Inoltre, alcuni Stati membri hanno già attuato una legislazione proprioa sul diritto alla disconnessione.

Francia

La Francia è considerata un pioniere del diritto alla disconnessione. Già nel 2013 è stato adottato un accordo intersettoriale sulla qualità della vita sul lavoro, che incoraggiava le aziende a non interferire con la vita privata dei dipendenti e definiva il momento in cui i dispositivi di contatto dei dipendenti dovevano essere spenti. Queste disposizioni sono state successivamente promulgate l'8 agosto 2016 e incorporate nel Codice del lavoro francese. Inoltre, da gennaio 2017, in Francia i datori di lavoro sono tenuti a negoziare accordi con i sindacati sul diritto alla disconnessione.

Italia

La Francia è stata seguita dall'Italia, che ha deciso di introdurre il diritto alla disconnessione nel 2017. La normativa si concentra sulle persone che svolgono un lavoro a distanza (*smart working*, *lavoro agile*) e stabilisce che i lavoratori a distanza hanno il diritto di disconnettersi dai dispositivi tecnologici e dalle piattaforme online senza subire alcuna

conseguenza da parte dei loro datori di lavoro. Anche in Italia esistono contratti collettivi settoriali e aziendali che prevedono il diritto alla disconnessione.

Spagna

Un altro paese che ha adottato il diritto alla disconnessione nella legislazione nazionale è la Spagna. Nel 2018, con il recepimento del GDPR nella legislazione spagnola, è stato introdotto un nuovo pacchetto di diritti digitali. Con esso, ai dipendenti che lavorano sia nel settore privato che in quello pubblico è stato riconosciuto il diritto alla disconnessione, con l'obiettivo di mantenere un equilibrio tra lavoro e vita privata. Secondo il regolamento, i datori di lavoro, dopo aver ascoltato i rappresentanti dei lavoratori, devono stabilire politiche interne su come i dipendenti possono esercitare il loro diritto alla disconnessione e fornire formazione ai dipendenti sull'uso corretto delle nuove tecnologie.

Belgio

In Belgio, nel 2018, tutti i datori di lavoro con più di 50 dipendenti sono stati obbligati a discutere l'uso sicuro degli strumenti digitali e il diritto dei dipendenti alla disconnessione con il comitato per la salute e la sicurezza. Vale la pena notare che, con l'introduzione del diritto alla disconnessione, i dipendenti stessi non hanno acquisito nuovi poteri, ma solo maggiori opportunità di negoziazione con il datore di lavoro. Tuttavia, nel 2022 è stato adottato un nuovo regolamento che consente ai dipendenti pubblici di spegnere le e-mail di lavoro e di non rispondere a messaggi di testo e telefonate al di fuori dell'orario di lavoro senza temere ripercussioni. Sono in discussione anche piani per estendere le nuove norme ai dipendenti del settore privato.

Irlanda

Nell'aprile 2021, il governo irlandese ha promulgato un codice di condotta in base al quale tutti i dipendenti hanno il diritto di disconnettersi e di non rispondere immediatamente a e-mail, telefonate o altri messaggi provenienti dal proprio datore di lavoro dopo l'orario di lavoro. Il codice stabilisce inoltre che un dipendente, di regola generale, non deve essere costretto a lavorare al di fuori del suo orario di servizio standard e non deve subire conseguenze per aver rifiutato di occuparsi di questioni aziendali dopo l'orario di lavoro.

2.1.3 Esigenza della reperibilità continua da parte del datore di lavoro e mobbing

Fonte: jobs.ca.

Il mobbing è un'azione o un comportamento nei confronti di un dipendente che consiste in molestie o intimidazioni persistenti e prolungate. Si verifica quando le azioni in questione hanno lo scopo di umiliare o ridicolizzare il dipendente, ma anche quando mirano a indurlo a sottovalutare la propria idoneità professionale.

Poiché il mobbing può assumere diverse forme di aggressione, il catalogo dei comportamenti che si qualificano come questo tipo di violenza rimane aperto. Pretendere che un dipendente sia sempre disponibile sotto la minaccia di conseguenze negative può quindi essere considerato mobbing. Lo dimostrano, ad esempio, le sentenze in cui i tribunali hanno dato ragione ai dipendenti che sostenevano che la ricezione opprimente e ripetuta di messaggi contenenti istruzioni di lavoro dopo l'orario di lavoro o nei giorni di riposo dovrebbe essere considerato come mobbing.

Sentenza del Tribunale regionale di Lublino del 20 giugno 2018. (VIII Pa 86/18)

Un tribunale ha riconosciuto a una dipendente di un ufficio comunale un risarcimento di 25.000 zloty dal suo datore di lavoro per i danni alla salute causati dall'invio invadente di e-mail dopo l'orario di lavoro. Il caso riguardava una donna impiegata come dipendente pubblico a tempo pieno e indeterminato. Dopo il cambio di sindaco nel comune, il nuovo supervisore ha adottato l'invio di istruzioni ai dipendenti sotto forma di e-mail ai loro indirizzi di lavoro e privati come metodo principale di comunicazione con loro. Dal 1° gennaio 2015, la ricorrente aveva ricevuto circa 200 e-mail dal sindaco, di cui più di 100 sono state inviate dopo l'orario di lavoro, anche di notte e nei giorni festivi, durante le ferie annuali o i congedi per malattia. Il procedimento è sfociato in una sentenza del Tribunale regionale di Lublino, in cui la Corte ha ritenuto che incaricare un dipendente di compiti e inviare e-mail con ordini

di lavoro in giorni non lavorativi, durante le assenze per malattia e ferie, e chiedergli di render conto in modo inadeguato delle sue prestazioni, possa essere considerato **mobbing.**

Violazione del diritto alla disconnessione - implicazioni per il datore di lavoro e meccanismi di reclamo

Le sanzioni per le violazioni del diritto alla disconnessione possono variare da un paese all'altro dell'UE. Ciò è dovuto al fatto che ogni Stato membro deve determinare individualmente il livello di sanzione imposto a un datore di lavoro per il mancato rispetto del tempo libero dei propri dipendenti.

In Polonia non è ancora stato introdotto un diritto separato del dipendente alla disconnessione, ma può essere dedotto dalle norme generali sull'orario di lavoro e dalla giurisprudenza dei tribunali. È quindi generalmente accettato che un dipendente non sia obbligato a rispondere al telefono o alle e-mail dopo l'orario di lavoro o durante le vacanze. Fa eccezione il caso in cui sia richiesto di essere reperibile, cioè di essere pronto a lavorare al di fuori dell'orario di lavoro.

I comportamenti scorretti più comuni da parte dei datori di lavoro in merito al rapporto di lavoro sono le irregolarità relative alla risoluzione dei contratti, le violazioni delle norme sull'orario di lavoro, il pagamento improprio dei salari e la concessione impropria di congedi. In Polonia a seconda dell'entità e del tipo di infrazione, il datore di lavoro può incorrere in una multa che va da 1.000 a 30.000 zloty. Pertanto, si può prevedere che in Polonia il mancato rispetto del diritto alla disconnessione sarà sanzionato come qualsiasi altra violazione delle norme sull'orario di lavoro, ossia il datore di lavoro dovrà pagare una multa fino a 30.000 zloty. Inoltre, in caso di trattamento inferiore di un dipendente a causa della sua limitata disponibilità al di fuori dell'orario di lavoro designato, possono sorgere problemi di risarcimento per discriminazione (per un importo non inferiore al salario minimo applicabile).

Secondo un sondaggio d'opinione[7] , il 23,9% dei dipendenti in Polonia riceve e-mail, sms o altri messaggi dai superiori dopo l'orario di lavoro. Sebbene, come sottolineano gli esperti, ciò non sia vietato, tale azione può essere considerata come un'istruzione a lavorare oltre l'orario di lavoro (soprattutto quando il contatto obbliga il dipendente a eseguire un particolare compito). Se è necessario rispondere a un'e-mail o a una telefonata per questioni di lavoro, ai sensi degli articoli 151 (1) e 151 (2) del Codice del lavoro, tale azione deve essere compensata con una retribuzione aggiuntiva o con permessi.

[7] Sondaggio condotto da UCE RESEARCH e da ePsycholodzy.it, https://uce-pl.com/news/blisko-24-proc-polakow-twierdzi-ze-pracodawca-kontaktuje-sie-z-nimi-w-czasie-wolnym-od-pracy

Cosa deve fare un dipendente polacco i cui diritti sono stati violati?

a) Colloquio con il datore di lavoro

Prima di decidere di denunciare una violazione alle autorità esterne, è consigliabile che il dipendente cerchi di comunicare con il datore di lavoro. È importante che il direttore o il proprietario dell'azienda sia coinvolto nella conversazione, poiché può accadere che i dirigenti non siano a conoscenza di illeciti commessi da supervisori che agiscono a un livello inferiore.

b) Cercare il sostegno dei sindacati

Se il dialogo con il datore di lavoro non funziona, il dipendente può chiedere il sostegno del sindacato, se presente sul posto di lavoro. Il sindacato ha il compito di rappresentare i dipendenti e dovrebbe rinnovare il tentativo di raggiungere un accordo con il direttore/proprietario dell'azienda o con la sua direzione.

c) Notifica delle violazioni all'Ispettorato statale del lavoro (PIP)

L'Ispettorato statale del lavoro (PIP) è l'istituzione più importante che si occupa di condizioni di lavoro e diritti dei lavoratori in Polonia. È ad esso che devono essere presentate, in prima istanza, le denunce formali di violazione dei diritti del lavoro. I contatti con il PIP sono disponibili all'indirizzo www.pip.gov.pl e le denunce possono essere presentate per iscritto, per telegrafo, fax, e-mail, tramite il modulo di denuncia elettronica o oralmente. I dati del dipendente che presenta il reclamo possono rimanere anonimi. Secondo la legge

sull'ispettorato del lavoro[8] , l'ispettore del lavoro è tenuto a non rivelare che un'ispezione è stata effettuata a seguito di un reclamo, a meno che il denunciante non acconsenta per iscritto. Tuttavia è importante ricordarsi di motivare adeguatamente le accuse mosse e di fornire prove solide, poiché sarà il PIP a decidere se la denuncia è credibile e se sarà verificata.

d) Portare il caso davanti al tribunale distrettuale

Il materiale presentato al PIP può anche costituire una prova nel caso in cui il caso venga sottoposto al tribunale distrettuale. Il ricorso al tribunale è tuttavia l'ultima risorsa, utilizzata solo quando le vie precedenti hanno fallito.

Nell'ordinamento italiano la disconnessione è uno dei contenuti necessari dell'accordo individuale di lavoro agile, che deve indicare in questo senso «le misure tecniche e organizzative necessarie per assicurare la disconnessione del lavoratore dalle strumentazioni tecnologiche di lavoro» (art. 19, c. 1, l. n. 81/2017).

Inoltre, al fine di tutelare i tempi di riposo e la salute, l'articolo 2, comma 1 *ter* del decreto legge n. 30 del 2021 convertito nella legge n. 61 del 2021 configura la disconnessione dalle strumentazioni tecnologiche e dalle piattaforme informatiche come diritto del lavoratore agile, il cui esercizio «non può avere ripercussioni sul rapporto di lavoro o sui trattamenti retributivi».

Per quanto riguarda la contrattazione collettiva del settore privato, l'articolo 3, comma 2 del Protocollo nazionale sul lavoro in modalità agile prevede l'individuazione per via negoziale di una «fascia di disconnessione nella quale il lavoratore non eroga la prestazione lavorativa».

In caso di violazione da parte del datore di lavoro degli articoli richiamati, oltre alla richiesta di assistenza (legale) all'organizzazione sindacale cui conferisce mandato, il lavoratore agile può adire il giudice del lavoro oppure ricorrere alle sedi extragiudiziali di risoluzione delle controversie stabilite dalla contrattazione collettiva.

[8] Articolo 44, paragrafo 3, della *legge del 13 aprile 2007 sull'Ispettorato statale del lavoro* (Gazzetta ufficiale 2017, voce 786 e successive modifiche).

2.1.4. Work-life balance: cos'è l'equilibrio tra la vita privata e quella lavorativa?

Fonte: zapier.com.

Secondo il rapporto dell'OCSE *How's Life? Measuring Well-being*, il concetto di *work-life balance* si riferisce al mantenimento di un equilibrio tra lavoro (sia retribuito che non), vita familiare e tempo libero. Si riferisce alla capacità di un dipendente di organizzare le proprie responsabilità in modo tale da non interferire con il proprio tempo libero. Tuttavia, il giusto equilibrio tra le diverse aree della vita non dipende solo dal dipendente, ma anche dal datore di lavoro. È il datore di lavoro che di solito crea la cultura del lavoro in azienda e impone determinate norme.

Il rispetto del tempo libero dei dipendenti, siano essi fissi, remoti o ibridi, è di grande importanza.

Dopo tutto, il benessere di ogni dipendente (benessere; stato mentale) dipende da un buon equilibrio tra lavoro e vita privata. Secondo le ricerche, il sovraccarico e il lavoro continuo (compresi i lavori domestici e di assistenza alla persona) possono portare all'esaurimento e a problemi di salute, allo stress cronico e alla riduzione della produttività.

Prima della pandemia, il tempo dedicato al tempo libero e alla cura del proprio benessere da chi lavorava a tempo pieno variava da circa 14 a 16,5 ore al giorno. Gli uomini che lavorano a tempo pieno impiegavano 30 minuti in meno in tempo libero rispetto alle donne. Tuttavia, le statistiche sono diverse per il lavoro a distanza, che si è diffuso durante il blocco causato dalla pandemia COVID-19. Il tempo trascorso davanti al computer è aumentato in modo significativo (fino a due ore in più al giorno) e la qualità del riposo è diminuita. I lavoratori che svolgono le loro mansioni da casa sono più propensi ad accettare di fare gli straordinari e di svolgere le mansioni la sera o nei fine settimana, rendendo così meno netta la linea di demarcazione tra vita privata e professionale.

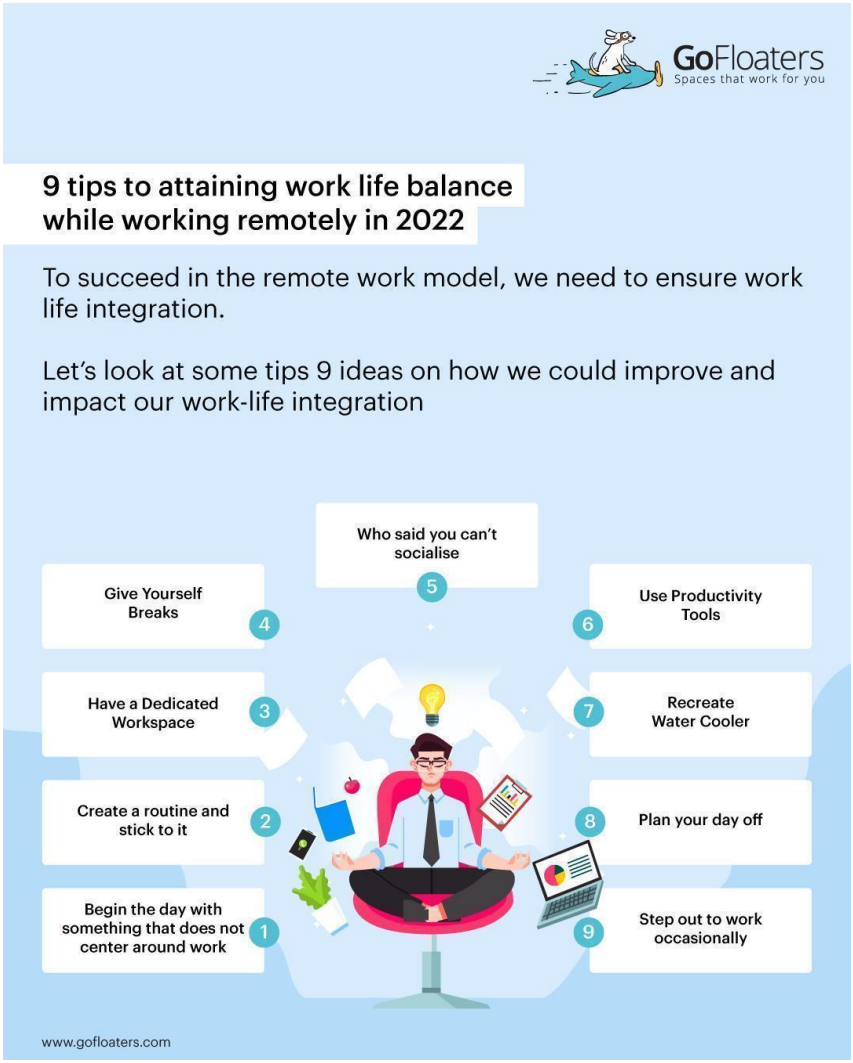
Eppure mantenere questo equilibrio è estremamente importante. Evita il *burnout* professionale, promuove una maggiore motivazione dei dipendenti e il loro impegno nei confronti dell'azienda. Contribuisce inoltre allo sviluppo personale e a una maggiore apertura a nuove sfide. In questo modo, nonostante il minor numero di ore lavorate, aumenta la produttività del personale e si riduce la necessità di cure mediche e di assenze per malattia.

Come possono i datori di lavoro migliorare l'*equilibrio tra lavoro e vita privata dei* loro dipendenti?

L'equilibrio tra lavoro e vita privata dei dipendenti dipende non di rado dai datori di lavoro e dai dirigenti. Sono loro che promuovono comportamenti specifici e a definire le politiche sul posto di lavoro. È quindi importante che sostengano le buone abitudini che consentono ai dipendenti di prendersi una pausa dalle responsabilità lavorative quotidiane. Ad esempio, i datori di lavoro possono incoraggiare i loro dipendenti a fare delle pause sul lavoro, a lavorare in orari flessibili e comodi per loro, a **esercitare il** loro diritto alla disconnessione, a comunicare chiaramente le loro esigenze (ad esempio, comunicando che sono sovraccarichi di responsabilità e hanno bisogno di rallentare).

È inoltre importante promuovere una cultura del lavoro sana, evitando il bonus di essere sempre disponibili o introducendo una politica di non rispondere a e-mail e messaggi dopo l'orario di lavoro. È anche una buona idea fornire ai dipendenti una formazione sull'*equilibrio tra lavoro e vita privata* e sul diritto alla disconnessione, e dare loro consigli su come ridurre facilmente l'uso eccessivo degli strumenti digitali.

2.1.5. Sicurezza e igiene sul posto di lavoro digitale, ovvero come limitare la reperibilità continua in modo autonomo



Suggerimenti per i dipendenti

1. **Disattivare le notifiche sul telefono**

Se il vostro telefono privato è dotato di messaggistica istantanea e di applicazioni utilizzate al lavoro o la casella di posta elettronica del lavoro è collegata a quella privata, disattivate tutte le notifiche che potrebbero disturbarvi durante il tempo libero. Può anche essere una buona idea impostare dei limiti di tempo per disattivare i messaggi dopo l'orario di lavoro standard.

2. **Utilizzare un computer aziendale durante il lavoro e un computer privato dopo l'orario di lavoro.**

Scegliere un computer aziendale piuttosto che un dispositivo privato per il lavoro è preferibile non solo per questioni di sicurezza informatica, ma anche per la possibilità di limitare l'esposizione ai messaggi e alle comunicazioni ricevute dai colleghi dopo l'orario di lavoro. Se la vostra azienda ha una politica BYOD (*bring your own device*), potete creare due account (professionale e privato) sul vostro dispositivo e passare da uno all'altro a seconda del momento della giornata e delle vostre esigenze.

3. Mattina e sera analogiche

Le radiazioni di un telefono o di un computer portatile sono simili alla luce del sole e riducono la secrezione di melatonina nel cervello. Ciò rende più difficile addormentarsi, riduce la qualità del riposo e porta a ulteriori problemi di sonno. Per il vostro benessere, cercate di non utilizzare il telefono e il computer portatile almeno un'ora prima di andare a letto. Inoltre, non iniziate la mattina controllando nervosamente la casella di posta elettronica o i social media.

4. Indicare l'arco di tempo in cui si utilizzano gli strumenti digitali

Anche se lavorate con orari flessibili, informate i vostri supervisori e le persone con cui lavorate sugli orari ai quali potete essere contattati e quando la vostra disponibilità è limitata.

5. Introdurre un giorno intero di *digital detox*

Anche se la disintossicazione digitale non è un principio centrale dell'idea di *equilibrio tra lavoro e vita privata*, staccare completamente la spina dal web e dai social media per un periodo di tempo prolungato può avere enormi benefici per il benessere di un individuo. L'esperienza di staccare la spina dall'elettronica ci rende più consapevoli di quanto tempo effettivamente trascorriamo online. Ci aiuta a stabilire dei confini sani tra lavoro e vita privata. Inoltre, ci motiva a eliminare le cattive abitudini, come controllare compulsivamente la casella di posta elettronica o prendere il telefono appena svegli. Per questo motivo, si consiglia di attuare una disintossicazione ciclica (ad esempio, staccando completamente la spina nei fine settimana) e di dedicare il tempo libero al relax, agli incontri con la famiglia e gli amici o all'attività fisica piuttosto che alla navigazione sui social media.

2.2 Mercificazione obbligatoria e facoltativa delle risorse private

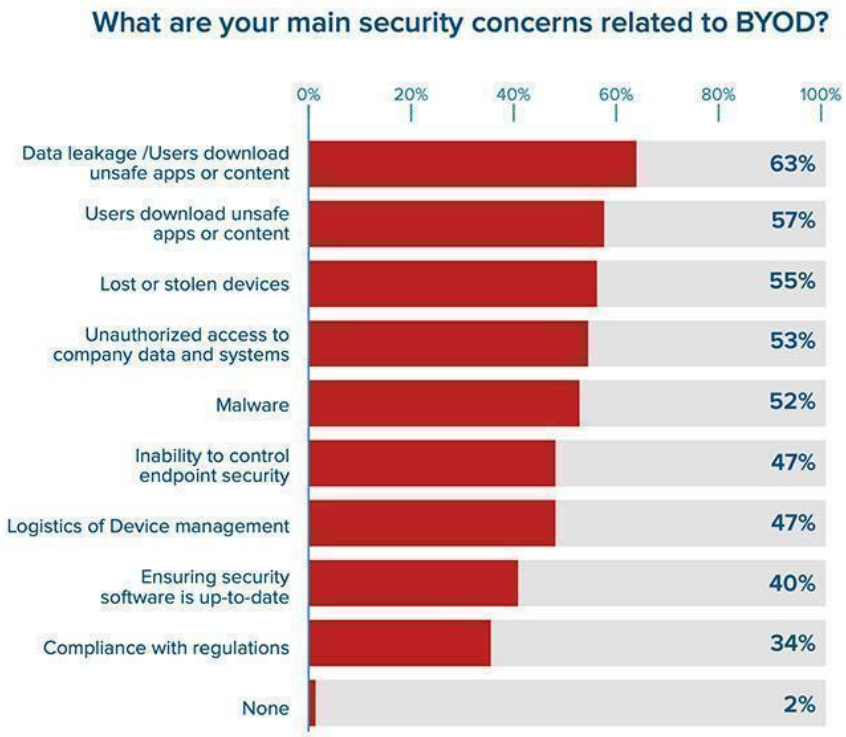
2.2.1. Che cos'è la politica BYOD (bring your own device)?

L'espressione *"bring your own device"* è nota anche con l'acronimo BYOD. Si tratta della tendenza a utilizzare dispositivi privati come laptop, smartphone o tablet per le mansioni lavorative. Questa tendenza è spesso il risultato della volontà dei dipendenti stessi (mercificazione volontaria di risorse private). Talvolta, tuttavia, le politiche BYOD sono preferite anche dai datori di lavoro (mercificazione forzata di risorse private). Sebbene questa tendenza presenti molti vantaggi, prima di implementarla in un'azienda è necessario considerare i rischi potenziali, come i problemi di sicurezza e di privacy.

Vale la pena di ricordare che il BYOD è l'esatto contrario dello stile di lavoro tradizionale, definito *"here's your own device"* (HYOD), in cui le aziende forniscono ai propri dipendenti i dispositivi elettronici di cui hanno bisogno per lavorare.

Vantaggi di una politica BYOD:

- **Flessibilità** - Il BYOD prevede che il datore di lavoro accetti di accedere ai documenti aziendali sui dispositivi privati del dipendente. In questo modo, lo svolgimento delle mansioni professionali diventa possibile ovunque e in qualsiasi momento. Inoltre, una maggiore flessibilità si manifesta nella possibilità di testare nuove soluzioni, software e strumenti digitali, poiché i dipendenti non sono limitati a utilizzare un solo tipo o marca di dispositivo.
- **Comfort**: uno dei vantaggi di una politica BYOD è che i dipendenti possono utilizzare dispositivi che conoscono bene e con cui si sentono a proprio agio.
- **Aumento della produttività** - l'uso del proprio computer portatile o smartphone può facilitare il processo di inserimento dei nuovi assunti, oltre ad aumentare la produttività dei dipendenti fissi.
- **Riduzione dei costi (vantaggio per il datore di lavoro)**: accettando una politica BYOD, i datori di lavoro spesso si sottraggono all'obbligo di fornire al dipendente le attrezzature di lavoro, evitando così costi aggiuntivi.
- **Decentramento dei dati (vantaggio per il datore di lavoro)**: tenere i documenti aziendali su un computer portatile privato (purché ben protetto) può essere vantaggioso per l'azienda grazie al maggior livello di decentramento dei dati. In caso di fuga di dati o di attacco malware al sistema aziendale, i file sui dispositivi dei dipendenti non saranno intercettati insieme al database centrale dell'azienda.



Fonte: helpnetsecurity.com, L'*adozione del BYOD sta crescendo rapidamente, ma la sicurezza è in ritardo*, https://www.helpnetsecurity.com/2020/07/09/byod-adoption-is-growing-rapidly-but-security-is-lagging/.

Svantaggi delle politiche BYOD:

- **Cyber(in)security** - oltre al vantaggio della decentralizzazione dei dati, i problemi di cyber security sono il più grande svantaggio delle politiche BYOD. Quando utilizzano dispositivi privati, i dipendenti tendono a conservare documenti riservati sulle loro unità, che tendono a essere meno sicure di quelle aziendali. Inoltre, quando lavorano in remoto da luoghi pubblici (ad esempio bar, biblioteche, mezzi di trasporto), spesso si collegano alla rete di qualcun altro, aumentando così la probabilità che i computer vengano
  violati e che vengano installati malware. Inoltre, c'è il rischio che il dispositivo di un dipendente venga rubato o perso.
- **Incompatibilità** - la flessibilità nella scelta degli strumenti di lavoro può tradursi in problemi di compatibilità con i sistemi utilizzati di default in azienda. Così, nel caso del BYOD, possono sorgere problemi dovuti all'incompatibilità dei formati e alla difficoltà di utilizzo dei documenti aziendali (ad esempio, a causa del diverso salvataggio dei file nel caso di Windows rispetto a macOS).
- **Recupero dei dati** - Le politiche BYOD possono causare problemi di recupero dei dati memorizzati sul dispositivo di un dipendente al termine del rapporto di lavoro.

Questo perché i dipendenti hanno il pieno controllo dei loro dispositivi e possono smaltire autonomamente i file in essi memorizzati.

Diritti e obblighi BYOD

Se il lavoro viene svolto su attrezzature di proprietà privata, è necessario che queste soddisfino i requisiti di salute e sicurezza. Tuttavia, l'assicurazione di tali attrezzature non è obbligatoria: il dipendente e il datore di lavoro possono concordare la portata dell'assicurazione e le regole per l'utilizzo da parte del dipendente delle attrezzature necessarie per il lavoro e di sua proprietà.

Esempio della Polonia - Modifica del Codice del lavoro e nuove norme sul lavoro a distanza

Vale la pena notare che un dipendente con un contratto di lavoro ha il diritto di richiedere un computer aziendale e il datore di lavoro è obbligato a fornirglielo. Tuttavia, se per lo svolgimento del lavoro si utilizzano apparecchiature private, il dipendente ha diritto a un'indennità in denaro. Inoltre, il datore di lavoro deve coprire i costi dell'elettricità e dei servizi di telecomunicazione necessari per il lavoro a distanza. Il rimborso può essere in valore reale o sotto forma di somma forfettaria concordata tra le parti. Nel determinare l'importo dell'indennità e della somma forfettaria, il datore di lavoro deve tenere conto dei prezzi dei materiali e delle attrezzature, nonché dell'elettricità e dei servizi di telecomunicazione[9] .

A condizione che il lavoro venga svolto a domicilio, il datore di lavoro deve adempiere agli obblighi di salute e sicurezza nei confronti del lavoratore, ad eccezione di:

- dovere di curare le condizioni di sicurezza e igiene dei locali di lavoro,
- obblighi relativi alla costruzione o alla modifica dell'edificio in cui si trovano i locali di lavoro,
- obbligo di fornire strutture igieniche e sanitarie adeguate.

Tali obblighi del datore di lavoro di fornire condizioni di lavoro adeguate ai propri dipendenti hanno anche un impatto sulle questioni relative alla portata del termine "infortunio sul lavoro" e alla sicurezza sociale. Un lavoratore che subisce un infortunio sul lavoro, a prescindere dal luogo in cui svolge le proprie mansioni - a distanza o sul posto di lavoro - ha diritto alle **prestazioni di sicurezza sociale.**

[9] *Legge del 1° dicembre 2022 che modifica il Codice del lavoro e alcune altre leggi* (GU del 2022, voce 240).

Prima di essere autorizzato a lavorare a distanza, il dipendente conferma in una dichiarazione (presentata in forma cartacea o elettronica) di aver letto la valutazione dei rischi e le informazioni del datore di lavoro contenenti i principi del lavoro a distanza sano e sicuro e si impegna a rispettarli.

La valutazione dei rischi professionali deve tenere in particolare considerazione gli effetti del lavoro a distanza sulla vista e sull'apparato muscolo-scheletrico del lavoratore. Vengono prese in considerazione anche le condizioni psicosociali del lavoro in questione. Sulla base dei risultati della valutazione, il datore di lavoro elabora informazioni contenenti principi e modalità di organizzazione adeguata del luogo di lavoro a distanza. Questi devono tenere conto dei requisiti di ergonomia, dell'esecuzione sicura e igienica del lavoro a distanza, delle attività da svolgere al termine del lavoro a distanza, nonché delle regole per affrontare le situazioni di emergenza che rappresentano un rischio per la vita o la salute umana. Il datore di lavoro può anche redigere una valutazione universale dei rischi per gruppi specifici di posizioni di lavoro a distanza.

Il caso dell'Italia

Per quanto concerne l'ordinamento italiano, si rinvia alla lettura del paragrafo «Telelavoro/lavoro agile in Italia» (pp. 27 – 28).

2.3 Tutela dei dati personali e sicurezza delle persone che lavorano on-line

2.3.1. Lavoro a distanza

A causa della crescente popolarità del lavoro a distanza ibrido o a tempo pieno, i legislatori di molti Stati membri hanno deciso di modificare di conseguenza il proprio diritto del lavoro. In particolare, è stato necessario adattare gli obblighi del lavoratore e del datore di lavoro alle nuove forme di lavoro. Questi obblighi derivano dalla necessità di garantire che l'infrastruttura informatica o lo spazio di lavoro presso il sito di lavoro remoto siano adeguati a soddisfare i requisiti di salute e sicurezza.

Lavoro a distanza e diritto del lavoro: l'esempio della Polonia

1. **Strumenti per il lavoro a distanza**

Secondo la proposta di modifica del Codice del lavoro, articolo 67 (24) § 1, il datore di lavoro è obbligato a fornire il lavoro a distanza al dipendente:

- **Materiali e strumenti di lavoro** - comprende l'attrezzatura tecnica necessaria per il lavoro a distanza (a seconda delle specificità del lavoro, a parte il computer, si possono includere i seguenti elementi ad esempio, cuffie adatte per le riunioni online, microfono, ecc.)
- **Installazione, assistenza e manutenzione degli strumenti di lavoro**, comprese le attrezzature tecniche, necessarie per il lavoro a distanza. In alternativa, il datore di lavoro può anche coprire i costi necessari per questi servizi.
- **Formazione e assistenza tecnica** necessarie per svolgere il lavoro a distanza.
- **Copertura dei costi dell'elettricità** - il datore di lavoro è tenuto a coprire anche i costi dell'energia e dei servizi di telecomunicazione necessari per il lavoro a distanza.

Un accordo tra il datore di lavoro e l'organizzazione sindacale aziendale o il regolamento del lavoro può obbligare il datore di lavoro a coprire altri costi direttamente connessi all'esecuzione del lavoro a distanza.

Per quanto concerne l'ordinamento italiano, si rinvia alla lettura del paragrafo «Telelavoro/lavoro agile in Italia» (pp. 27 – 28).

2. Disposizione dello spazio nel lavoro a distanza - controllo del datore di lavoro

Il dipendente è tenuto a organizzare la propria postazione di lavoro a distanza tenendo conto dei requisiti ergonomici. Ciò include, tra l'altro, la scelta di una sedia comoda, una scrivania di altezza adeguata, il posizionamento corretto del monitor rispetto agli occhi e un'illuminazione adeguata.

A condizione che il lavoro venga svolto presso il domicilio del lavoratore, il datore di lavoro deve adempiere ai doveri di salute e sicurezza nei confronti del lavoratore, ad eccezione di:

- dovere di curare le condizioni di sicurezza e igiene dei locali di lavoro,
- obbligo di cui al capitolo III della sezione 10 del Codice del lavoro (norme sulle strutture edilizie e sui locali di lavoro),
- obbligo di fornire strutture igieniche e sanitarie adeguate.

Tali obblighi del datore di lavoro di fornire condizioni di lavoro adeguate ai propri dipendenti hanno anche un impatto sulle questioni relative alla portata del termine

"infortunio sul lavoro" e all'assicurazione sociale. Un dipendente che subisce un infortunio sul lavoro, indipendentemente dal luogo in cui svolge le proprie mansioni (a distanza o sul posto di lavoro), ha diritto alle **prestazioni di sicurezza sociale.**

Visti gli obblighi del datore di lavoro in materia di:

- applicazione di misure adeguate per prevenire gli infortuni nel lavoro a distanza,
- adozione le misure necessarie per eliminare o ridurre il rischio che si verifichi tale incidente,
- prestazione di primo soccorso alle persone infortunate e le circostanze e le cause dell'infortunio in conformità all'accordo stipulato con l'organizzazione sindacale dell'azienda o nei regolamenti;

i**l datore di lavoro ha il diritto di effettuare un'ispezione per quanto riguarda**:

- salute e sicurezza sul lavoro,
- **rispetto della sicurezza e della protezione delle informazioni**, comprese le procedure per la protezione dei dati personali.

Secondo le nuove norme del Codice del Lavoro, un datore di lavoro potrà introdurre controlli di sobrietà per i dipendenti solo se ciò è necessario per garantire la protezione della vita e della salute dei dipendenti, di altre persone o la protezione dei beni.

Ogni controllo di sobrietà dovrebbe essere:

- effettuato in consultazione con il dipendente,
- svolto presso la sede di lavoro remota e durante l'orario di lavoro del dipendente,
- adattato al luogo e al tipo di lavoro a distanza,
- di non ostacolo all'uso dei locali domestici in modo coerente con la loro destinazione d'uso,
- in caso di lavoro occasionale a distanza, i controlli di sobrietà devono essere effettuati su base concordata con il dipendente,
- nel rispetto della privacy del dipendente e degli altri (ad esempio, altri membri della famiglia o inquilini).

Se durante un'ispezione il datore di lavoro riscontra carenze in materia di salute e sicurezza, e sicurezza e protezione delle informazioni, compresa la protezione dei dati, ha due possibilità. Può dare al dipendente un termine per correggere le carenze o ritirare il consenso a svolgere il lavoro a distanza.

Per quanto concerne l'ordinamento italiano, si rinvia alla lettura del paragrafo «Telelavoro/lavoro agile in Italia» (pp. 27 - 28).

3. Protezione dei dati personali nel lavoro a distanza secondo le modifiche al Codice del Lavoro

Dato l'aumento del rischio di fuga di dati personali e di altre violazioni in questo settore, il datore di lavoro deve stabilire delle procedure per la protezione dei dati personali. All'interno dell'organizzazione dovrà essere fornita una formazione adeguata. Un dipendente che svolge un lavoro a distanza, d'altra parte, dovrebbe confermare di aver familiarizzato con gli standard stabiliti dal datore di lavoro in forma scritta o elettronica.

Sia il dipendente che il datore di lavoro devono anche stabilire come e con quali strumenti comunicheranno a distanza e trasmetteranno le informazioni relative allo svolgimento del lavoro.

In Italia, ferma restando la distinzione tra telelavoro e lavoro agile, per quanto concerne la protezione dei dati rileva in via generale l'articolo 115, comma 1 del decreto legislativo n. 196 del 2003 (c.d. Codice *privacy*) secondo cui «il datore di lavoro è tenuto a garantire al lavoratore il rispetto della sua personalità e della sua libertà morale».

Quanto alla *privacy* nel telelavoro, si fa riferimento all'articolo 4 dell'accordo interconfederale 9 giugno 2004 che da un lato rimette al datore «la responsabilità di adottare misure […] atte a garantire la protezione dei dati utilizzati ed elaborati […] per fini professionali» (c. 1) e di «informare il telelavoratore in ordine a tutte le norme di legge e regole aziendali applicabili» (c. 2) e, dall'altro, grava il lavoratore di un obbligo di cooperazione configurabile «nel rispetto di tali norme e regole» (c. 3).

Con riguardo alla *privacy* nel lavoro agile, il Protocollo nazionale sul lavoro in modalità agile del 7 dicembre 2021 ha il merito di guardare alla figura del lavoratore agile non soltanto dalla prospettiva di persona autorizzata a trattare dati ai fini professionali sotto l'autorità del datore di lavoro – titolare, ma anche dall'angolo visuale di soggetto interessato dal trattamento.

In particolare, ferma restando l'osservanza della normativa sul trattamento dei dati personali, il datore di lavoro deve (art. 12, cc. 2 – 5, Protocollo): a) adottare tutte le misure tecnico – organizzative adeguate a garantire la protezione dei dati personali dei lavoratori agili e delle informazioni trattate da quest'ultimi; b) informare il lavoratore agile in merito ai trattamenti che lo riguardano fornendogli, tra l'altro, le istruzioni e l'indicazione delle misure di sicurezza da osservare per garantire la protezione, segretezza e riservatezza delle informazioni trattate ai fini professionali; c) aggiornare il registro delle attività di trattamento connesse allo svolgimento della prestazione lavorativa in modalità agile; d) verificare la conformità degli strumenti utilizzati dal lavoratore agile alla legislazione in materia di *privacy*, a cui si aggiunge l'onere di effettuare preventivamente la valutazione d'impatto dei trattamenti ai sensi dell'articolo 35 del regolamento europeo n. 679/2016 (*GDPR*); e) promuovere l'adozione di regolamenti aziendali sulla gestione delle violazioni dei dati personali (cc.dd. *data breach*) e sull'implementazione di misure di sicurezza (es. crittografia); f) favorire il coinvolgimento dei lavoratori in attività formative su utilizzo, custodia e protezione degli strumenti di lavoro nonché sulle cautele da adottare.

A fronte degli obblighi datoriali, il lavoratore agile da una parte è chiamato ad individuare – fatto salvo quanto stabilito dalla contrattazione collettiva sull'inidoneità di determinati luoghi – sedi d'adempimento dell'attività esterna ai locali aziendali «tali da consentire […] condizioni di sicurezza e riservatezza» (art. 4, c. 1) nonché a conformarsi «alle istruzioni fornite dal datore di lavoro» (art. 12, c. 1) e, dall'altra, ha «diritto alla formazione c.d. obbligatoria in materia di tutela della salute […] e di protezione dei dati» (art. 13, c. 5).

2.3.2. Come applicare il GDPR per la difesa dei dati personali nel caso del lavoro a distanza?

L'aumento della popolarità del lavoro a distanza ha aumentato il rischio di fuga di informazioni aziendali sensibili. Questo perché può essere difficile, sia per il dipendente che per il datore di lavoro, stabilire con esattezza in quali condizioni siano state violate le norme sulla protezione delle informazioni, sulla sicurezza e sulla protezione dei dati. Dato che il lavoro a distanza (almeno in parte) è destinato a rimanere tra noi per molto tempo, è necessario ricordare le norme sulla protezione dei dati più frequentemente violate. Vale anche la pena di esaminare i rischi in agguato per chi lavora a distanza e come mitigare il rischio che si verifichino.

RICORDA!

Ai sensi dell'articolo 32 del Regolamento GDPR, il datore di lavoro, in qualità di responsabile del trattamento dei vostri dati personali, deve mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza appropriato al grado di rischio di violazione dei diritti o delle libertà delle persone fisiche di varia probabilità e gravità.

A tal fine, il datore di lavoro può intraprendere le seguenti azioni:

(a) pseudonimizzare e crittografare i dati personali,

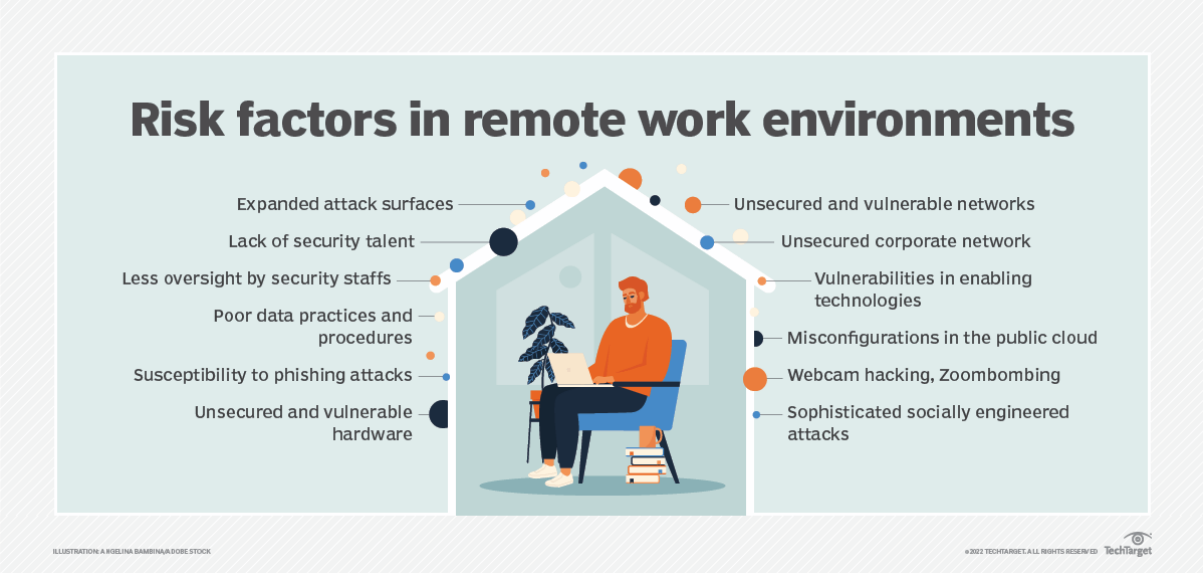
(b) garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di elaborazione dati,

(c) garantire che la disponibilità e l'accesso ai dati personali possano essere ripristinati rapidamente in caso di incidente fisico o tecnico,

(d) garantire che l'efficacia delle misure tecniche e organizzative per garantire la sicurezza del trattamento dei dati personali possa essere testata, misurata e valutata regolarmente.

Come spiegato dalla Commissione europea, i dipendenti che elaborano i dati nell'ambito del loro lavoro all'interno dell'organizzazione svolgono i compiti di un responsabile del trattamento dei dati. In quanto tali, anch'essi hanno la responsabilità di garantire la sicurezza dei dati personali.

2.3.3. Minacce online e lavoro a distanza



Sebbene la sicurezza informatica sia una delle sfide più importanti che le istituzioni statali si trovino ad affrontare oggi, la consapevolezza del pubblico al riguardo rimane limitata. Quasi tutti hanno sentito parlare di sicurezza informatica e della sua importanza, ma il comportamento dei cittadini non sempre riflette un alto livello di conoscenza dell'argomento. Secondo un sondaggio del sito web polacco ChronPESEL.pl e del Registro nazionale dei debiti condotto nel 2022, un polacco su tre teme la fuga di dati personali, ma meno della metà degli intervistati saprebbe cosa fare in una situazione del genere.

Sebbene sia impossibile garantire la protezione dei dati e la sicurezza delle informazioni al 100%, esistono una serie di misure preventive che possono ridurre adeguatamente il rischio di fuga di dati e altri pericoli.

Le minacce che si nascondono nell'ambiente di lavoro remoto non sono molto diverse da quelle di cui ogni utente di Internet dovrebbe diffidare. Il loro obiettivo è molto spesso quello di rubare informazioni protette o dati relativi a una persona o a un'azienda specifica, consentendo all'aggressore di ottenere un vantaggio finanziario, un vantaggio competitivo o altri scopi. Secondo un rapporto dell'Agenzia dell'Unione europea per la sicurezza informatica (ENISA), le minacce informatiche più comuni e pericolose sono:

1. **Software malevoli** (*malware*) - è un codice o un'applicazione dannosa che ostacola o impedisce completamente il normale utilizzo di un dispositivo finale (ad esempio, un computer o una stampante). Infettando il dispositivo in questione con il malware, i criminali possono ottenere l'accesso ai dati o ad altre funzioni del dispositivo. Possono anche puntare a bloccare completamente il dispositivo, a patto che venga pagato un riscatto dall'utente o da un'altra persona parzialmente colpita dall'attacco.
2. ***Ransomware*** - un tipo di malware con il quale un criminale blocca l'accesso degli utenti ai propri sistemi o ai propri file personali, chiedendo poi un compenso in cambio del loro ripristino.
3. **Attacchi attraverso siti web** - un metodo con cui gli hacker ingannano le vittime dei loro attacchi utilizzando i sistemi e i servizi Internet come canale per preparare e portare a termine un attacco. In particolare, si distingue la fornitura o l'agevolazione di URL o script dannosi per indirizzare l'utente verso un sito web desiderato o scaricare contenuti dannosi. Il risultato è l'attuazione di codice maligno su un vero sito web esistente al fine di rubare informazioni e ottenere vantaggi finanziari.
4. ***Phishing*** **-** come per altri attacchi informatici, l'obiettivo dei criminali informatici è quello di ottenere informazioni preziose, principalmente login, password, codici fiscali o numeri di carte di credito. Il nome deriva dal fatto che i criminali utilizzano un'esca personalizzata per la persona specifica di cui vogliono rubare i dati. A tal fine, di solito utilizzano e-mail o SMS falsi, nonché canali di comunicazione sui social network. Per creare fiducia, i criminali informatici si spacciano per società di

telecomunicazioni, servizi di corriere, banche, siti di aste e persino agenzie governative. Facendo leva sulle emozioni della vittima, cercano di convincerla a cliccare su un link che hanno preparato per raggiungere un sito web che, sebbene simile a quello autentico, è stato creato dal criminale e rappresenta il suo canale per commettere frodi.

5. **DDoS** - (*distributed denial of service*) è un tipo di attacco che prende di mira servizi di rete o sistemi informatici. Il loro compito è quello di sequestrare tutte le risorse disponibili e libere per impedire all'intero servizio di funzionare su Internet. L'attacco può colpire il sito web di un'azienda, la posta elettronica di un dipendente, ecc. Viene effettuato da diversi dispositivi informatici contemporaneamente, soprattutto da quelli su cui è stato preso il controllo tramite virus speciali - bot o trojan. Il pericolo di questo tipo di attacco è che l'utente dell'apparecchiatura in questione possa non rendersi conto che il suo computer viene utilizzato per effettuare un DDoS.
6. **Furto d'identità** - utilizzando il numero codice fiscale, i dati personali o la carta d'identità di una persona, un criminale si spaccia per tale persona al fine di ottenere, ad esempio, un credito o utilizzare in altro modo la sua identità a proprio vantaggio.
7. **Violazione della sicurezza dei dati** - è un tipo di incidente di sicurezza informatica in cui si accede alle informazioni (o a parte di un sistema informativo) senza un'autorizzazione adeguata, di solito con intento malevolo. Ciò comporta la potenziale perdita o l'uso improprio di tali informazioni. Il motivo per cui si verifica questo tipo di minaccia è spesso dovuto al cosiddetto errore umano, che può verificarsi durante la configurazione e l'implementazione di alcuni servizi e sistemi, con conseguente esposizione involontaria dei dati.
8. **Perdita di informazioni**: una conseguenza comune delle violazioni della sicurezza dei dati, che riguarda un'ampia gamma di informazioni a rischio, dalle informazioni di identificazione personale (IIP) ai dati finanziari memorizzati nell'infrastruttura IT, fino ai dati sanitari personali memorizzati negli archivi dei fornitori di servizi sanitari.
9. **Minaccia interna** (abuso di potere) - è un'azione intrapresa da un individuo o da un gruppo di individui legati alla vittima di un attacco da un rapporto professionale o di altro tipo, in cui sia l'aggressore che la vittima si trovano sulla stessa rete o infrastruttura o hanno la possibilità di ottenere informazioni grazie all'interconnessione. Esistono diversi modelli associati a questi tipi di minacce. Possono verificarsi anche quando gli esterni collaborano con gli interni per ottenere un accesso non autorizzato alle risorse. Gli insider possono anche causare danni inavvertitamente per disattenzione o mancanza di conoscenza. Poiché gli insider godono spesso della fiducia dei colleghi e conoscono i processi e le procedure

dell'organizzazione, può essere difficile distinguere tra l'accesso legittimo a dati e sistemi e le azioni in malafede.

10. **Botnet** - una rete di dispositivi interconnessi infettati da malware bot. Sono tipicamente utilizzate per lanciare attacchi DDoS. Le reti bot possono essere controllate da remoto da un criminale per agire in modo sincronizzato e ottenere un risultato specifico.

2.3.4. Igiene informatica: come difendersi in rete ogni giorno?

1. **Se potete, lavorate in uno spazio sicuro e privato.**

La fuga di dati può avvenire non solo in seguito a un attacco di hacking, ma anche attraverso metodi meno sofisticati e convenzionali, come ad esempio uno screen shot (fotografia dello schermo con lo stesso dispositivo). Va da sé che, a parte uno spazio di lavoro predisposto dal datore di lavoro, lo spazio più sicuro per il lavoro a distanza sembra essere il proprio spazio di lavoro domestico. L'ideale sarebbe una stanza chiusa a chiave dove potersi separare tranquillamente dal resto della famiglia.

Se non è possibile lavorare in una stanza isolata (ad esempio, durante un viaggio di lavoro), la questione della sicurezza si complica notevolmente. In particolare, fate attenzione agli spazi aperti (bar, treni, aeroporti) dove le persone intorno a voi sono costantemente nel vostro ambiente e cambiano in continuazione. Inoltre, in molti luoghi di questo tipo sono installate telecamere a circuito chiuso, che possono registrare non solo le azioni di chi si trova nel suo raggio d'azione, ma anche ogni sorta di altro elemento dell'ambiente, compresi gli schermi dei computer.

Soluzione: dotarsi di un filtro/copertura per la privacy

Con questo strumento, il contenuto dello schermo è visibile solo alla persona che utilizza il computer/telefono. La tecnologia funziona in modo simile alle micro-tende: il filtro è costituito da canali microscopici rivolti verso la persona che utilizza lo schermo del monitor. Chi guarda lo schermo da un'angolazione diversa non vedrà lo stesso contenuto.

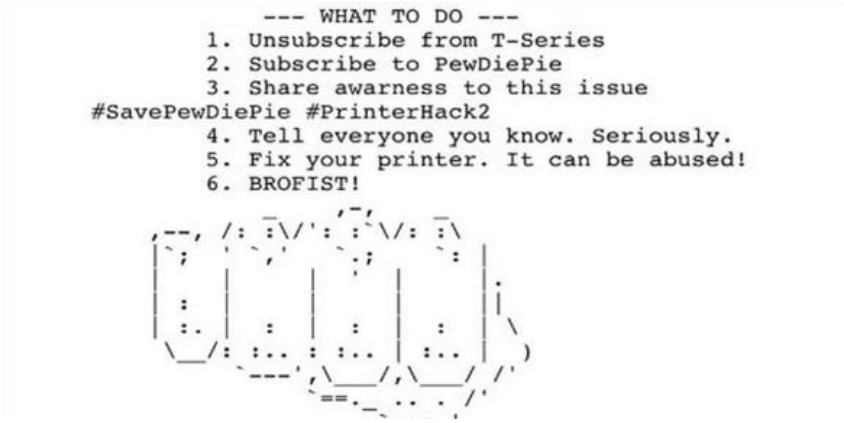
2. **Conservare i documenti in un'area sicura e chiudibile a chiave presso la sede di lavoro remota.**

La cosiddetta politica della scrivania pulita o dello schermo pulito, in vigore in molti luoghi di lavoro, dovrebbe essere applicata anche alla sede di lavoro remota. Anche se abbiamo fiducia nei membri della famiglia o nei coinquilini, nessun documento contenente informazioni personali dovrebbe essere lasciato in nostra assenza. Inoltre, non bisogna tenere in bella vista le password dei dispositivi di lavoro.

Soluzione: attrezzate il vostro spazio di lavoro remoto con un cassetto o un armadietto chiudibile a chiave.

Questo sarà il luogo in cui potrete riporre in modo sicuro tutti i vostri materiali durante il lavoro. Se possibile, tenete la chiave sempre con voi o nascondetela in un posto che conoscete solo voi.

3. **Se non è necessario, non stampate documenti a casa o nei punti di fotocopiatura pubblici.**



Da tempo gli esperti di cybersecurity avvertono che il dispositivo più trascurato in termini di necessità di implementare una sicurezza adeguata è... la stampante. Secondo una ricerca di InfoSecurity Magazine, circa il 66% dei lavoratori remoti intervistati ha stampato una media di cinque documenti a settimana. Un quarto di loro non ha ancora smaltito i documenti stampati, spiegando che intende riportarli in ufficio. Solo il 24% utilizza un distruggidocumenti domestico, ma ammette anche di gettare i documenti nel cestino di casa. Il 12% degli intervistati dichiara inoltre di non essere a conoscenza della normativa GDPR.

Le stampanti di oggi assomigliano sempre di più a computer piuttosto che a semplici dispositivi monouso: spesso fanno parte dell'*Internet delle cose (*IoT) e sono strumenti di lavoro multifunzionali. Uno degli attacchi di più alto profilo alle stampanti domestiche, che

ha messo in luce il problema dell'inadeguatezza della sicurezza di questi dispositivi, è stato quello legato al noto youtuber PewDiePie. Nel 2018, un hacker (o un gruppo di molti fan di PewDiePie) ha attaccato decine di migliaia di stampanti in tutto il mondo. Senza alcuna interferenza da parte dei proprietari, i dispositivi hanno iniziato a stampare una brochure che promuoveva i contenuti pubblicati da PewDiePie e a incoraggiare il sostegno alle sue attività.

Le stampanti odierne, sempre più sofisticate, dispongono di una *cache* in cui i documenti vengono stampati. Le stampanti moderne funzionano anche in modalità wireless, il che significa che chiunque abbia i driver giusti sul proprio computer e l'accesso alla rete in cui si trova la stampante può collegarsi ad essa.

Se un hacker prende il controllo della stampante (ad esempio in un'azienda), può accedere sia ai documenti già stampati sia ad altre risorse memorizzate sul computer o persino alle password dei dispositivi che hanno utilizzato i servizi della stampante.

Soluzione: stampate i documenti solo sul posto di lavoro e, se dovete farlo a casa, assicuratevi che le vostre apparecchiature siano protette adeguatamente.

A tal fine è possibile impostare una password sicura per il wi-fi della stampante (se possibile). Se i documenti stampati non vi servono più, non gettateli nel cestino di casa, ma portateli in azienda dove dovrebbe esserci un distruggidocumenti. Se questo non è possibile, chiedete al vostro datore di lavoro o all'ufficio risorse umane quali sono le procedure di distruzione dei documenti dell'azienda.

4. Sovrapposizione della webcam

Lavorare da casa significa di solito partecipare a teleconferenze e videochiamate che richiedono l'uso di una webcam. Purtroppo, gli hacker possono facilmente accedere alla vostra webcam, compromettendo la vostra privacy. Inoltre, se sul posto di lavoro fisico sono presenti documenti riservati che possono essere catturati da una webcam, i criminali potranno accedervi.

Soluzione: limitare la visualizzazione agli elementi contenenti dati personali

Quando la webcam è accesa, la possibilità di visualizzare oggetti contenenti informazioni personali nelle vicinanze deve essere limitata. Inoltre, se la webcam è separata dal dispositivo, deve essere scollegata quando non viene utilizzata. Se la webcam è incorporata, è opportuno adottare ulteriori misure di protezione, come ad esempio un cappuccio per la

fotocamera. Nei negozi si trovano facilmente copri webcam scorrevoli di vari tipi. Di solito sono facili da installare, in quanto la maggior parte di esse è dotata di uno strato adesivo che aderisce alla telecamera. Utilizzando software e applicazioni per videoconferenze, è possibile utilizzare anche funzioni come la **sfocatura dello sfondo**.

5. **Partecipare attivamente alla formazione aziendale sulla sicurezza informatica e alle modifiche della politica del datore di lavoro in materia di protezione dei dati e delle informazioni.**

Secondo il GDPR, se vengono emanate nuove procedure di protezione dei dati in azienda, il datore di lavoro deve consentire ai propri dipendenti di familiarizzare con esse prima di applicarle.

Se il datore di lavoro non ha fornito una formazione adeguata sull'uso dei dispositivi, sull'uso degli strumenti di comunicazione interna ed esterna o sui principi di base relativi alla protezione dei dati in azienda, il dipendente ha il diritto di chiedergliela. Se, anche dopo la formazione, il dipendente non è ancora sicuro delle procedure da seguire in una determinata situazione, deve segnalarlo al proprio datore di lavoro o alla persona designata all'interno dell'azienda responsabile della gestione informatica, del reparto risorse umane, ecc.

Igiene informatica quando si lavora da remoto

Cos'altro potete fare per proteggere il vostro computer?

Crittografia dei dati personali

Soprattutto se si tratta di dati sensibili o se li inviate all'esterno dell'organizzazione. Come già detto, i dipendenti che trattano i dati nell'ambito delle loro mansioni lavorative svolgono quindi i compiti del responsabile del trattamento dei dati, che è il datore di lavoro. In conformità con l'articolo 32 del GDPR, il responsabile del trattamento e l'incaricato del trattamento devono mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza dei dati appropriato all'ambito, al contesto e alle finalità del trattamento e al rischio di interferenza con i diritti o le libertà delle persone fisiche. Il regolamento GDPR cita tra le misure di sicurezza la pseudonimizzazione e la cifratura dei dati personali.

Sebbene il GDPR non contenga requisiti espliciti sul metodo di sicurezza più efficace, il regolamento sottolinea ripetutamente che la **crittografia e la pseudonimizzazione** sono misure tecniche e organizzative adeguate per mantenere la sicurezza dei dati personali.

La crittografia mira a codificare un determinato contenuto in modo tale che possa essere compreso solo da un destinatario in possesso della chiave giusta. In termini più semplici, l'idea è, ad esempio, quella di trasformare una stringa di lettere in una stringa di altre lettere o numeri, di aggiungere altre stringhe di lettere o numeri e così via.

La pseudonimizzazione, invece, è il trattamento dei dati personali in modo tale che non sia possibile identificarne l'identità senza accedere alle informazioni, conservate in modo sicuro altrove. Si tratta quindi di mascherare i dati sostituendo le informazioni su una persona con identificatori immaginari.

Qual è la differenza tra i due metodi?

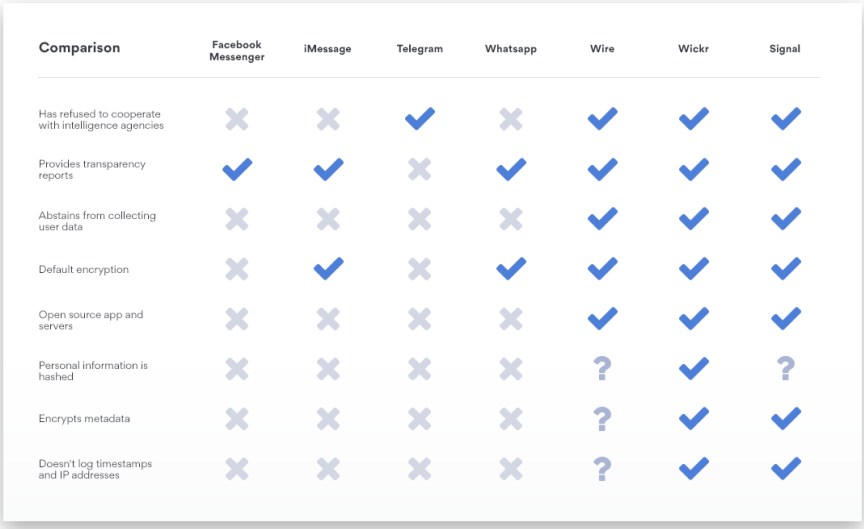
Come la pseudonimizzazione, la crittografia nasconde le informazioni sostituendo gli identificatori con qualcos'altro. Tuttavia, mentre la pseudonimizzazione consente a chiunque abbia accesso ai dati di vedere una parte del dataset, la crittografia permette solo agli utenti autorizzati di accedere all'intero dataset. La pseudonimizzazione e la crittografia possono essere utilizzate contemporaneamente o separatamente.

Metodi per proteggere/criptare i dati nelle comunicazioni interne e con l'esterno.

a. Comunicazione interna: utilizzo di messaggistica criptata e piattaforme sicure.

Sebbene l'e-mail rimanga ancora uno dei metodi di comunicazione aziendale più diffusi (316,9 miliardi di e-mail inviate e ricevute ogni giorno nel 2021 e si prevede che questo numero salirà a 376,4 miliardi entro il 2025), non è nemmeno il sistema più sicuro per lo scambio di informazioni riservate. A causa della sua elevata popolarità, l'e-mail è anche un importante canale per gli attacchi di hacking. Deloitte ha rilevato che il 91% di tutti gli attacchi informatici proviene da e-mail *di phishing*. Il costo di un attacco di questo tipo per le organizzazioni può essere molto elevato.

Per le comunicazioni interne, dove spesso vengono scambiate informazioni riservate sull'azienda, sui dipendenti o sui clienti, si possono utilizzare altri strumenti più sicuri.



Comparison	Facebook Messenger	iMessage	Telegram	Whatsapp	Wire	Wickr	Signal
Has refused to cooperate with intelligence agencies	✗	✗	✓	✗	✓	✓	✓
Provides transparency reports	✓	✓	✗	✓	✓	✓	✓
Abstains from collecting user data	✗	✗	✗	✗	✓	✓	✓
Default encryption	✗	✓	✗	✓	✓	✓	✓
Open source app and servers	✗	✗	✗	✗	✓	✓	✓
Personal information is hashed	✗	✗	✗	✗	?	✓	?
Encrypts metadata	✗	✗	✗	✗	?	✓	✓
Doesn't log timestamps and IP addresses	✗	✗	✗	✗	?	✓	✓

Whatsapp e Messenger: i messenger più popolari e le loro caratteristiche

1. **WhatsApp:**
   - utilizza la crittografia Signal,
   - la maggior parte delle persone in Europa probabilmente utilizzerà questa applicazione,
   - un'applicazione di facile utilizzo che offre funzionalità aggiuntive,
   - è di proprietà di Facebook,
   - in precedenza si sono verificate gravi violazioni della protezione dei dati nell'applicazione.
2. **Messenger:**
   - ampia portata - grazie al collegamento con Facebook, la maggior parte delle persone possiede questo programma di messaggistica,
   - può essere utilizzato anche dopo la disattivazione dell'account Facebook,
   - la crittografia non è quella predefinita,
   - il comunicatore non cripta le conversazioni passate,
   - l'applicazione tiene traccia del comportamento dell'utente.

Le migliori applicazioni in termini di sicurezza dei dati:

1. **Signal:**

- supporta chat di gruppo, SMS, messaggistica vocale e video e consente il trasferimento di documenti e foto,
- offre messaggi che scompaiono (con un timer),
- utilizza un protocollo di segnalazione - un protocollo crittografico non federato che può essere utilizzato per crittografare chiamate vocali e conversazioni di messaggistica istantanea, dove i messaggi in chiaro possono essere letti solo dai comunicanti,
- software *open source* (cioè il cui codice sorgente è reso disponibile gratuitamente e può essere distribuito e modificato senza alcun pagamento),
- non memorizza dati o metadati dell'utente,
- promosso da Edward Snowden,
- richiede un numero di telefono per la registrazione.

Piattaforme software e workspace sicure:

1. Microsoft Teams.
2. Google Workspace.
3. Slack.
4. Asana.
5. Trello.

b. Comunicazione esterna - crittografia di file contenenti dati personali ed elenchi di destinatari di posta elettronica

Si raccomanda che, ogni volta che i dati vengono trasferiti da una sede a un'altra, siano pseudonimizzati o criptati per proteggersi da eventuali fughe di notizie.

Conferimento dei dati personali nella mailing list

Utilizzare il campo UDW (hidden to message, BCC). Il campo UDW consente di inviare i messaggi in modo che i destinatari non vedano gli indirizzi degli altri. Questa opzione si trova in ogni e-mail.

Trasmissione di dati personali in file inviati per posta elettronica

Nei documenti inviati via e-mail possono essere nascosti molti dati personali o altre informazioni protette dalla legge, per cui è necessario proteggerli ulteriormente. I metodi di

crittografia dei file possono variare a seconda del formato in cui sono archiviati. Tuttavia, tutti hanno un principio di base in comune: trasmettere la password del documento crittografato attraverso un mezzo di comunicazione diverso dalla posta elettronica.

Per criptare correttamente un file, i programmi più comunemente scelti sono **WinRAR** e **7-zip**. Con ciascuno di essi, dopo aver selezionato l'opzione "aggiungi all'archivio", si apre una finestra che consente, tra l'altro, di impostare una password per accedere al documento.

Eseguite regolarmente il backup dei vostri dati e memorizzateli su unità esterne.

Nel caso in cui l'hardware venga infettato da un virus o da altri eventi che possono portare alla cancellazione dei dati dal computer e all'impossibilità di ripristinarli, la soluzione migliore è quella di effettuare regolarmente dei backup.

I backup, noti anche come copie di sicurezza, sono copie di informazioni che vengono archiviate in un luogo diverso dall'originale. Il primo passo da fare è decidere se si vuole fare un backup:

1. Dati specifici che sono importanti per qualche motivo.
2. L'intero sistema operativo.

La maggior parte degli strumenti di backup sono configurati di default per il primo scopo e copiano i dati in base ai documenti utilizzati più spesso. Se non si è sicuri di quali file copiare, si consiglia di archiviarli tutti.

Con quale frequenza effettuare i backup?

La risposta dipende dalle preferenze individuali e dalla frequenza dei cambi. Alcuni lo fanno ogni ora, altri una volta al giorno e altri ancora una volta alla settimana. Tuttavia, è consigliabile eseguire il backup dei documenti quotidianamente.

Come faccio a fare il backup dei miei documenti?

A seconda del sistema operativo del computer, esistono programmi consigliati che consentono di impostare un periodo ogni volta che viene eseguito automaticamente un backup. Tra questi vi sono Microsoft Windows Backup and Restore o Time Machine di Apple. Questi programmi funzionano sia quando il dispositivo è in uso sia quando è inattivo.

Dati su supporti esterni o dati nel cloud?

Preferibilmente entrambi. I supporti di memorizzazione esterni possono essere, tra l'altro, una chiavetta di memoria, un'unità esterna portatile o altri dispositivi a cui ci si può collegare tramite wi-fi. Il vantaggio di questi dispositivi è sicuramente quello di poter archiviare grandi quantità di dati in un periodo di tempo piuttosto breve. Purtroppo, trattandosi di un metodo di backup fisico, può subire gli stessi guasti o danni di un computer. Un backup su supporti esterni può essere rubato, perso, allagato, surriscaldato e così via. Inoltre, se il dispositivo da cui provengono i dati è stato precedentemente infettato da malware, c'è purtroppo il rischio che anche il supporto, e di conseguenza il backup stesso, venga infettato.

Il backup in cloud, invece, consiste nel collocare copie di documenti o altri file su Internet. Più precisamente, si tratta di collezioni di server e centri dati dispersi a livello globale in cui vengono archiviati i dati. Ciò avviene automaticamente, di solito tramite uno strumento predefinito di una piattaforma di elaborazione testi (ad esempio Google Docs), che crea un backup ogni periodo di tempo stabilito o dopo ogni modifica di un file. Un indubbio vantaggio dell'archiviazione di copie di file nel cloud è la loro permanenza e la possibilità di accedere al backup da qualsiasi altro dispositivo (a condizione, ovviamente, che si disponga della password dell'account all'interno del quale si trova il cloud). Tuttavia questa soluzione non è del tutto priva di inconvenienti: se si desidera eseguire rapidamente il backup di una grande quantità di dati, la soluzione può essere molto più lenta di un backup fisico su un'unità esterna. Inoltre, è possibile che il cloud esaurisca lo spazio per archiviare i nuovi dati e che si debba eliminare parte di essi o acquistare risorse aggiuntive dal provider cloud.

Accesso sicuro al computer, al telefono e persino alle riunioni online

Così come la crittografia dei dati stessi è necessaria per garantire la sicurezza dei dati personali, è estremamente importante che anche le apparecchiature che utilizziamo siano adeguatamente protette. L'uso di password o di altri tipi di crittografia garantisce che solo le persone autorizzate abbiano accesso a determinate risorse.

Esistono diversi metodi per fissare le apparecchiature:

- **Una password forte, cioè:**
    - **lunga** - contenente almeno otto caratteri (più lungo è, meglio è),
    - **complessa -** contenente almeno un carattere di ogni categoria: lettere maiuscole, lettere minuscole, caratteri speciali (ad es. !, ?), numeri,
    - **difficile da indovinare** - se volete scegliere una frase, una citazione o un modo di dire, assicuratevi che non sia direttamente collegata a voi, al

vostro lavoro o al vostro ambiente; tuttavia, se sapete che non ricorderete la password senza facili associazioni - sostituite le parole con simboli o numeri appropriati della tastiera, ad esempio "Ala ha un gatto" **può essere** scritto come "4Lah@1g@tT0",

- **diversa dalla password precedente per il dispositivo in questione** - se si cambia la password per un account esistente, non deve essere uguale a quella precedente; né si deve cambiare la password solo leggermente aggiungendo, ad esempio, una cifra alla fine o all'inizio.

Suggerimento: utilizzate uno strumento di gestione delle password per memorizzare le password crittografate online - vi permetterà di creare password complesse contenenti lettere maiuscole e minuscole, numeri, vari caratteri speciali ecc. In questo modo si creerà una stringa di caratteri senza senso che sarà difficile da decifrare.

RICORDATE!

- non utilizzate una password che sia anche un nome o che sia simile a un nome utente, al nome di una società, ecc..,
- non utilizzate una sequenza di lettere o numeri della tastiera o dell'alfabeto,
- non utilizzate più di due lettere o numeri ripetutamente (ad esempio, abba),
- non utilizzate i dati personali di nessuno per creare una password,
- non utilizzate versioni di parole scritte al contrario (ad esempio, janek1 come 1kenaj),
- non inserite la password in presenza di altre persone,
- non scrivete la vostra password su carta - se dovete scriverla, utilizzate uno strumento di gestione delle password su una chiavetta USB e portatelo con voi
- non utilizzate la stessa password per tutti i dispositivi o siti,
- non accedete a un dispositivo non vostro,
- non inviate la password via e-mail,
- non condividete le password online - se dovete condividere le informazioni di accesso con un collega, chiamatelo per comunicargli i dettagli e non inviategli la password via e-mail, SMS o altri messaggi,
- se il vostro computer/sito è stato violato, cambiate immediatamente la password.

Antipattern - un elenco delle password meno sicure[10] :

1. password
2. 123456
3. 123456789
4. ospite
5. qwerty
6. 12345678
7. 111111
8. 12345
9. col123456
10. 123123
11. 1234567
12. 1234
13. 1234567890
14. 000000
15. 555555
16. 666666
17. 123321
18. 654321
19. 7777777
20. 123

Autenticazione multicomponente

L'autenticazione a più fattori (MFA o 2FA) è un metodo di sicurezza che richiede l'uso di almeno due componenti indipendenti per autenticare un'azione (ad esempio, l'inserimento

[10] Secondo uno studio di NordPass, Top 200 delle password più comuni, https://nordpass.com/most-common-passwords-list/

della password di un account e la successiva immissione di un codice SMS). Questo metodo impedisce la maggior parte degli attacchi basati sulle credenziali di identità.

Molte applicazioni o piattaforme offrono già la possibilità di abilitare questo tipo di sicurezza (ad esempio Apple ID, Microsoft, Google, Twitter o Facebook). Il secondo componente di autenticazione può essere un codice SMS, un codice una tantum da un'applicazione (Google Authenticator o Microsoft Authenticator) o un codice permanente proposto dal fornitore dello strumento in questione e scelto dall'utente.

Chiavi U2F

Secondo gli esperti di sicurezza informatica, la chiave U2F è l'unico metodo di autenticazione in due fasi che protegge al 100% dagli attacchi *di phishing (*ma non da altri attacchi, come il *malware*). Infatti, se una persona in possesso della chiave U2F viene ingannata dai criminali informatici e inserisce login e password su un sito web falso, l'aggressore non riuscirà a impossessarsi dei dati dell'account dell'utente.

Ciò è dovuto a un *elemento sicuro* (un cosiddetto piccolo computer) integrato nella chiave U2F. Funziona in modo tale che, quando la chiavetta viene inserita in una porta USB (o quando viene avvicinata a un lettore su uno smartphone), questa si avvia e può eseguire operazioni crittografiche sul suo sistema interno anziché sul dispositivo dell'utente.

Inoltre, è bene procurarsi due chiavette: anche se la stessa può essere collegata a diversi servizi, vale la pena averne una di riserva. Una volta acquistata, la chiave deve essere configurata. Molti servizi offrono la possibilità di aggiungere una chiave come forma di autenticazione multilivello. Anche diversi social media, Amazon, GitHub o account di posta elettronica raccomandano questa soluzione. Se si decide di utilizzare la chiave U2F, gli altri metodi di autenticazione a due livelli devono essere rimossi dal servizio in questione.

Protezione delle riunioni online

Non è solo l'hardware a dover essere protetto, ma anche le riunioni in rete e le videoconferenze. Lavorare in remoto significa spesso affidarsi a un software di videoconferenza, che a sua volta crea potenziali rischi per la sicurezza del dispositivo. A seguito di una serie di attacchi alla piattaforma Zoom, in cui persone non invitate si sono introdotte nelle videoconferenze per intimidire o molestare i partecipanti (*zoom bombing*), l'azienda è stata costretta a correggere le falle di sicurezza. Nonostante il nome, lo *zoom bombing* può verificarsi anche su altre piattaforme. Questo tipo di attacco può provocare la fuga di informazioni riservate sull'azienda, sui clienti, sugli altri dipendenti o sull'utente stesso.

In risposta agli attentati di Zoom, l'FBI ha pubblicato dei consigli per aiutare gli utenti a proteggersi quando utilizzano un software di videoconferenza:

1. Verificare che la riunione sia privata, richiedendo una password per partecipare alla riunione o controllando l'accesso degli ospiti dalla sala d'attesa.
2. Considerare i requisiti di sicurezza nella scelta dei fornitori. La crittografia *end-to-end* (che nasconde il messaggio al mittente e lo decifra solo al destinatario) garantisce privacy e sicurezza, quindi verificate se il software di videoconferenza che state utilizzando è dotato di questa funzione.
3. Assicuratevi che il vostro software sia aggiornato installando le patch e gli aggiornamenti più recenti.

La piattaforma più sicura per le videoconferenze è attualmente Microsoft Teams. La perfetta integrazione di tutte le applicazioni di Office consente anche ulteriori impostazioni di sicurezza, in modo che tutti i membri dell'organizzazione possano lavorare insieme rimanendo al sicuro anche nell'ufficio di casa.

Installare e tenere aggiornato il software antivirus e la protezione contro il malware.

L'aggiornamento di sistemi, applicazioni e browser viene spesso trascurato e rimandato a un secondo momento. In realtà, farlo al momento giusto può prevenire gran parte degli attacchi. Assicuratevi quindi di utilizzare un software antivirus aggiornato e moderno. Gli aggiornamenti contengono importanti modifiche che migliorano le prestazioni e la sicurezza dei dispositivi. Oggi gli aggiornamenti vengono rilasciati addirittura mensilmente, ma vale la pena attivare la modalità di backup giornaliero. Questo aumenta significativamente la

sicurezza, in quanto gli sviluppatori possono applicare rapidamente le patch alle vulnerabilità di sicurezza individuate, proteggendo ulteriormente i dispositivi dalle minacce informatiche.

Un semplice passo da compiere è anche quello di assicurarsi che il software di protezione da *malware* sia installato e utilizzato in aggiunta al software antivirus standard. Questo strumento può non solo fornire una protezione contro gli attacchi, ma anche avvisare l'utente quando viene tentato un attacco.

Evitate di collegare i vostri dispositivi a reti pubbliche

L'utilizzo di una rete pubblica, cioè una rete a cui chiunque può connettersi, per il fatto stesso di essere completamente aperta può essere un canale per numerosi attacchi e comporta il rischio di perdita di dati. Se dovete lavorare in uno spazio pubblico, assicuratevi di collegarvi solo a reti fidate e sempre con una VPN o una connessione dal vostro telefono (tramite un cosiddetto hotspot).

Che cos'è una VPN?

Si tratta di reti private virtuali che forniscono connessioni sicure e dirette alla rete informatica di un'organizzazione. Possono essere essenziali quando si accede a file, si lavora con informazioni riservate o per l'utilizzo di determinati siti web.

La VPN cripta le connessioni degli utenti ai suoi server, consentendo un accesso sicuro alla rete dell'organizzazione. Un tunnel VPN aziendale crittografato contribuisce inoltre a garantire la sicurezza dei dati trasmessi. Inoltre, impedirà agli aggressori che non dispongono di una VPN aziendale, di accedere ai server.

La sicurezza delle VPN può essere migliorata utilizzando un metodo di autenticazione solido. Molte VPN utilizzano un nome utente e una password, ma si può anche pensare all'aggiornamento e all'utilizzo di *smart card per* proteggere il processo di login degli utenti e controllare meglio l'accesso agli account.

Naturalmente, non importa quanto sia forte la VPN. Se la password viene violata, gli hacker saranno in grado di accedervi facilmente. È quindi opportuno aggiornarla regolarmente. È una buona idea limitare l'uso di una VPN alle sole situazioni in cui è necessario. Se i dispositivi aziendali per uso personale vengono utilizzati la sera o nei fine settimana (se ciò è in linea con la politica aziendale), è meglio spegnere la VPN.

Quali altre opzioni oltre alla VPN?

Un'altra opzione è quella di utilizzare una rete 5G. Offre una migliore connettività e promette una maggiore sicurezza rispetto all'utilizzo di connessioni wi-fi o addirittura VPN. L'annunciata minore latenza del 5G potrebbe renderlo una valida alternativa al wi-fi. La

tecnologia è dotata di crittografia incorporata attraverso strumenti che impediscono il tracciamento o *spoofing*.

Quando si lavora da casa, è essenziale proteggere anche il router domestico. Dovrebbe essere aggiornato e protetto con una password lunga e unica, diversa da quella automatica di cui sono dotati tutti i router. A tal fine, è possibile accedere alla pagina delle impostazioni del router digitando la frase appropriata nel browser e modificare la password. Nella stessa pagina, di solito è possibile modificare anche l'SSID, ossia il nome della rete wireless, per rendere più difficile a terzi l'identificazione e l'accesso alla rete wi-fi domestica. Non utilizzate il vostro nome, l'indirizzo di casa o qualsiasi altro elemento che possa essere utilizzato per l'identificazione.

È inoltre necessario assicurarsi che la crittografia di rete sia abilitata nelle impostazioni di sicurezza della pagina di configurazione wireless. È possibile scegliere tra diversi metodi di sicurezza, come WEP, WPA e WPA2. Il più potente è il WPA2, che richiede un hardware più recente del 2006.

3. Effetto della digitalizzazione sul mercato del lavoro

3.1 Trattamento discriminatorio in fase di selezione del personale

In un mondo antecedente alla tecnologia, tutte le decisioni riguardanti l'assunzione e la valutazione di un dipendente venivano prese dalle persone. Queste decisioni tenevano solitamente conto del contesto locale, di considerazioni etiche, di aspetti legali in termini di trasparenza del processo e di validità delle scelte manageriali. Oggi, invece, molte aziende utilizzano sistemi informatici che offrono una maggiore efficienza e riducono il noioso esame dei documenti alla ricerca di informazioni specifiche.

Questi sistemi, noti come ADS (*sistemi decisionali algoritmici*), si basano sull'analisi di grandi quantità di dati elaborati per produrre risultati che costituiscono la base del processo decisionale. L'intervento umano in questo processo è solitamente assai limitato e, in alcuni casi, può essere completamente eliminato. Tuttavia l'impatto di una particolare decisione su una determinata persona può essere di grande importanza, in quanto ne condiziona la situazione di vita.

Affidarsi totalmente agli ADS nel processo decisionale solleva quindi una serie di problemi etici, politici o legali. A causa del rischio che i sistemi algoritmici trasmettano i pregiudizi dei loro creatori, un affidamento illimitato alla tecnologia è controverso in particolare in settori come l'occupazione o l'accesso a servizi pubblici e privati (ad esempio, assistenza sanitaria, sistemi di valutazione del credito).

3.1.1. Cosa può fare una persona colpita da discriminazione algoritmica

Si presume che le disposizioni sulla parità di trattamento in materia di occupazione (in Polonia questo tema è coperto dall'articolo 18 [3a] e seguenti del Codice del lavoro) e il divieto di discriminazione (articolo 11 [3] del Codice del lavoro) debbano essere applicati nel processo di assunzione. Ciò significa che qualsiasi discriminazione sul lavoro (in particolare per motivi di sesso, età, disabilità, razza, religione, nazionalità, credo politico, appartenenza sindacale, origine etnica, religione, orientamento sessuale) è inaccettabile.

Tuttavia i casi di comportamento discriminatorio nel processo di assunzione esistono. Tra questi, la preferenza per i candidati di sesso maschile, il rifiuto di assumere giovani donne sposate o con figli o l'inserimento di clausole discriminatorie nei confronti degli stranieri. I criteri di esclusione possono essere tanto più diffusi quanto più un'azienda utilizza l'e-

recruitment basato su sistemi decisionali automatizzati. Non solo si possono verificare discriminazioni involontarie contro i candidati a causa di un'intelligenza artificiale condizionata, ma la direzione di un'azienda può introdurre deliberatamente nel sistema criteri di esclusione.

In caso di discriminazione nel processo di assunzione, manifestata dal contenuto non inclusivo di un annuncio o da domande indiscrete sulla vita privata e familiare, la persona lesa può perseguire la tutela dei propri interessi in tribunale. L'onere della prova in questi procedimenti spetta al datore di lavoro, mentre il potenziale candidato deve solo rendere plausibile l'esistenza di una discriminazione (articolo 18 [3b] del Codice del lavoro). Se il tribunale conferma la violazione, il datore di lavoro sarà obbligato a pagare alla persona discriminata un risarcimento di importo non inferiore al salario minimo.

Con il processo decisionale algoritmico, tuttavia, dimostrare e rivendicare un rifiuto ingiustificato nel processo di assunzione è molto più difficile. Ciò è legato al cosiddetto *problema della scatola nera*, ovvero la mancanza di trasparenza nel funzionamento degli strumenti di intelligenza artificiale. Ciò significa che spesso anche gli stessi sviluppatori, e quindi anche i datori di lavoro che implementano uno strumento di intelligenza artificiale, non sono consapevoli del suo funzionamento indesiderato, ma ciò non significa che siano esenti da responsabilità in caso di violazioni. Una persona che sospetta di essere stata ingiustamente respinta da un algoritmo può intraprendere azioni concrete per tutelare i propri interessi e modificare la decisione presa dal sistema.

L'articolo 22 del GDPR rimane fondamentale a questo proposito. Questa disposizione impone al responsabile del trattamento di attuare misure adeguate per proteggere i diritti, le libertà e gli interessi legittimi degli interessati (e quindi delle decisioni), nonché meccanismi che consentano a una persona specifica di contestare una decisione basata esclusivamente su un trattamento automatizzato.

Per quanto concerne l'ordinamento italiano, si prevede in via generale la nullità di qualsiasi patto od atto discriminatorio posto in essere dal datore di lavoro in sede di assunzione oppure durante lo svolgimento del rapporto di lavoro (art. 15 l. n. 300/1970). Inoltre, acquista particolare rilievo l'obbligo specifico a carico del datore di lavoro o committente (pubblico o privato) di informare non soltanto il lavoratore, ma anche le rappresentanze sindacali presenti nei luoghi di lavoro o, in mancanza, le sedi territoriali delle associazioni sindacali comparativamente più rappresentative sul piano nazionale circa l'utilizzo di sistemi decisionali o di monitoraggio integralmente automatizzati ai fini connessi al rapporto di lavoro (art. 1 *bis*, cc. 1 – 6, d.lgs. n. 152/1997).

Il decreto Trasparenza (d.lgs. n. 104/2022) ha previsto obblighi informativi per i datori di lavoro nel caso di utilizzo di sistemi decisionali e di monitoraggio automatizzati deputati a fornire indicazioni:

a) rilevanti ai fini dell'assunzione o del conferimento dell'incarico, della gestione o della cessazione del rapporto di lavoro, dell'assegnazione di compiti o mansioni;

b) incidenti sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori.

Il datore di lavoro/committente deve fornire una serie di informazioni tra cui quelle relative a: gli aspetti del rapporto di lavoro sui quali incide l'utilizzo dei sistemi decisionali o di monitoraggio automatizzati, le finalità e le modalità di funzionamento dei sistemi, le misure di controllo adottate per le decisioni automatizzate ed eventuali processi di correzione, il livello di sicurezza informatica, le categorie di dati e i parametri utilizzati per programmare e addestrare i suddetti sistemi.

Resta fermo quanto previsto dall'art. 4 St. Lav. nel caso in cui dai sistemi in questione possa derivare un controllo a distanza dei lavoratori.

Il decreto Lavoro (DL 48/2023 convertito in L. 85/2023), nell'ottica di alleggerire gli adempimenti per le imprese, è intervenuto anche sul decreto Trasparenza limitando l'obbligo informativo in capo al datore ai casi in cui i sistemi in questione siano «integralmente» automatizzati.

Se, a vostro avviso, la vostra candidatura è stata erroneamente respinta nel processo di e-recruitment:

1. Verificate che la decisione sia stata completamente automatizzata. A tal fine, leggete attentamente i termini e le condizioni di assunzione o contattate l'ufficio risorse umane dell'azienda e stabilite come funziona l'algoritmo nel contesto del processo di candidatura.
2. Chiedete all'azienda (responsabile del trattamento dei dati) di darvi l'opportunità di fornire il vostro punto di vista e di spiegare perché ritenete che il rifiuto sia stato sbagliato.
3. Richiedete una spiegazione della decisione presa dall'azienda e chiedete che la domanda venga riesaminata nuovamente, ma questa volta da un essere umano. L'amministratore deve rispondere quanto prima a tale richiesta (entro un mese al massimo). Entro un mese, l'amministratore deve anche informare l'utente che la richiesta non è stata soddisfatta e le relative motivazioni.
4. Tuttavia, se il responsabile del trattamento ignora la richiesta o la risposta non è soddisfacente, è possibile rivolgersi alle autorità di protezione dei dati e presentare un reclamo.

5. Inoltre, indipendentemente dal procedimento dinanzi all'autorità di protezione dei dati, avete il diritto di tutelare i vostri diritti dinanzi a un tribunale civile. Se ritenete che il trattamento dei vostri dati violi la legge, potete citare in giudizio il responsabile del trattamento o l'incaricato del trattamento. Davanti al tribunale, potete chiedere il risarcimento dei danni per le violazioni della legislazione sulla protezione dei dati, nonché sollevare questioni di discriminazione che hanno causato danni patrimoniali o non patrimoniali.

3.1.2. Norme UE in materia di AI e selezione del personale

Come già accennato, nella bozza di regolamento sull'intelligenza artificiale (AI Act), le questioni relative all'occupazione e alla gestione delle risorse umane sono state inserite nell'elenco dei sistemi ad alto rischio. Ciò significa che gli strumenti per la valutazione automatizzata di un candidato a una posizione dovranno passare attraverso un percorso speciale per essere autorizzati.

Molti obblighi ricadranno sui fornitori di sistemi di IA, che saranno soggetti a requisiti rigorosi per la progettazione, il collaudo, l'audit e la certificazione dei sistemi di IA. Inoltre, coloro che utilizzano i sistemi di IA proposti dai fornitori (ad esempio le aziende) saranno tenuti a utilizzarli in conformità alla legge e alle istruzioni operative e a garantire l'adeguatezza dei dati inseriti nei sistemi, il loro monitoraggio e la conservazione dei registri degli eventi in caso di incidenti.

Le nuove disposizioni dovrebbero fornire ulteriori garanzie contro le decisioni discriminatorie prive di fattore umano. Allo stesso tempo, la legge sull'IA non concede ulteriori poteri alle entità interessate da tali decisioni. Il quadro dell'UE sarà tuttavia integrato dalla prevista *direttiva sulla responsabilità dell'intelligenza artificiale*, che introdurrà per la prima volta disposizioni sui danni causati dai sistemi di intelligenza artificiale. L'obiettivo è stabilire una protezione più ampia per coloro che sono stati danneggiati dall'IA applicata e rendere più facile per loro chiedere un risarcimento. I regolamenti proposti rappresentano quindi un passo avanti nel fornire un accesso effettivo ai rimedi anche nei casi di discriminazione nell'uso dei sistemi di impiego. Infatti, presuppongono che sia il datore di lavoro a non aver adempiuto al proprio dovere di diligenza utilizzando un sistema di impiego che discrimina determinate categorie di persone.

I lavori sulla bozza di regolamento sull'intelligenza artificiale (AI Act), e sulla direttiva sulla responsabilità dell'intelligenza artificiale sono già in fase avanzata. Tuttavia, secondo l'attuale formulazione dei nuovi regolamenti, le loro disposizioni non saranno applicabili in tutti gli Stati membri dell'UE prima di due anni dalla loro adozione.

3.2 Il futuro del lavoro

3.2.1. Professioni in via di estinzione, competenze del futuro e responsabilità del datore di lavoro per adattare le competenze dei lavoratori all'automazione

Secondo una recente ricerca del Centre for Economic Policy Research (CEPR), il 40% degli intervistati dichiara di avere più del 50% di probabilità di essere sostituito da macchine, robot o algoritmi nel prossimo decennio. I timori di una disoccupazione tecnologica non sono del tutto infondati. Secondo il rapporto *Future Jobs*, si registra un aumento significativo della quota di nuove tecnologie nelle mansioni svolte. Nel 2018, in media, il 71% del tempo di lavoro era rappresentato da attività umane e il 29% da quelle svolte da macchine. Si prevede che queste proporzioni cambieranno in modo significativo entro il 2025. Gli esseri umani saranno responsabili di circa il 48% delle attività, mentre il restante 52% dei compiti sarà completamente automatizzato.

Per quanto riguarda l'impatto dell'automazione, si può ipotizzare che i lavori manuali, che possono essere facilmente sostituiti dai robot (cioè basati su sequenze prevedibili), saranno i più colpiti. Tuttavia, la digitalizzazione può riguardare anche alcuni professionisti. Secondo il rapporto *Future of Jobs,* tra le professioni in esubero, come il meccanico, il magazziniere e il direttore di produzione, troveremo anche l'analista finanziario o l'impiegato. Tuttavia, gli esperti del McKinsey Global Institute stemperano questi timori, poiché si stima che a livello globale solo il 5% delle professioni sarà completamente eliminato.

Ciò che cambierà senza dubbio è il modo in cui vengono svolte le mansioni lavorative (una quota maggiore di sistemi informatici e macchine nelle mansioni svolte) e le competenze desiderate dai dipendenti. Dato che molti compiti saranno svolti dalle macchine, aumenterà la richiesta di competenze che i computer non possono riprodurre con precisione. Stiamo parlando di competenze soft, cioè quelle che richiedono creatività, intelligenza emotiva, pensiero critico. La digitalizzazione aumenterà anche la domanda di competenze tecniche e creerà posti di lavoro per colletti bianchi ben qualificati in grado di far funzionare i nuovi sistemi. D'altro canto, ciò può sollevare preoccupazioni circa una crescente polarizzazione del mercato (inferiorità dei colletti blu e crescente importanza di quelli più istruiti). Queste preoccupazioni sembrano essere confermate dai risultati di uno studio del Centro europeo per lo sviluppo della formazione professionale (Cedefop), secondo cui oltre il 70% degli occupati ha bisogno di competenze informatiche almeno di base per orientarsi nell'attuale mercato del lavoro, ma ben il 30% rischia di non poter acquisire in modo permanente le competenze desiderate (e quindi di perdere il posto di lavoro).

3.2.2. Competenze del futuro e professioni superflue nell'era digitale

L'uso crescente della tecnologia farà sì che le competenze richieste dal mercato del lavoro cambieranno in modo significativo nei prossimi anni. Si prevede che con l'automazione e l'algoritmizzazione la domanda di competenze facilmente sostituibili dalle macchine diminuirà. Si tratta sia delle competenze manuali (nel caso di lavoratori manuali e di produzione) sia di quelle relative al lavoro mentale (ad esempio, calcolo o scrittura creativa). D'altro canto, aumenterà la richiesta di **competenze del futuro**, come definite nel rapporto DELab (*Competences of the future. How to shape them in a flexible educational ecosystem*?) come: *abilità specifiche per svolgere compiti in un ambiente di lavoro fondamentalmente flessibile, geograficamente disperso, soggetto a frequenti e rapidi cambiamenti, che comporta la necessità di utilizzare le tecnologie digitali e di cooperare con sistemi automatizzati e macchine che utilizzano l'intelligenza artificiale*.

McKinsey ha suddiviso queste competenze in tre gruppi: tecniche e digitali, sociali e cognitive.

Le competenze del futuro	
Tecnico e digitale	• Secondo le indicazioni, la domanda di competenze digitali **di base** aumenterà del 65%. Stiamo parlando della capacità di utilizzare la tecnologia nel lavoro di tutti i giorni, soprattutto per quanto riguarda la risoluzione di problemi e il reperimento di informazioni. • Entro il 2030, i lavoratori europei dedicheranno più del 40% del tempo ad attività che utilizzano competenze digitali avanzate. Inoltre, la domanda di competenze di programmazione e IT aumenterà del 90%.
Sociale	• Entro il 2030, la domanda di competenze sociali da parte del mercato del lavoro europeo, in particolare di imprenditorialità e capacità di prendere iniziative, aumenterà del 22%.
Cognitivo (superiore): pensiero critico, creatività, capacità di gestire le persone	• La richiesta di competenze cognitive superiori aumenterà del 14% entro il 2030. Allo stesso tempo, l'importanza delle competenze cognitive di base come la lettura, la scrittura e l'elaborazione di base diminuirà del 23%.

Kompetencje przyszłości w podziale na trzy grupy umiejętności: poznawcze, społeczne i techniczne

Il World Economic Forum (WFE) indica che nei prossimi anni futuro queste saranno le competenze più importanti:

- **gestione delle persone (HR)** - costruire la forza lavoro trovando le persone migliori per compiti specifici; motivare e gestire le persone mentre lavorano,
- **capacità di negoziazione**: capacità di risolvere i conflitti e di superare le divergenze di opinione, dimostrando capacità di persuasione,
- **intelligenza emotiva** - la capacità di identificare e dare un nome alle proprie emozioni e le emozioni altrui; la capacità di gestire e utilizzare le emozioni nel prendere giudizi e decisioni; la comprensione dei bisogni degli altri (dipendenti e clienti),
- **cooperazione con gli altri** - capacità di lavorare in gruppo,
- **flessibilità cognitiva**: la capacità di "passare" da un compito all'altro,
- **risolvere problemi complessi** - capacità di trovare soluzioni non ovvie in contesti diversi,
- **pensiero critico** - usare la logica e il ragionamento per identificare i punti di forza e di debolezza di soluzioni e le debolezze di soluzioni, conclusioni o approcci alternativi ai problemi,
- **creatività** - la capacità di pensare fuori dagli schemi, di proporre idee innovative, di risolvere i problemi in modi non ovvi.

Inoltre, nel suo rapporto il Forum economico mondiale elenca anche le **professioni che perderanno importanza nell'era della digitalizzazione**. Si tratta di professioni quali: addetto all'inserimento dati, addetto alla contabilità e alle buste paga, segretario amministrativo ed esecutivo, addetto all'assemblaggio e alla produzione, addetto all'informazione e al servizio clienti, responsabile dei servizi amministrativi e commerciali, contabile e revisore dei conti, magazziniere, direttore generale e operativo, impiegato postale, analista finanziario, cassiere e controllore di biglietti, meccanico, addetto al telemarketing, installatore di elettronica e telecomunicazioni, banchiere, autista, broker e agente di vendita, venditore porta a porta e venditore ambulante, addetto alle assicurazioni, statistiche e finanza, avvocato.

Zawody – prognoza na 2020 r.

Stabilne zawody	Nowe zawody	Zbędne zawody
Dyrektor zarządzający i prezes	Analityk danych i data scientist*	Pracownik wprowadzający dane
Główny menadżer i kierownik operacyjny*	Specjalista AI i ML	Pracownik księgowości i listy płac
Programista i analityk oprogramowania*	Główny menadżer i kierownik operacyjny*	Sekretarz administracyjny i wykonawczy
Specjalista działu sprzedaży i marketingu*	Specjalista Big Data	Pracownik montażu i produkcji
Przedstawiciel handlowy	Specjalista ds. transformacji technologicznej	Pracownik działu informacji i obsługi klienta*
Specjalista ds. zarządzania zasobami ludzkimi	Specjalista działu sprzedaży i marketingu*	Menadżer administracji i usług biznesowych
Doradca finansowy i inwestycyjny	Specjalista ds. nowych technologii	Księgowy i rewident
Specjalista ds. baz danych i sieci	Specjalista ds. rozwoju organizacji*	Magazynier
Specjalista ds. logistyki i łańcucha dostaw	Programista i analityk oprogramowania*	Główny menadżer i kierownik operacyjny*
Specjalista ds. zarządzania ryzykiem	Specjalista ds. automatyzacji procesów	Urzędnik pocztowy
Analityk bezpieczeństwa danych*	Specjalista ds. innowacji	Analityk finansowy
Analityk zarządzania i organizacji	Analityk bezpieczeństwa danych*	Kasjer i kontroler biletów
Inżynier elektrotechniki	Specjalista działu e-commerce i mediów społecznościowych	Mechanik
Specjalista ds. rozwoju organizacji*	Projektant UX i interakcji maszyna-człowiek	Telemarketer
Operator zakładu przetwórstwa chemicznego	Specjalista ds. szkoleń i rozwoju	Elektronik i instalator telekomunikacyjny
Nauczyciel uniwersytecki i szkolnictwa wyższego	Specjalista i inżynier robotyki	Bankier
Urzędnik ds. zgodności	Specjalista ds. ludzi i kultury	Kierowca
Inżynier energetyki i naftowy	Pracownik działu informacji i obsługi klienta*	Broker i agent sprzedaży
Specjalista i inżynier robotyki	Projektant usług i rozwiązań	Obwoźny sprzedawca i akwizytor
Operator i pracownik rafinerii ropy naftowej i gazu ziemnego	Specjalista ds. marketingu i strategii online	Pracownik ubezpieczeń, działu statystycznego i finansowego
		Prawnik

Źródło: World Economic Forum (2018) The Future of Jobs Report 2018, s. 9. Zawody oznaczone * występują w więcej niż jednej kolumnie tabeli, co spowodowane jest różnicami między poszczególnymi sektorami.

3.2.3. Digitalizzazione e tendenze nell'ambito della gestione aziendale - il ruolo dei datori di lavoro

Per sfruttare appieno la digitalizzazione e i vantaggi derivanti dall'implementazione delle nuove tecnologie, le aziende dovranno riorganizzare le proprie strutture e cambiare l'attuale approccio al lavoro. A tal fine sarà necessario ridisegnare l'organizzazione formale

dell'azienda, aggiungere personale con nuove competenze, riqualificare o sviluppare i talenti esistenti. Secondo McKinsey, a causa del cambiamento delle professioni desiderate e delle competenze più ricercate le organizzazioni saranno costrette a **aggiornarsi in cinque aree chiave** - mentalità, struttura organizzativa, assegnazione del lavoro, composizione della forza lavoro e responsabilità del management e delle risorse umane.

In termini di mentalità aziendale, la chiave per il successo futuro dell'organizzazione sarà promuovere la tendenza del cosiddetto *apprendimento permanente*, ossia offrire ai dipendenti l'opportunità di acquisire nuove competenze e conoscenze durante tutto il percorso di carriera, non solo all'inizio. In termini di struttura organizzativa, l'introduzione di modalità di gestione più dinamiche e innovative, nonché una più frequente collaborazione tra i team e la condivisione di conoscenze e funzioni tra i dipendenti sono indicate come priorità per i prossimi anni.

Le aziende che implementano l'automazione su larga scala prevedono anche di trasferire le mansioni attualmente svolte da lavoratori altamente qualificati a lavoratori meno qualificati (con il supporto di macchine e computer). In termini di risorse umane si prevede un maggiore ricorso a vari tipi di freelance e lavoratori temporanei. Ciò deriverà dalla crescita della cosiddetta *sharing economy/economia on-demand*, ovvero modelli di business basati sull'intermediazione di piattaforme collaborative, che creano un mercato ad accesso libero per l'utilizzo temporaneo di beni o servizi, spesso forniti da privati.

Preservare la competitività dell'azienda sostenendo i dipendenti nel processo di digitalizzazione

Nel rapporto *Beyond Hiring. How companies are re-skilling to address talent shortages,* McKinsey ha delineato diverse tattiche per mantenere le aziende competitive e colmare il divario tra le competenze desiderate e quelle disponibili dei dipendenti del settore privato. Tra le pratiche che i datori di lavoro che cercano di far crescere la propria attività e di costruire una forza lavoro competente dovrebbero prendere in considerazione vi sono:

- **Riqualificazione** - incoraggiare l'acquisizione di nuove competenze e l'aggiornamento di quelle esistenti da parte dei dipendenti esistenti, nonché l'implementazione e la formazione dei nuovi assunti nelle capacità desiderate. Una questione fondamentale per le aziende sarà decidere le modalità di erogazione della formazione: internamente (utilizzando le risorse e i programmi disponibili) o esternamente (in collaborazione con un istituto di istruzione o un centro di formazione). Per quanto riguarda le aree in cui gli imprenditori intendono investire, il più delle volte riguardano la costruzione di competenze strategiche per la loro azienda, ad esempio competenze informatiche avanzate, capacità di scrittura creativa, pensiero critico,

capacità di risolvere problemi. D'altro canto, per le competenze meno complesse, i datori di lavoro dichiarano la possibilità di assumere persone esterne all'organizzazione.

- **Trasferimenti all'interno dell'azienda** - spostamento dei dipendenti con competenze specifiche in reparti/team dove possono sfruttare meglio le loro capacità. In un sondaggio McKinsey condotto nel febbraio 2018 tra i dirigenti d'azienda. Il 55% degli intervistati ha dichiarato che preferirebbe ricollocare alcuni dipendenti in ruoli diversi o completamente nuovi piuttosto che licenziarli completamente.

- **Assunzione** - ricerca di individui o interi team con le competenze specifiche richieste (anche se l'offerta di esperti sul mercato potrebbe non essere sufficiente per tutte le aziende per perseguire questa strategia). Da un lato, il costo dell'assunzione può essere inferiore a quello della riqualificazione, ma dall'altro l'approvvigionamento di nuovi membri del team comporta un rischio per le prestazioni del singolo. Per riuscire ad attrarre nuovi talenti chiave, le aziende dovrebbero quindi innovare il modo in cui reclutano i candidati, oltre a offrire una cultura del lavoro attraente e benefici non salariali.

- **Creare nuove forme di collaborazione** - le aziende possono beneficiare delle competenze apportate da persone esterne all'organizzazione (liberi professionisti, esperti, agenti temporanei di agenzie di reclutamento). L'aspetto negativo di questo modello, tuttavia, è il rischio di trasferire segreti commerciali (ad esempio, know-how, opere coperte da diritti di proprietà intellettuale) a persone esterne, nonché la difficoltà di inserirsi nella cultura e nelle modalità di lavoro dell'azienda. Per questo motivo, i datori di lavoro dichiarano di occupare posizioni non correlate alle attività principali dell'azienda o che richiedono basse qualifiche con appaltatori indipendenti.

- **Possibili esuberi** - In alcune aziende possono essere necessari degli esuberi, in particolare nei settori che non crescono abbastanza rapidamente e in cui l'automazione sostituirà in modo significativo la forza lavoro. Una strategia di esuberi può essere attuata riducendo o interrompendo l'assunzione di nuovi dipendenti, consentendo al contempo di continuare il normale processo di pensionamento e di uscita di quelli già impiegati.

Sebbene siano possibili licenziamenti dovuti al maggiore utilizzo delle macchine, è difficile pensare che i dipendenti di tutti i settori debbano temere per il proprio posto di lavoro. Tuttavia ci saranno indubbiamente nuove tecnologie, sistemi e programmi che richiederanno l'acquisizione di ulteriori competenze informatiche.

Come possono i datori di lavoro sostenere i propri dipendenti nella digitalizzazione dell'impresa?

Innanzitutto possono:

- familiarizzare i dipendenti con i nuovi strumenti - eliminare la paura e il conservatorismo nei confronti delle nuove tecnologie e mostrare come gli strumenti digitali possono essere utilizzati nel lavoro quotidiano,
- sensibilizzare i dipendenti - spiegare perché e come l'azienda utilizza la tecnologia; con informazioni in questo ambito, i dipendenti comprenderanno meglio i nuovi strumenti di lavoro e saranno motivati a utilizzarli,
- preparare bene i manager ai cambiamenti imminenti - i manager devono conoscere le risposte alle domande di base sui nuovi strumenti di lavoro e mostrare agli altri membri del team come utilizzare le tecnologie implementate,
- fornire formazione sui nuovi sistemi - anche i dipendenti esperti di tecnologia hanno bisogno di tempo per familiarizzare con nuovi software e strumenti digitali che non hanno mai usato prima; l'azienda dovrebbe fornire una formazione professionale a tutti i dipendenti.

3.2.4. Altri soggetti che svolgono un ruolo chiave nella processi di digitalizzazione del lavoro e nella riqualificazione dei lavoratori

Istituzioni educative

Il ruolo dell'istruzione nel processo di digitalizzazione è già riconosciuto dagli organismi dell'Unione Europea. Le conclusioni del Consiglio europeo hanno sottolineato che l'accesso a un'istruzione di alta qualità supportata dalle tecnologie digitali è un prerequisito per la trasformazione di singoli settori e per un'ulteriore crescita economica.

Inoltre, la Commissione europea ha incluso la creazione di un piano d'azione per l'istruzione digitale per il periodo 2021-2027 che definisce una visione per l'istruzione digitale in Europa. L'obiettivo di entrambe le iniziative era quello di incoraggiare le università, le scuole e il personale docente a svolgere un ruolo più attivo nella costruzione di competenze digitali e nel soddisfare le esigenze del mercato del lavoro. Il ruolo di queste istituzioni nella trasformazione digitale sembra essere confermato anche da pubblicazioni economiche, come il rapporto di PwC e WFE *Raising Skills for Shared Prosperity* (2021), che sottolinea come gli istituti di istruzione superiore abbiano il potenziale per guidare il cambiamento - per

aumentare le conoscenze, le abilità e le competenze complessive degli studenti e della società.

Autorità pubblica

Il ruolo dello Stato è quello di sostenere sia gli imprenditori che i dipendenti nel processo di digitalizzazione. È quindi importante che i responsabili politici attuino politiche che incoraggino l'acquisizione di competenze digitali o la riqualificazione dei dipendenti (ad esempio, attraverso programmi di sussidi alla formazione per le piccole e medie imprese). Inoltre, è importante stimolare il mercato del lavoro ed evitare la disoccupazione attraverso politiche attive per l'occupazione: invece di affidarsi ai sussidi di disoccupazione, lo Stato dovrebbe investire in agenzie per l'impiego che diventino centri di collocamento e facilitino la riqualificazione dei disoccupati.

ONG

Le ONG e i think tank spesso fungono da incubatori di soluzioni socialmente utili. Tendono ad avere maggiore libertà d'azione rispetto alle istituzioni statali e possono proporre soluzioni diverse ai problemi. Per questo motivo, alcune aziende intraprendono iniziative filantropiche o collaborano con fondazioni in settori legati all'acquisizione di nuove competenze da parte dei dipendenti. Un esempio è l'iniziativa Generation, che lavora per combattere la disoccupazione colmando il divario di competenze tra i giovani e sostenendo gli adulti nella ricerca di un lavoro adatto a loro attraverso il reclutamento, la formazione e il tutoraggio.

Sindacati e organizzazioni professionali

In qualità di parti sociali, le associazioni industriali e i sindacati svolgono un ruolo importante nella digitalizzazione del mercato del lavoro. In Svezia, ad esempio, sono stati istituiti dei consigli per la tutela del lavoro finanziati dalle aziende e dai sindacati. Questi enti formano le persone che hanno perso il lavoro, fornendo loro un sostegno finanziario temporaneo e facilitando il processo di riqualificazione in modo che i disoccupati rientrino più rapidamente nel mercato del lavoro.

3.3 Nuovi business model e loro impatto sul mercato del lavoro

3.3.1. Erosione del la forza negozianel dei lavoratori - in che modo le tecnologie ostacolano la sindacalizzazione dei lavoratori

Le nuove tecnologie facilitano la comunicazione e mettono in contatto gli utenti tra loro, nonostante la distanza che li separa. Allo stesso tempo, però, stanno portando a una maggiore alienazione e a una sempre minore interazione umana. Questo fenomeno non riguarda solo la sfera privata, ma anche quella professionale. La digitalizzazione e lo spostamento del lavoro nel mondo online hanno fatto sì che i dipendenti sporadicamente instaurino relazioni durature e che si incontrino e discutano dei problemi sul posto di lavoro meno frequentemente.

Le nuove tecnologie favoriscono l'isolamento, non solo a causa del lavoro a distanza. Gli strumenti di intelligenza artificiale utilizzati dalle aziende per controllare i dipendenti e misurare la loro produttività sono spesso usati anche per sorvegliarli e impedire l'associazione dei lavoratori.

Talvolta i modelli di business delle grandi imprese si basano su un controllo estensivo dei lavoratori e su una costante accelerazione dei ritmi di lavoro. La sindacalizzazione dei lavoratori per rappresentare i loro diritti e interessi collettivi e individuali rappresenta quindi un rischio reale per un sistema che si preoccupa solo di massimizzare i profitti aziendali. Per questo motivo, le imprese adottano misure per impedire ai lavoratori di sindacalizzarsi. Questa pratica si è intensificata durante la pandemia da COVID-19, quando le raccomandazioni in materia di salute e sicurezza introdotte in quel periodo hanno iniziato a essere utilizzate per implementare nei luoghi di lavoro strumenti per misurare la distanza tra le persone nei magazzini, vietando loro di stare troppo vicine. Le aziende hanno iniziato a dotarsi di software che consentivano di analizzare e visualizzare i dati sulle relazioni all'interno dei luoghi di lavoro (ad esempio, la geoSPatial Operating Console o SPOC). Inoltre, i dipartimenti delle risorse umane hanno monitorato le mailing list dei dipendenti utilizzate per scopi attivistici o i gruppi di dipendenti sui social media.

Nel caso del lavoro su piattaforma, l'impatto delle nuove tecnologie sull'associazione dei lavoratori non è nettamente solo positivo o negativo. Le app utilizzate per fornire servizi possono facilitare la mobilitazione di corrieri e autisti - le chat room interne disponibili nei loro sistemi offrono ai lavoratori delle piattaforme (*gig-worker*) uno spazio per scambiare informazioni, mentre le reti di comunicazione di massa possono collegare i singoli corrieri a livello di città, regioni e persino Paesi.

Allo stesso tempo, l'efficacia dei sindacati dei lavoratori delle piattaforme dipende spesso dal sostegno delle autorità pubbliche a varie forme di auto-organizzazione. A Bologna, ad esempio, è stata creata, in collaborazione con i sindacalisti, una *Carta dei diritti fondamentali*

del lavoro digitale nel contesto urbano, che stabilisce un quadro di standard minimi per i salari, l'orario di lavoro e la protezione assicurativa dei lavoratori delle piattaforme. È significativo, tuttavia, che lo stesso sindaco di Bologna abbia mostrato grande sostegno per l'iniziativa e abbia invitato i clienti a boicottare le piattaforme che non avessero firmato la Carta.

Nei Paesi in cui lo Stato non estende l'assistenza ai lavoratori delle piattaforme, il loro livello di sindacalizzazione è molto più basso e il loro potere contrattuale più debole. Di questo aspetto abusano talvolta le piattaforme, che utilizzano i meccanismi delle app per controllare meglio i corrieri o gli autisti e vanificare i tentativi di opporsi alle politiche aziendali.

Un esempio di come i giganti della sharing economy stiano usando la tecnologia per limitare le iniziative dei lavoratori che lottano per i loro diritti è stato lo sciopero nell'aprile 2021, rapidamente messo a tacere, dei rider polacchi che consegnano i pasti. Lo sciopero è stato motivato dall'iniquità con cui l'algoritmo distribuiva gli ordini e fissava la retribuzione. Il metodo di protesta è stato che i corrieri avevano smesso di evadere gli ordini, nonostante la loro dichiarata disponibilità a lavorare nell'app. Gli autisti speravano di fare pressione sull'azienda e di convincerla a parlare con i rappresentanti della comunità. Tuttavia, l'azienda, utilizzando l'app, senza alcun tentativo di comunicare con i corrieri, ha bloccato gli scioperanti e ha passato gli ordini a persone disposte a svolgere il lavoro nonostante le condizioni avverse.

3.3.2. Effetto della digitalizzazione sul mercato del lavoro - il lavoro tramite piattaforma

Il lavoro su piattaforma è una forma di occupazione in cui un lavoratore utilizza una piattaforma digitale per accedere ad altre organizzazioni o individui per fornire determinati servizi in cambio di un determinato stipendio. I compiti svolti a pagamento attraverso le piattaforme digitali includono servizi di taxi e corriere, consegne, servizi di riparazione a domicilio, nonché lavori impiegatizi come il copywriting e la contabilità. Sebbene app come Uber e Bolt si siano sviluppate nello spazio europeo solo da un decennio, i lavoratori che forniscono servizi attraverso piattaforme di questo tipo costituiscono oggi una parte significativa della forza lavoro (28,3 milioni di lavoratori nel 2022 nell'Unione Europea). Questo dato è paragonabile al numero di persone impiegate nei settori produttivi industriali (29 milioni di lavoratori). Inoltre, secondo la Commissione europea, le piattaforme dovrebbero aggiungere altri 15 milioni di dipendenti entro il 2025. Le piattaforme più popolari nell'UE includono Uber, Deliveroo, Amazon Mechanical Turk, Fiverr, Upwork, Appjobs, Glovo o JustEat.

Il modello di business delle piattaforme di lavoro si basa su tecnologie che utilizzano algoritmi per far incontrare efficacemente la domanda e l'offerta di lavoratori e i servizi che essi forniscono. Inoltre, l'uso di applicazioni opportunamente progettate consente di prendere decisioni automatiche senza contatto e di monitorare le mansioni svolte. Con un sistema di gestione basato su algoritmi, è possibile fare a meno del personale dirigente tradizionale. Questo, a sua volta, fa sì che le piattaforme sostengano di agire semplicemente come un intermediario che offre servizi per mettere in contatto i lavoratori autonomi con i potenziali clienti, piuttosto che come un datore di lavoro.

Chi è più propenso a cercare lavoro attraverso le piattaforme di lavoro?

- giovani
- uomini
- immigrati (soprattutto per quanto riguarda i lavori manuali),
- persone con istruzione post-secondaria, per le quali questo lavoro rappresenta una fonte di reddito aggiuntiva.

Inoltre, i lavoratori delle piattaforme possono essere suddivisi in due gruppi agli antipodi nel mercato del lavoro. Il primo gruppo comprende i colletti bianchi, privilegiati in termini di competenze, ad esempio i programmatori che possono influenzare i termini e le condizioni di collaborazione con i clienti (freelance, fornitura di servizi informatici). Il secondo gruppo, invece, comprende persone con competenze basse e facilmente sostituibili, il cui potere negoziale sul mercato del lavoro è basso (ad esempio, gli immigrati che forniscono servizi di taxi).

Vantaggi e svantaggi del lavoro su piattaforma

I vantaggi del lavoro su piattaforma includono:

- orari di lavoro flessibili e la possibilità di pianificare il proprio programma di lavoro,
- contatto diretto con i committenti,
- maggiore indipendenza.

Allo stato attuale delle piattaforme digitali, tuttavia, questo tipo di impiego presenta una serie di svantaggi:

- problemi di salute e sicurezza:

    - mancanza di norme regolamentate in materia di salute e sicurezza,
    - rischi fisici,
    - stress causato dall'insicurezza del lavoro;
- termini e condizioni di impiego:
    - 5,5 milioni di persone che lavorano attraverso piattaforme di lavoro nell'UE sono erroneamente classificate come lavoratori autonomi,
    - le persone classificate erroneamente come lavoratori autonomi non hanno diritto agli stessi diritti e benefici dei lavoratori dipendenti;
- problemi derivanti dall'algoritmizzazione del lavoro,
- opportunità limitate di associazione,
- salari e orari di lavoro imprevedibili (secondo la Commissione europea, il 41% dell'orario di lavoro dei lavoratori delle piattaforme consiste in attività non retribuite, come la consultazione di annunci o l'attesa di ordini).

Diritto dell'UE e lavoro su piattaforma

Alcuni Stati membri hanno già introdotto norme per il lavoro su piattaforme nella legislazione nazionale. Anche a livello comunitario si sta discutendo di questo particolare tipo di occupazione. Il concetto di lavoratore su piattaforma è già stato introdotto nella legislazione dell'UE, ad esempio attraverso la direttiva sulle condizioni di lavoro trasparenti e prevedibili nell'Unione europea. Tuttavia il punto di svolta è rappresentato dalla **Direttiva sul miglioramento delle condizioni di lavoro dei lavoratori delle piattaforme**, la cui bozza è stata presentata dalla Commissione europea alla fine del 2021.

Alcune disposizioni chiave incluse nella proposta di direttiva sul miglioramento delle condizioni di lavoro dei lavoratori tramite piattaforme:

- Coloro che lavorano attraverso le piattaforme digitali otterranno uno status occupazionale che corrisponde alle loro effettive condizioni di lavoro, che saranno verificate stabilendo i criteri necessari per riconoscere la piattaforma come datore di lavoro.
- Una piattaforma sarà considerata un datore di lavoro se soddisfa almeno due dei seguenti criteri:
    - determina il livello di remunerazione o fissa un tetto massimo,
    - supervisiona per via elettronica l'esecuzione del lavoro,

- limita la libertà di scegliere l'orario di lavoro o i periodi di assenza, la libertà di accettare o rifiutare incarichi o la libertà di ricorrere a subappaltatori o sostituti,
- stabilisce regole specifiche e vincolanti sull'aspetto e sul comportamento nei confronti del destinatario del servizio o del committente dell'opera,
- limita la capacità di espandere la base di clienti o di eseguire lavori per conto di terzi.

- Ai lavoratori delle piattaforme dovrebbero spettare i diritti lavorativi e sociali in base al loro status occupazionale:
  - tempi di riposo garantiti e ferie pagate,
  - salario minimo,
  - la possibilità di contrattazione collettiva,
  - sicurezza e protezione della salute,
  - indennità di disoccupazione e di malattia,
  - pensioni basate sui contributi.

- La piattaforma può contestare la classificazione, ma deve dimostrare che non esiste un rapporto di lavoro.
- Le piattaforme dovranno aumentare la trasparenza nell'uso degli algoritmi e garantire il monitoraggio umano delle condizioni di lavoro.
- I dipendenti avranno il diritto di contestare le decisioni automatizzate.