UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Sede Amministrativa: Università degli Studi di Padova

Dipartimento di Scienze Politiche, Giuridiche e Studi Internazionali (SPGI)

CORSO DI DOTTORATO DI RICERCA IN:

DIRITTO INTERNAZIONALE, PRIVATO E DEL LAVORO

CICLO: XXXVI

LA TUTELA DELLA RISERVATEZZA DEL LAVORATORE NELL'AMBITO DELLE FONTI DELL'ORGANIZZAZIONE INTERNAZIONALE DEL LAVORO

Coordinatore: Ch.ma Prof.ssa Arianna Fusaro

Supervisore: Ch.mo Prof. Andrea Sitzia

Dottorando: Massimiliano Rosa

LA TUTELA DELLA RISERVATEZZA DEL LAVORATORE NELL'AMBITO DELLE FONTI DELL'ORGANIZZAZIONE INTERNAZIONALE DEL LAVORO

* * *

* * *

Introduzione

La tutela della riservatezza del lavoratore non ha tradizionalmente rivestito un ruolo centrale nell'ambito dell'Organizzazione Internazionale del Lavoro (d'ora in avanti, per semplicità, anche ILO o Organizzazione) [1].

Infatti, l'unico strumento organico adottato dall'ILO in merito alla protezione della *privacy* dei prestatori di lavoro è costituito dal *Code of Practice on the protection of workers' personal data* del 1997 (di seguito, per brevità, anche "il Codice ILO", "*Code of practice*" o "Codice di condotta")[2].

L'ILO non ha invece adottato Convenzioni o Raccomandazioni[3] specificatamente dedicate alla tematica oggetto del presente elaborato.

---

[1] L'International Labour Organization (ILO) o *Organisation Internationale du Travail* (OIT) è l'Agenzia specializzata delle Nazioni Unite che promuove a livello globale la tutela dei diritti dei lavoratori e la giustizia sociale.
L'ILO, quale organizzazione a vocazione universale, presenta una triplice funzione.
Alla funzione di carattere umanitario consistente nel miglioramento delle condizioni dei lavoratori risulta strettamente connessa una finalità di tipo politico giacché le tensioni scaturenti dall'ingiustizia sociale rappresentano una minaccia fondamentale per il mantenimento della pace e dell'armonia a livello globale. Inoltre, l'ILO presenta una funzione economica in quanto gli Stati che adottano riforme sociali sono chiamati a sostenere maggiori costi e, quindi, "*la non adozione da parte di alcuni paesi di condizioni di lavoro più umane costituisce un ostacolo per altri che, al contrario, intendono migliorare la situazione dei lavoratori nei propri paesi*" (Preambolo della Costituzione dell'ILO).
Per adempiere a tali funzioni (umanitarie, politiche ed economiche) l'ILO adotta norme internazionali del lavoro, sotto forma di Convenzioni e Raccomandazioni, che individuano *standard* globali di protezione del lavoro.
L'Organizzazione si caratterizza per la sua peculiare struttura tripartita giacché negli organi dell'ILO sono rappresentati non solo i governi, ma anche i rappresentanti delle organizzazioni imprenditoriali e delle associazioni sindacali dei lavoratori, così da coinvolgere nell'attività istituzionale dell'Organizzazione i principali attori interessati alla regolamentazione dei fenomeni attinenti al lavoro umano.
Per un'analisi della struttura e dell'attività dell'ILO si rinvia, *ex multis*, a R. TREMELLONI, *L'Organizzazione internazionale del lavoro*, Aracne, Milano, 1924; A. ALCOCK, *History of the International Labour Organization*, London, Macmillan, 1971; R. ADAM, *Attività normative e di controllo dell'OIL e evoluzione della comunità internazionale*, Giuffrè, Milano, 1993; R. BLANPAIN, M. COLUCCI (a cura di), *L'organizzazione internazionale del lavoro. Diritti fondamentali dei lavoratori e politiche sociali*, Jovene Editore, Napoli, 2007; V. FERRANTE (a cura di), *A tutela della prosperità di tutti. L'Italia e l'Organizzazione Internazionale del Lavoro a un secolo dalla sua istituzione*, Giuffrè, Milano, 2019; L. MECHI e A. SITZIA, *Cento Anni nell'Organizzazione Internazionale del Lavoro. Prospettive storiche e giuridiche sulla partecipazione italiana*, CEDAM, Milano, 2023.

[2] Il Codice di condotta sulla tutela dei dati personali dei lavoratori rappresenta uno strumento di *soft law*, privo di forza vincolante per gli Stati aderenti all'ILO, che si propone di fungere da riferimento per lo sviluppo di leggi, regolamenti, contratti collettivi, regole di lavoro e *policy* aziendali.

[3] L'ILO formula le norme internazionali in materia di lavoro attraverso l'adozione di Convenzioni e di Raccomandazioni. Le Convenzioni sono trattati internazionali, aperti alla ratifica degli Stati aderenti all'ILO, che si pongono l'obiettivo di fornire un livello uniforme di tutela dei lavoratori a livello globale, mentre le Raccomandazioni, pur essendo prive di forza vincolante, a differenza dei Codici di condotta, comportano obblighi procedurali.

Ciò, tuttavia, non significa che l'argomento affrontato non sia di estrema attualità e rilevanza.

Ne è dimostrazione evidente la *Centenary Declaration for the Future of Work* [4], approvata dalla Conferenza Internazionale del Lavoro in data 21 giugno 2019, documento programmatico – adottato nell'anno di ricorrenza del centenario della Organizzazione, fondata, appunto, nel 1919 – che formalizza le principali sfide e opportunità di lungo termine essenziali per il raggiungimento degli obiettivi strategici dell'ILO[5].

Per quanto di interesse ai fini del presente elaborato, risulta particolarmente significativa la volontà dell'ILO di promuovere "*politiche e misure che garantiscano un adeguato rispetto della vita privata e la protezione dei dati personali, e che reagiscano alle sfide e colgano le opportunità che si presentano nel mondo del lavoro in relazione alla trasformazione digitale del lavoro, ivi compreso il lavoro su piattaforma*".

Con un evidente cambio di paradigma rispetto al passato, l'ILO sta dimostrando di reputare la protezione della *privacy* dei prestatori di lavoro come una componente imprescindibile del *decent work*.

In sostanza, l'ILO sembra aver preso definitivamente atto della circostanza che il potenziamento tecnologico della capacità delle imprese di raccogliere e trattare grandi quantità di dati personali consente lo sviluppo di modalità di organizzazione e di controllo della prestazione, che, se non adeguatamente governate, sono in grado di incidere sulla stessa qualità e dignità del lavoro, con possibile *vulnus* del nucleo più essenziale dei diritti dei lavoratori.

Infatti, l'esecuzione della prestazione di lavoro è sempre più governata da sistemi tecnologicamente avanzati alimentati da dati personali che forniscono automaticamente istruzioni continue e puntuali ai lavoratori, indicando le attività da compiere nonché le modalità e le tempistiche assegnate per la realizzazione di ogni singola *task*.

---

[4] Le Dichiarazioni sono risoluzioni adottate dalla Conferenza Internazionale del Lavoro contenenti impegni simbolici e politici da parte degli Stati membri.

[5] La Dichiarazione del Centenario esprime la necessità di agire urgentemente "*in un momento di profondi cambiamenti nel mondo del lavoro, determinati dalle innovazioni tecnologiche, dai cambiamenti demografici, dai cambiamenti ambientali e climatici e dalla globalizzazione, e in una fase di diseguaglianze persistenti, che hanno delle profonde ripercussioni sulla natura e sul futuro del lavoro, nonché sul ruolo e sulla dignità delle persone*" per *"cogliere le opportunità e far fronte alle sfide al fine di costruire un futuro del lavoro equo, inclusivo e sicuro, caratterizzato da piena occupazione, lavoro produttivo e liberamente scelto e lavoro dignitoso per tutti"* (traduzione a cura dell'Ufficio OIL per l'Italia e San Marino).

In questo modo, peraltro, il datore di lavoro può costantemente acquisire flussi informativi che gli consentono di ottenere una conoscenza estremamente precisa su tutte le attività svolte dal prestatore di lavoro nell'arco di ogni giornata lavorativa.

Ciò comporta inevitabili ripercussioni sulla libertà e sulla dignità del lavoratore che viene a trovarsi in una condizione di costante pressione, sapendo che il datore di lavoro è potenzialmente in grado di ricostruire ogni suo movimento, di individuare ogni errore e ritardo nonché ogni c.d. licenza comportamentale, seppur sostanzialmente ininfluente sul risultato complessivo della prestazione lavorativa.

Altra sfida sollevata dall'evoluzione delle tecniche di trattamento consiste nella possibilità di elaborare i dati al fine di assumere determinazioni direttamente incidenti sull'assunzione e sulla gestione del rapporto di lavoro.

Infatti, sempre più frequentemente, gli *output* di processi di analisi algoritmiche indicano quali siano i lavoratori da assumere, promuovere, trasferire o "epurare".

La sempre maggiore capacità di gestione dei c.d. *big data* ha altresì accresciuto la probabilità che le imprese vengano a conoscenza di informazioni relative alla personalità e alla vita privata dei lavoratori.

Una delle ragioni fondamentali delle cautele che circondano il trattamento dei dati personali dei lavoratori consiste nel rischio che il datore di lavoro possa utilizzare le informazioni acquisite per attuare condotte discriminatorie ai danni dei lavoratori. Infatti, la conoscenza di informazioni costituenti dati personali – quali le condizioni di salute, le opinioni politiche, religiose e sindacali e, persino, i gusti e le preferenze soggettive – rischia di esporre i lavoratori a trattamenti sfavorevoli e, financo, all'attuazione di condotte finalizzate all'emarginazione e/o all'allottamento dalla compagine aziendale.

Ebbene, le moderne elaborazioni algoritmiche alimentate dal trattamento di dati personali, comportando il rischio di generare *output* discriminatori, espongono i lavoratori al fenomeno delle discriminazioni algoritmiche.

Ulteriori problematiche attengono, poi, alla trasparenza e alla conoscibilità del funzionamento delle più moderne tecnologie utilizzate nella gestione del lavoro.

Se per un lavoratore o un'organizzazione sindacale risulta agevole la comprensione del funzionamento di un sistema di video-monitoraggio, non altrettanto vale per il funzionamento di un algoritmo o di un sistema di intelligenza artificiale.

Infatti, si pone, innanzitutto, una difficoltà di accedere alle informazioni, ma, quandanche tale ostacolo fosse superato, sono necessarie competenze tecniche e specialistiche al fine di comprendere a pieno "i ragionamenti" che conducono agli *output* espressi da tali sistemi.

Lo scenario così delineato rende evidente come la vulnerabilità e la soggezione dei lavoratori, elementi intrinseci alla relazione contrattuale lavoristica, risultino notevolmente accresciuti a causa della crescente difficoltà a mantenere un effettivo controllo sul flusso e sull'utilizzo dei propri dati personali.

Da qui la rinnovata attenzione dell'ILO per la *privacy* quale componente della relazione lavorativa da regolamentare al fine di garantire ai prestatori condizioni di lavoro dignitose.

Ciò detto, di seguito si esporrà l'ordine di trattazione dei temi oggetto di indagine.

La prima parte dell'elaborato sarà dedicata all'individuazione e all'analisi delle previsioni in materia di riservatezza dei lavoratori contenute all'interno delle fonti dell'Organizzazione Internazionale del Lavoro.

Come anticipato, ferma restando la rinnovata centralità della tematica nell'attuale dibattito interno all'ILO, bisogna dare atto che, allo stato, la *privacy* nel contesto lavorativo trova una disciplina compiuta solamente all'interno del *Code of practice on workers' personal data*, adottato dall'ILO nel 1997 insieme al *Commentary on the Code of practice* (d'ora in poi, per brevità, "il Commentario"), utile ausilio interpretativo del Codice ILO.

Tuttavia, la circostanza che non siano state adottate Convenzioni e Raccomandazioni *ad hoc* sulla tutela della riservatezza dei lavoratori[6] non implica necessariamente che manchino del tutto disposizioni *in subiecta materia*.

Uno degli obiettivi del presente elaborato consiste proprio nel procedere alla ricognizione delle Convenzioni e delle Raccomandazioni dell'ILO al fine di individuare ed estrapolare, all'interno delle stesse, le disposizioni dedicate alla protezione della riservatezza dei lavoratori.

Si reputa tale attività di ricerca scientificamente rilevante in quanto, allo stato dell'arte,

[6] Sotto il profilo terminologico, nel presente elaborato il termine riservatezza è inteso con un significato ampio, tale da ricomprendere al suo interno non solo il trattamento dei dati personali, ma anche la tutela della vita privata del lavoratore. In altri termini, il trattamento dei dati dei lavoratori rientra all'interno del concetto di riservatezza, senza tuttavia esaurirne la portata.

per quanto consta, manca uno studio di ricognizione e analisi delle norme riguardanti la tutela della riservatezza contenute all'interno delle fonti primarie dell'Organizzazione Internazionale del Lavoro, essendo i lavori dedicati alla tutela della *privacy* nel contesto dell'ILO esclusivamente incentrati sull'analisi del *Code of practice*.

Invece, il presente lavoro mira a ricostruire un quadro normativo generale che tenga conto anche delle previsioni contenute in Convenzioni e Raccomandazioni che, seppur dirette a regolamentare tematiche diverse, purtuttavia si occupano, per così dire, incidentalmente anche della protezione della riservatezza dei lavoratori.

Più nello specifico, per quanto concerne la prima parte dell'elaborato, in primo luogo si procederà all'analisi del *Code of Practice* attraverso l'esame del suo contenuto anche attraverso il raffronto con strumenti normativi europei in materia di privacy (Reg. UE 679/2016 e art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, c.d. CEDU, così come interpretato dalla giurisprudenza della Corte Europea dei Diritti dell'Uomo).

In particolare, sarà oggetto di approfondimento la soluzione adottata dal Codice ILO in ordine all'ammissibilità dei c.d. controlli difensivi occulti, tenuto conto della centralità rivestita della tematica all'interno della giurisprudenza nazionale e della Corte Edu.

Seguirà l'analisi delle Convenzioni e Raccomandazioni dell'ILO allo scopo di verificare quale sia l'effettivo grado di tutela della riservatezza del lavoratore garantito dalle fonti costituenti international labour standards in senso proprio.

Dal punto di vista metodologico, si è prescelto di procedere alla suddivisione dei risultati scaturiti dalla ricognizione delle suddette fonti per nuclei tematici.

In primo luogo, verrà esaminata la disciplina del trattamento dei dati personali dei *job applicant*s e dei *workers* ad opera delle agenzie per l'impiego private contenuta nella Convenzione n. 181 del 1997 e nella Raccomandazione n. 188 del 1997.

Il secondo nucleo tematico riguarderà la protezione dei dati relativi alla salute del lavoratore, considerato che le Convenzioni e Raccomandazioni in materia di salute e sicurezza sul luogo di lavoro contengono disposizioni riguardanti il trattamento degli *health data* (si vedano, tra le altre, le Convenzioni n. 124/1965 e la Raccomandazione n. 171/1985).

Di primario interesse, sempre con riferimento alla tutela della riservatezza dei dati sanitari, è anche la Raccomandazione su HIV e AIDS n. 200 del 2010, la quale, da un

lato, prevede il diritto a non rivelare il proprio stato di sieropositività, così da prevenire fenomeni discriminatori e di stigmatizzazione, dall'altro, incoraggia i lavoratori ad effettuare test su base volontaria e nel rispetto della *privacy*.

Successivamente, si esaminerà la protezione accordata dalle Convenzioni nn. 81 del 1947 e 129 del 1969 all'identità dei lavoratori che effettuano segnalazioni agli ispettori del lavoro.

Considerato che il timore dei lavoratori di subire ritorsioni rappresenta un disincentivo alle segnalazioni e, quindi, all'emersione di situazioni di irregolarità, viene stabilito che gli ispettori del lavoro "*dovranno considerare assolutamente confidenziale l'origine di qualsiasi reclamo che segnali loro un difetto nelle installazioni o un'infrazione alle disposizioni di legge e dovranno astenersi dal rivelare al datore di lavoro o al suo rappresentante che la visita di ispezione è stata effettuata in seguito ad un reclamo*" (art. 15, par. 1, lett. c), Convenzione n. 81/1947 e art. 20, par. 1, lett. c), Convenzione n. 129/1969).

Nelle predette Convenzioni, tuttavia, viene espressamente "*fatta riserva delle eccezioni che la legislazione nazionale potrebbe prevedere*". Pertanto, si indagherà sulla presenza all'interno dell'ordinamento nazionale di eventuali limitazioni alla tutela dell'identità del lavoratore autore di un reclamo agli organismi ispettivi, anche tenuto conto dell'elaborazione giurisprudenziale sul punto.

La sezione seguente sarà dedicata alla disciplina della privacy delle persone coinvolte in episodi di violenza o molestie sul luogo di lavoro prevista dalla Convenzione n. 190 del 2019 e dalla Raccomandazione n. 206 del 2019.

Nella seconda parte del presente lavoro saranno meglio affrontate le principali sfide globali connesse alla *data protection* nel mondo del lavoro, tra cui l'utilizzo dei dati personali dei lavoratori nel contesto dell'*algorithm-based management*[7], individuato nella Dichiarazione del Centenario e del Consiglio di Amministrazione come una delle priorità verso cui deve orientarsi l'azione dell'ILO. Ciò anche in ragione di alcune iniziative rilevanti che l'ILO sta intraprendendo in materia di tutela della privacy dei *platform workers*.

A tal proposito, si valorizzerà il lavoro di ricognizione e analisi delle fonti svolto nella

[7] All'impatto dell'*algorithm-based management* sul mondo lavoro è dedicato il *background paper* n. 9 dell'ILO e della Commissione Europea di S. BAIOCCO, E. FERNANDEZ-MACÍAS, U. RANI, A. PESOLE, *The Algorithmic Management of work and its implications in different contexts*, giugno 2022.

prima parte dell'elaborato allo scopo di stabilire se, in una prospettiva attualizzante, gli strumenti di cui dispone l'ILO siano idonei o meno a fronteggiare adeguatamente tali fenomeni. Successivamente, verranno svolte riflessioni sul possibile ruolo dell'ILO e fornite proposte operative in merito a possibili iniziative dell'Organizzazione Internazionale del Lavoro.

Infine, nelle conclusioni saranno ripresi i principali risultati a cui l'indagine svolta è pervenuta.

Capitolo I

Il Code of practice on the protection of workers' personal data

1. Code of practice on the protection of workers' personal data: finalità

Il capitolo dedicato alle fonti dell'ILO inerenti alla tutela della riservatezza dei lavoratori non può che partire dall'analisi del *Code of Practice on the protection of workers' personal data*[8], strumento privo di efficacia vincolante[9], ma che si propone come utile riferimento per *policy makers*, attori sindacali e per lo sviluppo di prassi virtuose all'interno dei luoghi di lavoro.

L'obiettivo del Codice ILO è quello di dettare una disciplina del trattamento dei dati personali che tenga conto delle peculiarità proprie del contesto lavorativo.

Infatti, al tempo dell'adozione del Codice, erano già state adottate normative sovranazionali generali in materia di *data protection*[10], le quali, tuttavia, non erano incentrate sul trattamento dei dati personali in ambito lavorativo.

Da qui la decisione del Consiglio di Amministrazione dell'ILO, adottata nella sessione n. 264 del novembre 1995, di indire la convocazione di un gruppo di ventiquattro esperti che, riunitosi a Ginevra dal 1° al 7 ottobre 1996, ha elaborato il Codice di Condotta[11].

---

[8] Per un'analisi completa del Codice di condotta cfr. S. P. EMILIANI, *Italia, OIL e protezione dei dati personali*, in L. MECHI-A. SITZIA (a cura di), *op. cit.*
Ampi cenni al Codice ILO sono presenti anche in A. SARTORI, *Il controllo tecnologico sui lavoratori: la nuova disciplina italiana tra vincoli sovranazionali e modelli comparati*, Torino, 2020; in F. HENDRICKX, *Protection of workers' personal data: General principles*, ILO Working paper n. 62, 5 maggio 2022 nonchè nel saggio del medesimo Autore, *Privacy and workplace monitoring in a global legal prerspective*, in C. PISANI-G. PROIA-A. TOPO, (a cura di), *Privacy e lavoro: la circolazione dei dati personali e i controlli nel rapporto di lavoro*, Milano, 2022.

[9] Come chiarito nella *Preface* del Codice ILO, "*the code does not replace national laws, regulations, international labour standards or other accepted standards*".

[10] Si sta facendo riferimento alla Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (c.d. Convenzione 108), alla Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (abrogata dal Reg. UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, c.d. GDPR) e alle Linee guida OCSE sulla tutela della vita privata e i flussi transfrontalieri di dati a carattere personale del 1980.

[11] L'obiettivo del Codice ILO, enunciato nel suo Preambolo, consiste nello sviluppo di "*data protection provisions which specifically address the use of workers' personal data in order to safeguard the dignity of workers, protect their privacy and guarantee their fundamental right to determine who may use which data for what purposes and under what conditions*".

Non vi è dubbio che il trattamento dei dati personali dei lavoratori presenti peculiarità che devono essere tenute in considerazione al fine di implementare un adeguato quadro regolatorio settoriale.

La prima criticità riguarda la caratterizzazione della relazione lavorativa quale rapporto di durata che richiede un continuo e costante trattamento di dati personali dei lavoratori[12], il quale può iniziare anche prima della formale instaurazione del rapporto di lavoro nella fase di selezione del personale e può continuare financo a seguito della cessazione della relazione lavorativa qualora risulti necessaria la conservazione di alcuni dati per adempiere a obblighi di legge o per precostituirsi mezzi di prova in eventuali futuri contenziosi con *ex* occupati.

Peraltro, frequentemente, datore di lavoro-titolare del trattamento e *worker* sono titolari di interessi antitetici per quanto concerne il flusso dei dati personali in quanto l'imprenditore è indotto a raccogliere la maggiore quantità possibile di informazioni, mentre il lavoratore vuole evitare la perdita di ogni spazio di riservatezza e libertà nel luogo di lavoro.

Pertanto, il trattamento dei dati personali dei lavoratori si caratterizza per la compresenza di interessi contrapposti, entrambi meritevoli di tutela, e, segnatamente, da un lato, l'interesse del datore di lavoro a organizzare efficacemente la propria attività produttiva, ad acquisire informazioni sulle attitudini dei propri collaboratori, a controllare e valutare l'esecuzione della prestazione lavorativa, dall'altro, l'interesse del lavoratore a mantenere privati determinati aspetti della propria vita e personalità e a svolgere la prestazione all'interno di una "dimensione lavorativa umana".

In questo conflitto tra esigenze contrapposte, il governo dei dati personali dei lavoratori gioca un ruolo sempre più cruciale.

Tuttavia, un equo contemperamento tra gli interessi implicati difficilmente può raggiungersi all'interno della relazione lavorativa, in assenza di un intervento riequilibratore esterno.

Ciò in quanto un'altra criticità del trattamento dei dati personali nel contesto lavorativo consiste nella particolare relazione che intercorre tra il titolare del trattamento e gli

[12] Nella Preface del Codice di condotta si legge che "*employers collect personal data on job applicants and workers for a number of purposes: to comply with law; to assist in selection for employment, training and promotion; to ensure personal safety, personal security, quality control, customer service and the protection of property*".

interessati.

Infatti, i dati oggetto di trattamento appartengono a candidati all'assunzione che mirano ad ottenere un'occupazione e a lavoratori in forza interessati al mantenimento dell'occupazione, cioè a soggetti che si trovano in una condizione di debolezza strutturale rispetto al datore di lavoro-titolare del trattamento.

Conseguentemente, i lavoratori, specie quelli caratterizzati da una accentuata posizione di debolezza economico-contrattuale, potrebbero essere indotti a cedere completamente il controllo sul flusso dei propri dati personali, così inaugurando un "circolo vizioso" capace di accrescere ulteriormente la loro posizione di assoggettamento nei confronti del datore di lavoro.

Infatti, l'accesso generalizzato ai dati personali dei lavoratori può accrescere considerevolmente i poteri datoriali[13].

Come ben espresso nel *preamble* del Commentario che accompagna il Codice di condotta "*the less, therefore, that the persons concerned know about who is processing which data for which purposes, the less they are able to assess their individual situation and to express and defend their interests: in short, they have difficulty in determining their own personal development. The quest for principles to govern the processing of personal data expresses, therefore, the need to protect human dignity*".

Ed è proprio per le ragioni appena espresse che l'ILO ha avvertito la necessità di adottare una regolamentazione settoriale del trattamento dei dati personali in ambito lavorativo, così da meglio prevenire il rischio che i lavoratori-interessati, a causa della loro posizione di subalternità, perdano completamente il controllo sui propri dati personali.

2. Code of practice on the protection of workers' personal data: scelte tecnico-redazionali

Il gruppo di esperti si è attenuto a precise direttrici tecnico-redazionali che costituiscono espressione alcune scelte di fondo operate nell'elaborazione del *Code of practice*.

[13] Nel Preambolo del Commentario viene spiegato come "*the gathering of a large number of data and the many different uses to which they are put not only multiply the risk of false or misunderstood information, but also permit close monitoring of the persons concerned and intensify tendencies to influence or even to manipulate their behaviour*".

Innanzitutto, il Codice ILO mira a fare proprio il patrimonio normativo già esistente, procedendo ad adattarlo in base alle peculiarità e criticità che caratterizzano il trattamento dei dati personali all'interno del contesto lavoristico.

Tale scelta si manifesta nella circostanza che il Codice di condotta recepisce terminologia e principi propri di strumenti internazionali generali di *data protection* allora esistenti quali la Direttiva 95/46/CE (oggi sostituita dal Regolamento UE 2016/679, c.d. GDPR)[14].

In secondo luogo, il gruppo di esperti si prefigge di porre una regolamentazione esaustiva di tutti i possibili trattamenti di dati personali effettuati nel contesto lavorativo. Per tale ragione, il Codice di condotta viene strutturato in modo da ricomprendere all'interno del proprio ambito di applicazione soggettivo non solo i lavoratori pubblici e privati[15] in forza, ma anche i lavoratori cessati e i candidati all'assunzione[16].

Infine, il Codice di condotta si prefigge l'obiettivo di non limitarsi a fronteggiare le più avanzate tecniche di trattamento dei dati allora conosciute, ma di essere in grado di adattarsi all'evoluzione tecnologica senza perdere la propria di rilevanza.

A tale scopo, il Codice ILO, piuttosto che fornire definizioni puntuali e precise, privilegia l'utilizzo di espressioni ampie, maggiormente adeguate a ricomprendere all'interno del proprio alveo regolativo anche fattispecie e sviluppi tecnologici non ancora realizzatisi[17].

---

[14] È lo stesso Commentario, p. 9, a chiarire che "*the terminology used in the code relies upon terms generally accepted and used in international instruments such as the OECD Guidelines on data protection, the Data Protection Convention of the Council of Europe and the EU Directive on data protection, as well as in national data protection laws"*.

[15] Ai sensi dell'art. 4, par. 1, lett. b), il Codice sia applica "*to the public and private sectors*".

[16] Infatti, l'art. 3, par. 3, specifica che "*the term worker include any current or former worker or applicant for employment*".
Il Commentario spiega che la scelta di utilizzare una definizione ampia del termine *worker* deriva dalla considerazione per cui "*employers tend to conserve at least some of the data, for example to furnish proof that a certain person was employed during a specific period of time or to provide information on former employees. In the course of recruitment procedures employers also store and retrieve data concerning job applicants*".

[17] In tal senso, è emblematica la definizione di *processing* di cui all'art. 3, par. 2, all'interno della quale - oltre a "*collection, storage, combination, communication*" – viene ricompreso, attraverso l'utilizzo di una clausola generale di chiusura, anche "*any other use of the personal data*".
Come spiegato nel commentario, "*the code covers every form of processing … any attempt to lay down rules for one specific form of processing would therefore not be in the best interest of workers*".
Allo stesso modo, con una formula aperta, all'interno della nozione di "*monitoring*" viene ricompreso "*any other method of surveillance*".

3. Code of practice on the protection of workers' personal data: principi generali

Prima di procedere a dettare regole più specifiche, il Codice di condotta individua i principi fondamentali che devono governare il trattamento dei dati personali dei lavoratori.

In linea con tecnica redazionale di valorizzazione del patrimonio normativo esistente di cui si è dato conto nel paragrafo che precede, nella sostanza, i principi generali individuati dal Codice ILO sono i medesimi principi che si ritrovano nell'attuale art. 5 del GDPR[18] - ossia i canoni di liceità, correttezza, sicurezza, minimizzazione e esattezza dei dati, di limitazioni delle finalità del trattamento e del periodo di conservazioni dei dati - con alcuni adattamenti giustificati dalla specificità del contesto in cui viene eseguito il trattamento.

Per quanto concerne gli adattamenti operati, il Codice provvede a contestualizzare il c.d. principio di finalità, prevedendo che i dati debbano essere trattati solo per ragioni "*directly relevant to the employment of the worker*[19]" (art. 5, par. 1)[20].

---

[18] I medesimi principi contenuti nell'attuale art. 5 del GDPR si ritrovano nell'art. 6, comma 1, della previgente Direttiva 95/46/CE, rubricato, "*Principi relativi alla qualità dei dati*" ai sensi del quale "*gli Stati membri dispongono che i dati personali devono essere:*
a) trattati lealmente e lecitamente;
b) rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità. Il trattamento successivo dei dati per scopi storici, statistici o scientifici non è ritenuto incompatibile, purché gli Stati membri forniscano garanzie appropriate;
c) adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati;
d) esatti e, se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare i dati inesatti o incompleti rispetto alle finalità per le quali sono rilevati o sono successivamente trattati, cancellati o rettificati;
e) conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati. Gli Stati membri prevedono garanzie adeguate per i dati personali conservati oltre il suddetto arco di tempo per motivi storici, statistici o scientifici".

[19] Il Commentario giustifica la scelta di utilizzare la formula generale e ampia di "*reasons directly relevant to the employment of the worker*" - senza indicare, nemmeno a titolo identificativo, le singole finalità che possono giustificare il trattamento dei dati dei lavoratori, pur nella consapevolezza che "*the criterion chosen might at first seem too vague*" - in considerazione della circostanza che "*in practice attempts to list them are simply futile, unless the enumeration is restricted to a few data such as name, age, address and sex, the processing of which does not create problems at least as long as it is for strictly internal use by the employer and is consistent with the law*".

[20] L'art. 5, par. 1, del Codice ILO rappresenta la declinazione giuslavoristica del c.d. principio di limitazione della finalità enunciato dal vigente art. 5, comma 1, lett. b), GDPR, in forza del quale i dati devono essere "*raccolti per finalità determinate, esplicite e legittime*".

Pertanto, mentre generalmente è possibile effettuare un trattamento di dati personali per qualsivoglia finalità determinata, esplicita e legittima, la possibilità di trattare dati personali dei lavoratori risulta maggiormente circoscritta.

Infatti, *condicio sine qua non* del trattamento è la presenza di ragioni direttamente pertinenti con l'occupazione del lavoratore, risultando, *a contrario*, precluso al datore di lavoro il trattamento di dati personali di prestatori e candidati per finalità diverse[21].

Tuttavia, per alcune categorie particolari di dati personali, il Codice contiene una maggiore specificazione delle situazioni in cui i dati possono essere legittimamente trattati.

Infatti, il *Code of practice* stabilisce il divieto relativo di trattare determinati dati che espongono il lavoratore ad un elevato pericolo di utilizzo improprio e/o discriminatorio delle informazioni, salvo che per specifiche finalità tassativamente individuate dal Codice stesso.

In sostanza, il Codice ILO stabilisce che, in via generale, non sussistono ragioni connesse alla gestione del rapporto di lavoro capaci di giustificare l'acquisizione e l'utilizzo di alcune informazioni sensibili relative al lavoratore, a meno che non ricorrano speciali condizioni derogatorie.

E così le informazioni relative a vita sessuale, convinzioni politiche, religiose e condanne penali non possono essere trattate, salvo che "*in exeptional circumstances ... if the data are directly relevant to an employment decision and in conformity with national legislation*" (art. 6, par. 5).

Invece, i dati relativi all'appartenenza e all'attività sindacale non possono essere trattati, a meno che ciò non sia consentito o imposto da una legge nazionale o da un contratto collettivo (art. 6, par. 6).

---

[21] Sempre in relazione al *finality principle*, viene, poi, stabilito che i dati personali debbano essere tendenzialmente utilizzati esclusivamente per la finalità per i quali sono stati originariamente raccolti, non potendo, invece, venire riutilizzati per finalità incompatibile.
Si tratta di un principio sancito anche dall'art. 5, comma 1, lett. b), GDPR e, ancor prima, dall'art. 6, comma 1, lett. b) dell'abrogata 95/46/CE, a norma del quale "*gli Stati membri dispongono che i dati personali devono essere … rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità*".
Il Codice ILO, tuttavia, arricchisce tale principio attraverso la precisazione per cui il datore di lavoro, nel caso in cui riutilizzi i dati per una finalità compatibile con quella originaria, deve adottare tutte le misure necessarie ad evitare ogni "*misinterpretation*" causata dal cambiamento di contesto.

Infine, i dati relativi alla salute non possono essere oggetto di trattamento se non in conformità alla legislazione nazionale, al segreto medico e ai principi generali di salute e sicurezza sul lavoro e qualora sia necessario per il conseguimento di tre scopi alternativi specificamente prestabiliti: per valutare l'idoneità del lavoratore allo svolgimento delle proprie mansioni; per adempiere ad obbligazioni in materia di salute e sicurezza sul lavoro; per ottenere la concessione di prestazioni sociali (art. 6, par. 7).

Qualora il datore di lavoro richieda comunque al lavoratore informazioni la cui raccolta è preclusa o può determinare effetti discriminatori, al lavoratore è riconosciuto il diritto di fornire una risposta imprecisa o incompleta, senza correre il rischio di incorrere in alcuna sanzione disciplinare (art. 6, par. 8).

Tale soluzione risulta particolarmente ingegnosa, consentendo al prestatore di sottrarsi impunemente alla richiesta datoriale volta ad ottenere informazioni a cui non avrebbe diritto di accedere.

Pertanto, a titolo di esempio, in fase di colloquio preassuntivo, il candidato a cui sia richiesto di indicare la propria appartenenza sindacale potrebbe scegliere sia di non rispondere alla domanda illegittima, però con il rischio di indispettire il *recruiter*, sia di fornire informazioni imprecise o incomplete.

Nel diverso caso in cui il lavoratore per errore fornisca dati personali protetti, malgrado gli stessi non gli siano stati richiesti dal datore di lavoro, quest'ultimo non dovrebbe comunque trattare tali informazioni (art. 6, par. 9).

Infatti, il c.d. principio di minimizzazione impone che dati non pertinenti o eccedenti rispetto a quanto necessario per il conseguimento della finalità di trattamento non possano essere legittimamente utilizzati, nemmeno nel caso in cui sia stato lo stesso lavoratore a fornirli.

Un ulteriore adattamento di principi fondamentali della *data protection regulation* riguarda il c.d. principio di limitazione del periodo di conservazione dei dati.

Infatti, la regola che impone la conservazione dei dati personali dei lavoratori solamente per il tempo necessario a soddisfare la specifica finalità per la quale i dati sono raccolti può essere oggetto di deroga al ricorrere di tre specifiche ipotesi: quando un lavoratore voglia rimanere incluso all'interno di una lista di possibili canditati per un periodo di tempo definito; se la conservazione dei dati personali è imposta al datore di lavoro dalla

legislazione interna; se il datore di lavoro o il lavoratore richiedano la conservazione di dati personali per un contenzioso legale (art. 8, par. 5).

All'interno dei principi generali, viene altresì espresso quello che, con terminologia corrente, verrebbe indicato come *human in command approach*, approccio rispetto all'evoluzione tecnologica che mira al mantenimento del controllo umano sui sistemi automatizzati utilizzati all'interno dell'organizzazione imprenditoriale[22].

Infatti, innanzitutto, è previsto che le decisioni riguardanti i lavoratori non dovrebbero essere adottate esclusivamente sulla base di un trattamento automatizzato dei loro dati personali (art. 5, par. 5)[23].

Ne deriva che gli *output* di trattamenti automatizzati di dati personali dei lavoratori (ovviamente legittimamente raccolti) potranno essere valutati al fine di assumere decisioni che impattano sulla loro sfera personale, ma è sempre necessario che l'assunzione della decisione finale sia riservata a un supervisore umano, l'unico in grado di considerare compiutamente tutte le circostanze rilevanti del caso concreto che possano influire sul risultato e/o sull'interpretazione dei dati.

Similmente, il Codice prevede che i dati personali raccolti da strumenti tecnologici non dovrebbero essere gli unici fattori considerati nella valutazione della *performance* dei lavoratori (art. 5, par. 6).

Ancora una volta, quello che si vuole evitare è che l'attività del lavoratore sia ridotta a meri dati, dovendo le informazioni sempre passare attraverso "uno sguardo umano" che possa fornire una valutazione contestualizzata delle informazioni raccolte.

A titolo di esempio, dai dati forniti da un macchinario potrebbe risultare un calo quantitativo della produttività che, tuttavia, non implica automaticamente un peggioramento della *performance* del lavoratore giacché quei dati potrebbero spiegarsi con la speciale difficoltà insita in alcune operazioni ad alto valore aggiunto realizzate dal prestatore o con problematiche della strumentazione o dell'organizzazione produttiva non imputabili al prestatore.

---

[22] Lo *human in command approach*, sempre più centrale all'interno del dibattito interno all'ILO, è richiamato nel paper Global Commission on the future of work, *Work for a brighter future*, ILO, Ginevra 2019, che propone una "*human-centred agenda*" basata anche su un "*human-in-command approach to technology ... that ensures that the final decisions affecting work are taken by human beings, not algorithms*" (v. pagg. 13 e 43).

[23] Il Codice, quindi, non preclude il ricorso di procedure automatizzate, ma richiede che queste fungano da supporto meramente ausiliario rispetto all'adozione della decisione.

Infine, risulta di estrema rilevanza anche il principio secondo cui il trattamento di dati personali non deve produrre effetti discriminatori (5.10)[24].

Tale previsione, in una prospettiva attualizzatrice, potrebbe assumere un potenziale applicativo più ampio rispetto a quello preventivato dal gruppo di esperti che ha elaborato il Codice di condotta in ragione dell'emersione del fenomeno della c.d. discriminazione algoritmica[25].

[24] Il Commentario, con un maggiore grado di precisazione rispetto alla formulazione dell'art. 5, par. 10, specifica che il principio si riferisce sia alle discriminazioni dirette sia alle discriminazioni indirette e riguarda discriminazioni di tipo individuale o collettivo.

[25] La discriminazione algoritmica, termine con cui si identifica l'*output* discriminatorio generato da un trattamento automatico di dati personali attraverso algoritmi, presenta caratteristiche del tutto peculiari e, per certi versi, paradossali rispetto alla discriminazione "umana".
Infatti, sebbene le decisioni con effetti discriminatori scaturenti dalle elaborazioni di dati operate da un algoritmo "mal costruito" siano seriali, in quando destinate a ripetersi continuativamente fino alla correzione del *bias*, tuttavia, malgrado il carattere reiterato dei trattamenti discriminatori, potrebbe essere estremamente difficile assumere consapevolezza dell'esistenza delle discriminazioni a causa della complessità e dell'opacità di funzionamento dell'algoritmo.
Per quanto riguarda l'ordinamento nazionale, emblematica è l'ordinanza del Tribunale di Bologna del 31 dicembre 2020 che ha ravvisato la natura discriminatoria del funzionamento dell'algoritmo "*Frank*" utilizzato dalla compagnia di *food delivery Deliveroo Italy S.r.l.*
Nel caso di specie è stato ravvisato che il *rating* dei riders, da cui dipendeva la possibilità di prenotare le sessioni di lavoro preferite con priorità rispetto ai ciclo-fattorini con punteggi inferiori, diminuiva in caso di mancata cancellazione del turno prenotato via *app* almeno ventiquattro ore prima del suo inizio.
Tuttavia, in questo modo, un rider che aderiva ad uno sciopero rischiava di veder peggiorare le proprie statistiche e, conseguentemente, di perdere i vantaggi derivanti dall'attribuzione di un *rating* più elevato.
I riders dovevano quindi scegliere se aderire allo sciopero, riducendo le proprie *chances* di accedere prioritariamente alle fasce di lavoro più remunerative oppure non partecipare allo sciopero.
Pertanto, le modalità di funzionamento dell'algoritmo producevano l'effetto discriminatorio di sfavorire i lavoratori a causa del fattore protetto rappresentato dalla propria appartenenza e attività sindacale.
In merito alla tematica delle discriminazioni algoritmiche e all'ordinanza del Tribunale di Bologna del 31 dicembre 2020 cfr., *ex multis*, C. ALESSI, *Lavoro tramite piattaforma e divieti di discriminazione nell'UE*, in C. ALESSI, M. BARBERA, L. GUAGLIANONE (a cura di), *Impresa, lavoro e non lavoro nell'impresa digitale*, Cacucci, 2019; M.V. BALLESTRERO, *Ancora sui rider. La cecità discriminatoria della piattaforma*, in *Labor*, 1/2021; A. PERULLI, *La discriminazione algoritmica:* brevi note introduttive a margine dell'ordinanza del Tribunale di Bologna, in Lavoro Diritti Europa, 1/2020; G. GAUDIO, *La Cgil fa breccia nel cuore dell'algoritmo di Deliveroo: è discriminatorio*, nota a Tribunale Bologna 31/12/2020, in *RIDL*, 2/2021, pp. 175-195; E. FALLETTI, *La discriminazione algoritmica: una prospettiva comparata*, Giappichelli, 2023 e della medesima Autrice, *Algoritmi: la discriminazione non è uguale per tutti*, in *Lavoro Diritti Europa*, 2/2023; G. GAUDIO, *Le discriminazioni algoritmiche*, in *Lavoro Diritti Europa*, 1/2024; E. LACKOVÀ, *Opacità degli algoritmi e decreto trasparenza: il sindacato fa la sua parte*, in *RIDL*, 2/2023, pp. 367-379; R. XENIDIS, *Tuning EU equality law to algorithmic discrimination: three pathways to resilience*, in *Maastricht Law Journal of European and Comparative Law*, vol. 27, 2020.

4. Code of practice on the protection of workers' personal data: rimedi individuali e collettivi

Al fine di garantire il rispetto e l'effettiva applicazione delle proprie previsioni, il Codice di Condotta introduce un sistema duale di tutelata, riconoscendo, da un lato, diritti individuali esercitabili dai lavoratori *uti singuli*, dall'altro, diritti di natura collettiva in favore delle rappresentanze sindacali dei lavoratori.

La *ratio* dell'introduzione del duplice piano di tutela risiede nella circostanza che i diritti individuali richiedono, per il loro esercizio, l'adozione di un comportamento attivo del lavoratore, in assenza del quale le prerogative sono destinate a rimanere "lettera morta". Pertanto, in ragione del rischio che i lavoratori, a causa del *metus* nei confronti del datore di lavoro, si astengano dall'esercizio delle proprie prerogative, il Codice OIL ritiene opportuno attribuire specifici diritti altresì alle rappresentanze sindacali dei lavoratori, così da poter esercitare al meglio la loro funzione di contropotere collettivo.

Per quanto concerne il regime di tutela, il Codice innanzitutto contempla un diritto di informazione al contempo individuale e collettivo particolarmente ampio, prevedendo che non solo i singoli lavoratori, ma anche le loro rappresentanze dovrebbero essere regolarmente informate di qualsiasi processo di raccolta dei dati, delle norme che lo regolano e dei diritti di cui sono titolari (art. 5, par. 8).

Anche in questo caso, il Codice ILO, nonostante costituisca un documento oramai risalente nel tempo, grazie all'utilizzo di espressioni generali capaci di adattarsi all'evoluzione tecnologica, dimostra un potenziale applicativo estremamente rilevante anche nel contesto attuale.

Infatti, il dovere di informare lavoratori e rappresentanze in ordine alle "*rules that govern that process*" potrebbe rivelarsi idoneo a ricomprendere, in via interpretativa, anche il dovere di spiegare le logiche di funzionamento di trattamenti di dati personali effettuati dall'impresa attraverso il ricorso ad algoritmi.

I lavoratori, oltre al descritto diritto di informazione, sono titolari anche di un'ulteriore serie di prerogative.

L'art. 11, par. da 1 a 8, disciplina il diritto dei lavoratori di accedere, esaminare e estrarre copia dei dati che lo riguardano, anche nel caso in cui siano trattati attraverso sistemi automatizzati (c.d. diritto di accesso).

Nell'esercizio del diritto di accesso il lavoratore ha la facoltà di farsi assistere da un rappresentante sindacale o da un collega o, in caso di accesso a dati sanitari, da un professionista da lui prescelto.

Tale previsione, evidentemente, mira a che l'esercizio del diritto di accesso possa avere un'utilità effettiva per il lavoratore, il quale potrebbe essere privo delle competenze necessarie per verificare la correttezza e la conformità dei propri dati personali oggetto di trattamento.

Al lavoratore sono altresì riconosciuti il diritto di chiedere la cancellazione dei dati personali trattati in violazione delle regole introdotte dal Codice nonché la rettifica dei propri dati personali in caso di inesattezza o incompletezza degli stessi (art. 11, par. 9).

In tal caso, il datore di lavoro dovrà attivarsi per comunicare l'avvenuta cancellazione o rettifica agli altri soggetti a cui siano stati precedentemente forniti i dati personali inesatti o incompleti, salvo che il lavoratore non lo ritenga necessario.

Il Codice ILO si occupa anche di regolare le conseguenze dell'istanza avanzata dal lavoratore per ottenere la rettifica di giudizi e valutazioni che lo riguardano.

Essendo i giudizi e le valutazioni ontologicamente connotate da una ineliminabile componente soggettiva, non pare possibile considerare i giudizi formulati sul lavoratore non esatti o incompleti, salvo nel caso in cui il giudizio espresso faccia riferimento o si basi su informazioni inveritiere.

Pertanto, al lavoratore non viene attribuito un vero e proprio diritto alla cancellazione o alla rettifica dei *judgmental data*.

Il rimedio individuato dal Codice ILO invece consiste nell'attribuzione al lavoratore del diritto di esprimere il proprio punto di vista in una dichiarazione da conservare insieme al giudizio (art. 11.12)

La statuizione in esame potrebbe ritrovare un rinnovato vigore come possibile mezzo di tutela dei lavoratori rispetto ai c.d. sistemi reputazionali di *customer satisfaction*.

Sempre più spesso imprese e piattaforme digitali raccolgono il gradimento espresso dal cliente rispetto al servizio o l'assistenza offerta dal lavoratore.

In questo modo, l'azienda riesce ad individuare i lavoratori giudicati come i "migliori" dalla clientela e, allo stesso tempo, a conoscenza di eventuali problemi o disfunzioni dei servizi offerti.

Ebbene, l'ampia formulazione adottata dal Codice ILO potrebbe consentire la

riconduzione dei *feedback* espressi dai clienti nel novero dei *judgmental data* relativi al lavoratore.

Se così fosse, i lavoratori sarebbero titolari del diritto a poter esprimere la propria posizione, così da contestualizzare o replicare a valutazioni e/o recensioni dei clienti non condivise.

Ciò che, peraltro, già avviene rispetto a sistemi reputazionali dei datori di lavoro come l'applicazione *Trip Advisor*, la quale consente ai ristoratori di rispondere a recensioni e critiche dei clienti esprimendo il proprio punto di vista, talvolta diametralmente opposto rispetto a quello del fruitore del pasto.

Il Codice ILO, oltre all'attribuzione del "diritto di replica", prevede che lo *statement* del lavoratore sia in tutte le successive comunicazioni dei dati personali, salvo diverso accordo tra le parti (art. 11, par. 12).

Da ciò potrebbe derivare che, qualora il giudizio o la valutazione del cliente sia destinata a rimanere o circolare *on line*, allo stesso modo anche la replica del lavoratore dovrebbe sempre "seguire" il *feedback* del cliente in modo che anche i terzi possano "farsi la loro opinione" sulle contrapposte letture dei fatti.

Per quanto concerne i *collective rights*, il Codice ILO valorizza la partecipazione attiva del sindacato nelle diverse fasi dei trattamenti.

Innanzitutto, il Codice richiede che i rappresentanti sindacali, insieme ai lavoratori, siano coinvolti dal datore di lavoro nell'individuazione di procedure e pratiche di trattamento dei dati rispettose della privacy (art. 5, par. 11).

Ai sensi dell'art. 12, par. 2, viene, inoltre, riconosciuto che i rappresentanti dei lavoratori, in conformità alla legislazione e alle prassi nazionali, debbano essere informati e consultati in merito all'introduzione o alla modifica di sistemi automatizzati che trattano i dati personali dei lavoratori nonché prima dell'introduzione di qualsiasi tipo di monitoraggio elettronico del comportamento dei lavoratori sul luogo di lavoro. Tale disposizione deve essere coordinata con quanto stabilito dall'art. 5, par. 8, che, come visto *supra*, riconosce un diritto di informazione generalizzato e ampio in favore dei rappresentati sindacali dei lavoratori.

Tali disposizioni, *prima facie*, sembrerebbero presentare un ambito di applicazione parzialmente sovrapponibile.

Infatti, per un verso, il Codice riconosce il diritto delle rappresentanze sindacali di essere informate di qualsivoglia tipologia di trattamento, per un altro, viene attribuito il diritto di informazione e consultazione sull'introduzione di sistemi automatizzati e di monitoraggio dei prestatori, che altro non sono che sistemi che eseguono trattamenti di dati personali.

L'interpretazione che sembra scaturire dal combinato disposto delle due disposizioni è la seguente: il datore di lavoro deve informare le rappresentanze di qualsivoglia trattamento dei dati personali dei lavoratori e, in caso di trattamento da realizzarsi attraverso l'introduzione o la modifica di sistemi automatizzati e di monitoraggio, al dovere di informazione si aggiunge quello di preventiva consultazione delle rappresentanze.

Pur valorizzando il ruolo delle rappresentanze sindacali - le quali, in termini metaforici, assumono un ruolo di controllo sul rispetto della *privacy* in azienda analogo a quello attribuito al Rappresentante dei Lavoratori per la Sicurezza (RLS) in tema di sicurezza sul lavoro - tuttavia, il Codice non sembra spingersi sino ad affermare un principio di necessaria codeterminazione sindacale degli strumenti automatizzati e di monitoraggio[26], essendo riconosciuto alle rappresentanze un mero diritto di consultazione.

5. Code of practice on the protection of workers' personal data: controlli occulti

Uno degli argomenti centrali nell'ambito del dibattito giuslavoristico è rappresentato dai controlli occulti.

Con tale espressione si indicano quei controlli effettuati dal datore di lavoro all'insaputa dei prestatori attraverso la raccolta di informazioni in assenza di preventiva informazione ai lavoratori circa l'esistenza e le modalità dei controlli.

La tematica è stata oggetto di un lungo dibattito giurisprudenziale sia a livello nazionale che comunitario che, attualmente, sembra essersi definitivamente assestato.

[26] Pertanto, *il Code of practice* non sembra richiedere che, prima di introdurre tali sistemi, l'imprenditore debba raggiungere un accordo sindacale o, in mancanza, ottenere l'autorizzazione organo pubblico tecnico e indipendente, come invece imposto nell'ordinamento nazionale dall'art. 4, comma 1, Statuto dei Lavoratori.
Ciò a meno che non si voglia ravvisare un vero e proprio diritto di codeterminazione in capo ai lavoratori e alle rappresentanze sindacali nella previsione, in vero assai generica, di cui all' art. 5, par. 11, ai sensi della quale "*employers, workers and their representatives should cooperate in protecting personal data and in developing policies on workers' privacy consistent with the principles in this code*".

Infatti, da un lato, la Corte Europea dei Diritti dell'Uomo si è pronunciata sui controlli occulti nella nota sentenza López Ribalda e altri c. Spagna (C. EDU 17 ottobre 2019, ricorsi n. 1874/13 e 8567/13), dall'altro, a livello nazionale, la Corte di Cassazione sembra aver definitivamente chiarito presupposti e limiti di legittimità dei controlli occulti a partire dalla sentenza 22 settembre 2021, n. 25732, la quale sembra aver inaugurato un orientamento destinato a divenire tralatizio.

Ebbene, la questione dei controlli occulti è affrontata anche all'art. 6, par. 14, del *Code of practice*.

Nello specifico, in ossequio al principio di trasparenza, la citata previsione, innanzitutto, prevede che, qualora i lavoratori siano monitorati, questi dovrebbero essere informati in anticipo delle ragioni, tempi, metodi e tecniche utilizzate nonché dei dati raccolti e il datore di lavoro "*must minimize the intrusion on the privacy of workers*".

Pertanto, il Codice ILO non sembra prevedere un divieto di utilizzo di strumenti aventi la specifica finalità di controllare l'esecuzione della prestazione lavorativa, richiedendo, però, al datore di lavoro che intenda avvalersene, di essere trasparente e di minimizzare l'impatto sulla privacy dei lavoratori[27].

Tuttavia, il Codice, individua due situazioni, da considerarsi tassative ed alternative, in presenza delle quali è possibile ricorrere al "*secret monitoring*". I controlli occulti sono, infatti, ammessi nei casi in cui sia consentito dalla legislazione nazionale ("*if it is in conformity with national legislation"*) oppure qualora vi sia un sospetto ragionevolmente fondato di perpetrazione di reati o altri gravi illeciti ("*if there is suspicion on reasonable grounds of criminal activity or other serious wrongdoing*").

A questo punto, si ritiene di particolare interesse operare un confronto tra la soluzione suggerita nel 1997 dall'ILO e gli approdi giurisprudenziali della Corte Edu e della Corte di Cassazione.

Per quanto concerne la giurisprudenza della Corte Europea dei Diritti dell'Uomo, la sentenza López Ribalda e altri v. Spagna (C. EDU 17 ottobre 2019, ricorsi n. 1874/13 e 8567/13), punto di riferimento in *subiecta materia*, è scaturita da un ricorso presentato alla Corte Edu da un gruppo di lavoratori spagnoli di un supermercato licenziati dopo

[27] È di questa opinione anche A. SARTORI, *op. cit.*, p. 5, la quale rileva come "*esso* [il controllo tecnologico sui lavoratori] *è, dunque, in linea di principio consentito, ma assoggettato a rigorose condizioni*".

essere stati ripresi mentre rubavano da telecamere segretamente installate dal datore di lavoro.

I ricorrenti lamentavano la violazione del loro diritto alla tutela della vita privata sancito dall'art. 8 CEDU in ragione della mancanza di trasparenza del datore di lavoro che li aveva ripresi senza il loro consenso e a loro totale insaputa in assenza di un'informativa preventiva e chiara circa l'esistenza dei controlli (c.d. *warning*).

Il riferimento è, evidentemente, ai principi generali di trasparenza e correttezza sanciti anche dall'art. 5, comma 1, lett. a, GDPR, ai sensi del quale i dati personali devono essere trattati in modo "*corretto e trasparente nei confronti dell'interessato*" (principio della c.d. *prior information*).

La Grand Chamber, nel caso di specie, ponendosi in continuità con l'orientamento espresso nella sentenza Kopke c. Germania (C. EDU 5 ottobre 2010, ricorso n. 420/07), ha precisato come, in presenza di specifici requisiti e cautele, possa prescindersi dalla preventiva informazione ai lavoratori, senza che, per ciò solo, sia ravvisabile una violazione dell'art. 8 CEDU.

Infatti, la sentenza ha riconosciuto la possibilità di effettuare controlli realizzati all'insaputa dei lavoratori qualora il datore di lavoro abbia un ragionevole sospetto circa la commissione di condotte illecite, sempre che il monitoraggio occulto avvenga nel rispetto dei principi di proporzionalità e non eccedenza[28].

Per quanto concerne la giurisprudenza domestica, la Corte di Cassazione, con la sentenza n. 25732 del 22 settembre 2021, est. Raimondi[29], ha adottato una posizione in materia di c.d. controlli tecnologici difensivi che, allo stato, sembra destinata a divenire

---

[28] Non è, quindi, possibile, anche qualora sussista una fondata *notitia criminis*, attivare controlli occulti generalizzati, estremamente pervasivi e continuativi, pena la violazione dei predetti principi.
Nel caso di specie, il controllo, seppur occulto, è stato ritenuto proporzionato dalla Corte EDU in quanto il gestore del supermercato aveva agito sulla base di un ragionevole sospetto di perpetrazione di condotte appropriative di beni aziendali da parte dei dipendenti derivante dall'aver riscontrato discrepanze tra le scorte di magazzino e gli incassi di fine giornata; le riprese dei furti provenivano da telecamere installate all'insaputa dei lavoratori *ex post* solo in un momento successivo rispetto a quando era sorto il fondato sospetto di illecito; l'attività di sorveglianza era risultata proporzionata giacché il controllo è stato limitato solo alle aree prossime alle casse attraverso operazioni di videosorveglianza cessate dopo dieci giorni al momento del raggiungimento dello scopo di identificazione dei responsabili; nessun'altra misura alternativa poteva essere efficacemente adottata.

[29] Per un commento della citata sentenza si rinvia ai contributi di V. NUZZO, *Sulla sopravvivenza dei controlli c.d. difensivi dopo la riscrittura dell'art. 4 St. Lav.*, in *Riv. it. dir. lav.*, 2022, n. 1; L. DI PAOLA, *Sopravvivenza dei controlli c.d. "difensivi" dopo la modifica dell'art. 4 st. lav.*, in IUS Lavoro, 30 settembre 2021; C. COLAPIETRO-A. GIUBILEI, *Controlli difensivi e tutela dei dati del lavoratore: il nuovo punto della Cassazione*, in *Labour & Law Issues*, V, 7, 2021, n. 2.

giurisprudenza consolidata, mettendo il punto – almeno a livello giurisprudenziale – sull'intenso dibattito in ordine alla legittimità dei controlli occulti.

Nel contesto nazionale, è stato, infatti, a lungo dibattuto se il datore di lavoro, in determinate circostanze e con specifiche cautele, potesse installare apparecchiature di controllo a distanza senza ottenere il previo accordo sindacale o l'autorizzazione amministrativa prevista dall'art. 4, Stat. Lav. e senza dover preavvertire i lavoratori[30].

La Suprema Corte, con la citata sentenza, emanata sulla base dell'attuale formulazione della norma statutaria, ha chiarito che "*sono consentiti i controlli anche tecnologici posti in essere dal datore di lavoro finalizzati alla tutela di beni estranei al rapporto di lavoro o ad evitare comportamenti illeciti, in presenza di un fondato sospetto circa la commissione di un illecito, purché sia assicurato un corretto bilanciamento tra le esigenze di protezione di interessi e beni aziendali, correlate alla libertà di iniziativa economica, rispetto alle imprescindibili tutele della dignità e della riservatezza del lavoratore, sempre che il controllo riguardi dati acquisiti successivamente all'insorgere del sospetto*".

La sentenza della Suprema Corte individua quindi in maniera specifica i presupposti per valutare la legittimità del datore di lavoro di attuare controlli al di fuori dei vincoli posti dall'art. 4, Stat. Lav.

È innanzitutto richiesto che l'iniziativa datoriale sia mirata ed abbia la finalità specifica di accertare determinati comportamenti illeciti.

Utilizzando la terminologia della Cassazione è necessario, cioè, che si tratti di controlli difensivi in senso stretto[31] "*diretti ad accertare specificamente condotte illecite ascrivibili - in base a concreti indizi - a singoli dipendenti*".

---

[30] Come noto – a seguito della riscrittura dell'art. 4 Stat. lav., operata dall'art. 23, d.lgs. n. 151/2015, con la quale il legislatore ha espressamente inserito tra le esigenze che possono giustificare l'introduzione di strumenti "*dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori"* quelle di "*tutela del patrimonio aziendale"* – dottrina e giurisprudenza si sono poste la questione se i controlli difensivi siano stati definitivamente attratti nell'ambito di applicazione della citata disposizione, ovvero se sia tutt'ora possibile affermare l'esistenza di controlli situati all'esterno del perimetro applicativo dell'art. 4 Stat. lav.

Per un approfondimento in ordine alle principali argomentazioni avanzate in dottrina a sostegno dell'una e dell'altra tesi si rinvia a V. MAIO, *I controlli difensivi e la tutela del patrimonio aziendale,* in C. PISANI-G. PROIA-A. TOPO, (a cura di), *Privacy e lavoro: la circolazione dei dati personali e i controlli nel rapporto di lavoro,* Milano, 2022 nonché ad A. BELLAVISTA, *Controlli tecnologici e privacy del lavoratore,* in A. BELLAVISTA-R. SANTUCCI (a cura di), *Tecnologie digitali, poteri datoriali e diritti dei lavoratori,* Torino, 2022.

È, poi, richiesto che l'iniziativa datoriale sia assunta sulla base di un ragionevole sospetto circa la perpetrazione di condotte illecite.

Inoltre, il controllo deve basarsi esclusivamente su dati e informazioni raccolte *ex post* solo a partire dal momento in cui è sorto il ragionevole sospetto circa la commissione dell'illecito da parte di uno o più dipendenti.

In sostanza, la Cassazione, al sorgere del ragionevole sospetto, attribuisce al datore di lavoro la possibilità di svolgere indagini all'insaputa dei lavoratori mirate alla raccolta di nuove informazioni da utilizzare a fini disciplinari.

Invece, il ragionevole sospetto non consente il "recupero" retroattivo di dati personali e informazioni sul prestatore che siano state raccolte *ex ante* in assenza delle garanzie statutarie "*perché solo a partire da quel momento* [del fondato sospetto] *il datore può provvedere alla raccolta di informazioni utilizzabili*".

Del resto, se così non fosse, si produrrebbe l'effetto di giustificare retroattivamente l'utilizzo di informazioni relative ai lavoratori illegittimamente raccolte, così "*estendendo a dismisura l'area del controllo difensivo lecito*".

Tuttavia, anche in presenza delle predette condizioni (fondato sospetto e controllo mirato *ex post*), il datore di lavoro non rimane svincolato da qualsivoglia limite nell'esecuzione dell'investigazione difensiva giacché l'attività di controllo deve comunque essere progettata e attuata realizzando un adeguato bilanciamento tra le esigenze di salvaguardia della dignità e riservatezza del dipendente e quelle di protezione dei beni aziendali in senso lato.

Infatti, anche il controllo difensivo deve sempre rimanere all'interno di una "dimensione umana", non potendosi in nessun caso giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e della *privacy* del lavoratore.

Nella sentenza del 2021, tuttavia, la Suprema Corte non aveva proceduto ad una dettagliata enucleazione dei parametri che devono orientare il giudice nazionale "*nella delicata opera di bilanciamento e di delimitazione del confine tra l'interesse del lavoratore e l'interesse del datore di lavoro, con un contemperamento che non può prescindere dall'apprezzamento di tutte le circostanze del caso concreto*".

[31] Ai controlli difensivi in senso stretto si contrappongono i c.d. controlli difensivi in senso lato, soggetti alle previsioni di cui all'art. 4 Stat. lav., intesi quali "*controlli a difesa del patrimonio aziendale che riguardano tutti i dipendenti (o gruppi di dipendenti) nello svolgimento della prestazione di lavoro che li pone a contatto con tale patrimonio*".

Tale questione – solamente accennata nella pronuncia del 2021 - è, invece, affrontata nella sentenza della Corte di Cassazione 26 giugno 2023, n. 18168, la quale, aggiungendo un ulteriore "tassello" alla giurisprudenza nazionale sui controlli difensivi, specifica maggiormente i criteri orientativi di siffatta operazione di bilanciamento.

Nello specifico, la Suprema Corte rinviene tali criteri all'interno delle fonti domestiche e sovranazionali che regolano il trattamento dei dati personali e, segnatamente, nei principi fondamentali di «*minimizzazione e proporzionalità, di pertinenza e di non eccedenza rispetto ad uno scopo che sia legittimo, di trasparenza e correttezza»* sanciti dall'art. 5 del GDPR (reg. UE 679/2016) e dal Codice Privacy (d.lgs. n. 196/2003) [32] nonché nel c.d. test di proporzionalità elaborato dalla giurisprudenza della Corte Europea dei Diritti dell'Uomo formatasi in relazione all'art. 8 della CEDU, la quale, a partire dalla sentenza Bărbulescu c. Romania, ha indicato una serie di parametri "*utili anche ad orientare il bilanciamento del giudice italiano nei casi di controlli difensivi in senso stretto*" e, quindi, a verificare se la sorveglianza occulta attuata dal datore di lavoro risulti "*proporzionata e accompagnata da adeguate e sufficienti garanzie contro gli abusi*".

Del resto, i controlli difensivi operati dal datore di lavoro, sostanziandosi nell'acquisizione di informazioni riguardanti i lavoratori, costituiscono una particolare forma di trattamento di dati personali [33].

Il che impone al diritto del lavoro di confrontarsi con il complesso regolatorio della *data protection,* proprio come avviene per i controlli a distanza attuati ai sensi dei commi 1 e 2 dell'art. 4. Stat. lav., per i quali il comma 3 della disposizione statutaria pretende espressamente «*il rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196* [Codice Privacy]».

La citata sentenza, dedicando ampio spazio all'approfondimento del legame intercorrente tra controlli datoriali e regole sulla protezione dei dati personali, si colloca a pieno titolo all'interno della tendenza, sempre più avvertita nel contesto giuslavoristico, di affrontare

[32] Il richiamo operato ai principi di correttezza e trasparenza sembrerebbe ultroneo giacché l'informazione ai lavoratori appare ontologicamente incompatibile con la fattispecie dei controlli difensivi, i quali, per definizione, sono realizzati in modo occulto.

[33] Ciò in quanto, come noto, l'art. 4 GDPR adotta una definizione particolarmente ampia di dato personale ("*qualsiasi informazione riguardante una persona fisica identificata o identificabile*") nonché di trattamento ("*qualsiasi operazione o insieme di operazioni ... applicate a dati personali*").

e analizzare la tematica del monitoraggio sui prestatori anche per mezzo dei principi e delle regole, nazionali e sovranazionali, proprie del settore della *data protection* [34].

Pertanto, per una maggiore comprensione del ragionamento e delle indicazioni fornite dalla Suprema Corte, si ritiene opportuno procedere – senza pretesa alcuna di esaustività e nella misura ritenuta rilevante ai fini del confronto della giurisprudenza nazionale con le previsioni del Codice ILO – all'esame delle principali fonti richiamate dalla sentenza: GDPR, Codice Privacy e art. 8 CEDU come interpretato dalla giurisprudenza della Corte EDU.

Il GDPR e il Codice Privacy non contengono uno statuto speciale e "organico" dedicato al trattamento dei dati personali dei lavoratori [35], a differenza del Codice di condotta ILO sulla protezione dei dati personali dei lavoratori[36].

Ciononostante, il GDPR, all'art. 5, individua i principi generali, richiamati anche dal Codice Privacy, che costituiscono condizione di legittimità di qualsiasi trattamento di dati personali relativi a persone fisiche, i quali, quindi, assumono rilevanza anche rispetto alla raccolta di dati effettuata dal titolare del trattamento-datore di lavoro in sede di attuazione di un controllo per fini difensivi [37].

---

[34] Il tema è stato approfondito in dottrina, tra gli altri, da A. INGRAO, *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata,* Torino, 2018; A. SARTORI, *Il controllo tecnologico sui lavoratori: la nuova disciplina italiana tra vincoli sovranazionali e modelli comparati,* Torino, 2020; G. PROIA, *Controlli a distanza e trattamento di dati personali: due discipline da integrare (ma senza fare confusione),* in C. PISANI-G. PROIA-A. TOPO (a cura di), *op. cit.*; M. RICCI-A. OLIVIERI (a cura di), *La tutela dei dati del lavoratore: visibile e invisibile in una prospettiva comparata,* Bari, 2022.

[35] Su punto, cfr. A. TOPO-D. TARDIVO, *Hard e soft law nel diritto dell'Unione Europea in materia di trattamento dei dati personali e di tutela della riservatezza del lavoratore,* in C. PISANI-G. PROIA-A. TOPO (a cura di), *op. cit.*

[36] Una regolamentazione settoriale del trattamento dei dati personali dei lavoratori si rinviene anche nella Raccomandazione CM/Rec(2015)5 del Consiglio d'Europa del 1° aprile 2015 relativa alla protezione dei dati personali utilizzati per fini lavorativi .
Per un'analisi della Raccomandazione CM/Rec(2015)5 del Consiglio d'Europa si rinvia ad A. SARTORI, *op. cit.*

[37] Nello specifico, i dati personali devono essere: trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (c.d. principio di liceità, correttezza e trasparenza); raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità (c.d. principio limitazione della finalità); adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (c.d. principio di minimizzazione dei dati); esatti e, se necessario, aggiornati (c.d. principio di esattezza); conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità (c.d. limitazione della conservazione); trattati in maniera da garantire un'adeguata sicurezza dei dati personali (c.d. principio di sicurezza).

Lo stesso GDPR, al Considerando n. 4, però, precisa che "*il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità*".

La *privacy,* quindi, non costituisce un diritto assoluto, potendo subire deroghe ed eccezioni in ragione della coesistenza con altre prerogative fondamentali tutelate a livello costituzionale e sovranazionale.

Risulta, infatti, estranea all'ordinamento la logica dei c.d. diritti tiranni: tutti i diritti fondamentali si trovano in un rapporto di integrazione reciproca, per cui nessuno di essi si colloca in una posizione di preminenza assoluta rispetto agli altri in quanto, diversamente, si verificherebbe la "*illimitata espansione di uno dei diritti che diverrebbe tiranno nei confronti delle altre situazioni giuridiche costituzionalmente riconosciute e protette*" (Corte Cost., 9 maggio 2013, n. 85)[38].

[38] All'interno del GDPR sono contemplate alcune circostanze in cui è possibile derogare all'obbligo di informativa, principale adempimento in cui si concreta il principio di trasparenza.
L'obbligo di informativa è disciplinato negli art. 13 e 14, GDPR, che regolamentano, rispettivamente, l'ipotesi in cui i dati trattati siano stati ottenuti o non ottenuti presso l'interessato.
Nel dettaglio, l'art. 13 del GDPR, rubricato "*Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato*", impone al titolare del trattamento, in caso di raccolta presso l'interessato di dati che lo riguardano, di fornire a quest'ultimo la c.d. informativa privacy "*nel momento in cui i dati personali sono ottenuti*".
Questo significa che il GDPR impone di trattare dati personali raccolti presso l'interessato solo rendendolo edotto in anticipo e in maniera chiara circa l'esistenza, delle modalità e della portata del trattamento.
L'art. 14, GDPR, regola invece l'ipotesi opposta in cui i dati personali non siano stati ottenuti dal titolare del trattamento presso l'interessato, stabilendo che, in questo caso, l'informativa debba essere sempre resa all'interessato, seppur non in anticipo, ma "*entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese"* ovvero "*nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato*" ovvero, infine, "*nel caso in cui sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali*".
L'art. 14 GDPR, poi, individua delle specifiche ipotesi in cui il titolare non è tenuto a fornire all'interessato l'informativa circa il trattamento di dati personali non ottenuti presso il medesimo: la circostanza che potrebbe presentare una qualche rilevanza nel caso dei controlli difensivi è quella per cui l'obbligo di informativa "*rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il titolare del trattamento adotta le misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato*".
Con un certo sforzo ermeneutico, si potrebbe tentare di "salvare" la piena riconducibilità del trattamento dei dati personali nel contesto dei controlli difensivi con la disciplina privacy ammettendo che il trattamento posto in essere dal datore di lavoro costituisca un trattamento di dati personali non direttamente raccolti presso il lavoratore-interessato in cui è possibile non fornire l'informativa poiché, mettendo il lavoratore a conoscenza dell'esistenza del controllo difensivo, le finalità dello stesso rischierebbero di essere grandemente pregiudicate: il lavoratore, sapendo dell'esistenza e delle modalità dei controlli, potrebbe essere indotto a non compiere l'illecito oppure potrebbe trovare il modo di attuarlo eludendo le misure di sicurezza organizzate dal datore.

Nel caso di specie, al diritto alla riservatezza del lavoratore si contrappone il diritto alla libertà di iniziativa economica privata e il diritto alla difesa in giudizio [39] del datore di lavoro.

Tali diritti, infatti, potrebbero essere grandemente compromessi laddove al datore di lavoro fosse completamente preclusa l'effettuazione di controlli difensivi giacché le tempistiche e "la pubblicità" dell'accordo sindacale o dell'autorizzazione amministrativa e/o la necessità di fornire ai lavoratori "*adeguata informazione delle modalità (...) di effettuazione dei controlli*" difficilmente consentirebbero di raccogliere elementi idonei a sanzionare condotte esulanti rispetto al mero inadempimento della prestazione lavorativa.

E così, da un lato, il diritto alla libertà di iniziativa economica privata non può privare di contenuto il diritto alla riservatezza, il quale protegge i lavoratori dall'adozione di controlli oltremodo invasivi, dall'altro, il diritto alla *privacy* non può "svuotare" il legittimo interesse del datore di lavoro a poter reprimere efficacemente condotte illecite commesse dai prestatori.

Tuttavia, il GDPR e il Codice Privacy, non contenendo un compendio esaustivo di regole dedicate al contesto lavorativo, non forniscono indicazioni precise su come debba effettuarsi il bilanciamento tra i contrapposti interessi coinvolti.

A colmare tale lacuna, in un certo senso, "soccorre" la giurisprudenza della Corte Europea dei Diritti dell'Uomo elaborata con riferimento all'art. 8 della CEDU.

Come noto, la Corte di Strasburgo, attraverso una graduale estensione dell'ambito applicativo della disposizione convenzionale, ha ricondotto anche la tutela della *privacy*

Tuttavia, l'opzione che, a parere di chi scrive, sembra più convincente è quella di rinvenire il fondamento della deroga al principio di trasparenza e alle sue declinazioni concrete non tanto nella normativa del GDPR, ma nel principio di proporzionalità tra diritti contrapposti.

Quello che si sta affermando è che, rispetto ai controlli difensivi, il diritto alla *privacy* costituisce solo una "faccia della medaglia", imprescindibile, ma non unica, involgendo anche la libertà di iniziativa economica e il diritto ad agire e difendersi in giudizio.

Ciò considerato, si ritiene che lo sforzo di ricercare una disciplina dei controlli occulti perfettamente aderente all'impianto del GDPR – rinvenendo all'interno di questo il fondamento in grado di spiegare la deroga del principio di trasparenza - costituisca un'operazione non necessaria e, probabilmente, anche non realizzabile in maniera soddisfacente giacché la disciplina dei controlli occulti sembra scaturire piuttosto dall'applicazione del principio di proporzionalità espresso dallo stesso GDPR al Considerando n. 4.

[39] Secondo il costante orientamento della giurisprudenza di legittimità, espresso anche di recente in Cass., 29 settembre 2022, n. 28398, il diritto alla difesa "*non è limitato alla pura e semplice sede processuale, estendendosi a tutte quelle attività dirette ad acquisire prove in essa utilizzabili, ancor prima che la controversia sia stata formalmente instaurata*".

sul luogo di lavoro nell'alveo del diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza sancito dall'art. 8 della CEDU.

Infatti, secondo la Corte EDU, la predetta disposizione impone agli Stati contraenti l'obbligo positivo di predisporre misure adeguate a tutelare la vita privata dei propri cittadini, compresi i lavoratori, la cui concreta individuazione rientra nel c.d. *margin of appreciation* riservato ai singoli Stati.

Nelle sentenze Bărbulescu c. Romania, López c. Spagna e Gramaxo c. Portogallo [40] – i precedenti della Corte EDU relativi alla tutela della *privacy* nel luogo di lavoro richiamati dalla Cassazione nella pronuncia del 2023 – i giudici di Strasburgo hanno indicato gli elementi che devono essere oggetto di valutazione al fine di stabilire se, alla luce dell'insieme delle risultanze di causa, siano stati adeguatamente bilanciati i contrapposti interessi in gioco, ossia le istanze legittimamente perseguite dall'impresa attraverso il controllo e il diritto dei lavoratori alla protezione della propria vita privata.

Nello specifico, il c.d. test di proporzionalità elaborato dalla Corte EDU [41] richiede all'interprete, nell'effettuare il giudizio di bilanciamento nel caso concreto, di verificare i seguenti elementi: i) se lavoratori siano stati informati circa la possibilità che il datore di lavoro adotti misure di monitoraggio, con la precisazione che l'informazione dovrebbe, in linea di principio, essere chiara sulla natura della sorveglianza ed essere precedente alla sua attuazione; ii) il grado di invasività del controllo, tenendo conto, in particolare, della natura più o meno privata del luogo in cui si svolge il monitoraggio, dei limiti spaziali e temporali di quest'ultimo, nonché del numero di persone che hanno accesso ai

[40] Le sentenze Bărbulescu e Gramaxo trattano di monitoraggio tecnologico attuato, rispettivamente, sulla posta elettronica e attraverso strumenti di geolocalizzazione, mentre la sentenza López riguarda una fattispecie di controllo occulto realizzato all'insaputa dei lavoratori coinvolti.
Per un'analisi più approfondita della sentenza Bărbulescu c. Romania si rinvia a F. PERRONE, *Corte Europea dei Diritti dell'Uomo, sentenza López Ribalda c. Spagna: la tutela della privacy sul luogo di lavoro dopo Barbulescu 2,* in *Labor,* 22 febbraio 2018; per quanto concerne la sentenza López c. Spagna cfr. V. NUZZO, *Il ragionevole sospetto di illecito e la possibilità di controlli difensivi occulti all'esame della Grande Camera della Corte Europea dei diritti dell'uomo,* in *Labor,* 2020, n. 2; quanto alla sentenza Gramaxo c. Portogallo si rinvia a M. NOGUEIRA GUASTAVINO, *Geolocalización lícita, probablemente desproporcionada. La necesidad de una vigilancia cualitativa, no cuantitativa ,* in *Revista de jurisprudencia laboral,* 2023, n. 2 e a D. TARDIVO, *Controlli tramite l'(ab)uso di dispositivi di geolocalizzazione alla luce dell'art. 8 Cedu,* in *Arg. dir. lav.,* 2023, n. 3.

[41] Il test di proporzionalità, così come declinato nella sentenza Bărbulescu, è stato riproposto pedissequamente anche nelle successive sentenze López e Gramaxo.
Per un approfondimento sulla tematica si rinvia a P. PINTO DE ALBUQUERQUE-A. SITZIA, *Lavoro e monitoraggio: il "test di proporzionalità" nella giurisprudenza della CEDU,* nonché a S. BERTOCCO, *Il conflitto tra sfera privata del lavoratore e libertà di impresa: la tutela del patrimonio e dell'organizzazione aziendale nella prospettiva del diritto europeo,* in C. PISANI-G. PROIA-A. TOPO, (a cura di), *op. cit.*

suoi risultati; iii) l'esistenza di una giustificazione all'uso della sorveglianza e alla sua estensione con motivi legittimi, con la precisazione che quanto più invadente è la sorveglianza, tanto più gravi sono le giustificazioni richieste; iv) se lo scopo legittimo perseguito dal datore di lavoro potesse essere raggiunto causando una minore invasione della vita privata del dipendente; v) come il datore di lavoro abbia utilizzato i risultati della misura di monitoraggio e se siano serviti per raggiungere lo scopo dichiarato della misura; vi) se siano state fornite ai prestatori adeguate garanzie sul grado di invasività delle misure di sorveglianza, mediante informazioni ai lavoratori interessati o ai rappresentanti del personale circa l'attuazione e l'entità del monitoraggio, dichiarando l'adozione di tale misura a un organismo indipendente o mediante la possibilità di presentare reclamo.

In un certo senso, potrebbe affermarsi che i parametri del test enucleato dalla giurisprudenza CEDU, "*evidentemente utili anche ad orientare il bilanciamento del giudice italiano"*, costituiscano la concretizzazione nella materia dei controlli del principio di proporzionalità tra diritti fondamentali enunciato dal Considerando n. 4 del GDPR.

Sempre con riferimento alla giurisprudenza della Corte EDU, rispetto alla tematica dei controlli difensivi risulta particolarmente rilevante la sentenza López c. Spagna.

Come anticipato, tale pronuncia, applicando proprio il test di proporzionalità espresso dalla sentenza Bărbulescu, ha ritenuto legittimo il controllo realizzato da un datore di lavoro spagnolo tramite strumenti di videosorveglianza installati occultamente in presenza di un ragionevole sospetto circa la commissione di condotte illecite consistenti nella sottrazione di beni aziendali.

Ciò significa che, secondo la Corte EDU, è possibile che, sulla base delle risultanze del caso concreto, il monitoraggio dei lavoratori possa risultare proporzionato e, quindi, giustificato malgrado il controllo (e, quindi, il trattamento di dati personali) sia stato realizzato "derogando" al principio fondamentale di trasparenza.

La disapplicazione del principio di trasparenza in nome del contemperamento tra interessi datoriali e dei prestatori non è di poco momento, considerando che si tratta di una delle colonne portanti dell'edificio della protezione dei dati personali costruito dalla disciplina nazionale ed europea in materia di *privacy*.

Tali normative, infatti, contemplano tra i propri pilastri costitutivi il mantenimento in capo all'interessato del controllo sui propri dati personali: sebbene i dati personali possano essere trattati anche senza il consenso del soggetto a cui appartengono [42], risulta però necessario fornire tempestivamente all'interessato informazioni chiare ed esaustive in merito alle operazioni compiute sui dati relativi alla sua persona.

Inoltre, il principio di trasparenza risulta, per così dire, interiorizzato all'interno dei punti i) e vi) [43] del test di proporzionalità della giurisprudenza della Corte EDU.

Considerata la centralità del suddetto principio nel contesto del diritto alla protezione dei dati personali, la possibilità di invadere la sfera personale del lavoratore a sua insaputa attuando un monitoraggio occulto richiede la sussistenza di circostanze giustificative *extra ordinem* che "impongano" l'attuazione di un trattamento sconosciuto all'interessato.

Tale motivazione, come visto, è stata ravvisata dalla sentenza López – espressamente richiamata sia nelle sentenze n. 25732/2021 e 2023, n. 18168/2023 per argomentare la sopravvivenza dei controlli difensivi alla riformulazione dell'art. 4 Stat. lav. – proprio nella sussistenza di un ragionevole sospetto circa la perpetrazione di condotte illecite ad opera di uno o più lavoratori.

In tale situazione, infatti, l'applicazione del principio di trasparenza implicherebbe un nocumento alle prerogative datoriali tale da impedire o rendere estremamente improbabile l'irrogazione di sanzioni a carico dei responsabili.

---

[42] Come noto, il consenso dell'interessato costituisce solamente una delle possibili condizioni di liceità del trattamento di dati personali, potendo il titolare procedere al trattamento anche al ricorrere di una diversa c.d. base giuridica individuata dagli artt. 6 (per i dati "comuni") e 9 (per le categorie particolari di dati) del GDPR.

Per quanto concerne i controlli difensivi in senso stretto, il fondamento di liceità sembra essere individuato dalla Corte nella base giuridica di cui all'art. 6, comma 1, lett. f), GDPR, ossia nella circostanza che il trattamento risulti «*necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali*».

[43] Come visto, il primo elemento da tenere in considerazione nella valutazione di bilanciamento è «*l'informazione del lavoratore circa la possibilità che il datore di lavoro adotti misure di monitoraggio, con la precisazione che la stessa dovrebbe, in linea di principio, essere chiara sulla natura della sorveglianza ed essere precedente alla sua attuazione*», mentre il sesto elemento è rappresentato dalla «*offerta di adeguate garanzie sul grado di invasività delle misure di sorveglianza, mediante informazioni ai lavoratori interessati o ai rappresentanti del personale circa l'attuazione e l'entità del monitoraggio, dichiarando l'adozione di tale misura a un organismo indipendente o mediante la possibilità di presentare reclamo*».

Fermo restando che, sia per la giurisprudenza interna che per quella di Strasburgo, anche in presenza della *notitia criminis,* il controllo, seppur occulto, per risultare legittimo dovrà comunque mantenersi nei limiti della proporzionalità e non eccedenza [44].

La sentenza del 2023, individuando le condizioni in presenza delle quali la Cassazione ritiene i controlli difensivi legittimi, fornisce utili indicazioni agli operatori pratici per orientarsi all'interno dei frequenti contenziosi che sorgono in *subiecta materia.*

Innanzitutto, in ossequio al principio di vicinanza della prova e in conformità alla struttura distributiva del carico probatorio propria delle controversie in materia di sanzioni disciplinari e della normativa *privacy* [45], spetta al datore di lavoro-titolare del trattamento l'onere di provare la legittimità del controllo difensivo.

In particolare, il datore di lavoro deve essere in grado di allegare e dimostrare gli elementi di fatto dai quali scaturisce il fondato sospetto che legittima tale tipologia di controllo [46].

In ogni caso, tali elementi non possono consistere né in dati precedentemente raccolti in violazione delle prescrizioni di cui all'art. 4 Stat. lav. né derivare dall'analisi degli stessi: del resto, se così non fosse, sarebbe resa retroattivamente lecita la raccolta di dati personali dei prestatori effettuata in difetto di autorizzazione sindacale o amministrativa e/o di adeguata informazione ai lavoratori.

Inoltre, da tali elementi dovrà essere possibile ricavare il momento di insorgenza del sospetto.

L'individuazione di tale momento, infatti, rileva sotto un duplice profilo in quanto, da un lato, "*segna il momento a partire dal quale i dati acquisiti possono essere utilizzati nel procedimento disciplinare e, successivamente, nel giudizio*", dall'altro, serve a dimostrare la tempestività del controllo considerato che il decorso di un significativo intervallo temporale potrebbe rivelare la volontà datoriale di "riciclare" condotte già da tempo

---

[44] Così anche A. SITZIA, *Lavoro, controlli e privacy: un nouveau parcours per il test di bilanciamento nell'elaborazione della sezione lavoro (e del garante privacy),* in *Massimario di giurisprudenza del lavoro,* n. 4/2021, secondo il quale "*il sospetto circa la commissione di un illecito rende recessiva la regola della trasparenza, ma non il principio del sempre necessario bilanciamento tra interessi contrapposti "*.

[45] Nella quale, è il titolare del trattamento – nel caso di specie, il datore di lavoro – a dover dimostrare che il trattamento sia stato posto in essere nel rispetto dei principi e delle regole dettate dal GDPR.

[46] La dottrina ha sottolineato le difficoltà insiste nell'individuazione della soglia di ragionevolezza del sospetto necessaria al fine di poter dare legittimamente corso al controllo difensivo. Sul punto, cfr. R. ROMEI, *Il "ragionevole sospetto" in Cassazione,* in *Lavoro Diritti Europa,* 28 febbraio 2023.

conosciute (e tollerate) al fine di epurare dalla compagine aziendale un lavoratore divenuto successivamente sgradito.

Il datore-titolare, poi, in attuazione dei principi di *privacy by design e by default,* dovrà assicurarsi di implementare il trattamento (ossia, il controllo) in modo che risulti proporzionato e non eccessivo rispetto alle imprescindibili esigenze di protezione della *privacy* dei lavoratori-interessati [47].

Seppur sul punto rimanga inevitabilmente un qualche spazio per la discrezionalità giudiziale, secondo le indicazioni fornite dalla Suprema Corte, al fine di verificare la proporzionalità del trattamento-controllo, dovranno essere presi in considerazione i principi fondamentali della *data protection* e i parametri individuati dalla giurisprudenza della Corte EDU [48].

Pertanto, dovranno attentamente valutarsi le concrete modalità di esercizio del controllo e, in particolare, la durata dell'indagine; la natura più o meno privata dei luoghi in cui è condotta; il numero di persone che hanno accesso ai risultati; la gravità delle motivazioni alla base dell'indagine; la possibilità di raggiungere efficacemente il risultato perseguito mediante modalità di controllo meno invasive della sfera personale dei lavoratori; la pertinenza e la non eccedenza delle informazioni raccolte rispetto al raggiungimento degli scopi per cui è attivato il monitoraggio.

In definitiva, la medesima soluzione individuata già nel 1997 dal Codice ILO all'art. 6, par. 14, lett. b), ove è espresso che il monitoraggio occulto dovrebbe poter essere attuato "*if there is suspicion on reasonable grounds of criminal activity or other serious wrongdoing"*, a seguito di un lungo percorso giurisprudenziale, sembra essere stata sostanzialmente accolta, seppur con un maggiore grado di specificazione e approfondimento, sia dalla giurisprudenza comunitaria sia da quella domestica quale

[47] Secondo A. SITZIA, *op. cit.,* "*pare evidente che per potersi dimostrare al giudice che l'indagine difensiva (occulta) è stata posta in essere in conformità ai tre requisiti delineati dalla Sezione lavoro (fondato sospetto, raccolta ex post ed effettuazione del corretto bilanciamento tra esigenze contrapposte), il titolare del trattamento dovrà essere in grado di documentare il processo di valutazione e strutturazione del trattamento*".

[48] Sul punto, si segnala la critica avanzata da A. BELLAVISTA, *Sorveglianza elettronica, protezione dei dati personali e tutela dei lavoratori,* in *Lavoro Diritti Europa,* 21 febbraio 2023, secondo il quale la giurisprudenza della Corte europea dei Diritti dell'Uomo sul rispetto della vita privata nei luoghi di lavoro "*rappresenta, per la Cassazione, un argomento per giustificare la disapplicazione dell'art. 4 St. lav. e lasciare campo libero ad un imprevedibile e soggettivo bilanciamento giudiziale"*.

risposta alla *querelle* relativa alle condizioni di liceità del *secret monitoring* nell'ambito del rapporto di lavoro.

Capitolo II

La tutela della riservatezza del lavoratore nelle Convenzioni e Raccomandazioni dell'Organizzazione Internazionale del Lavoro

6. Premessa metodologica

Esaurita la trattazione del *Code of Practice* che - malgrado la crescente attenzione dell'ILO rispetto alle nuove sfide di tutela della privacy poste dal ricorso a sistemi di *alghoritm management* sempre più evoluti - tutt'ora rappresenta la principale fonte organica nella materia oggetto di analisi, si procederà con l'analisi delle disposizioni "settoriali" dedicate alla protezione dei dati personali presenti all'interno degli atti normativi fondamentali dell'ILO (Convenzioni e Raccomandazioni).

L'attività di ricognizione delle fonti svolta, lungi dall'avere una finalità meramente compilatoria, si pone l'obiettivo di verificare quale sia l'effettivo livello di protezione della privacy garantito ai lavoratori dalle fonti dell'ILO.

Dal punto di vista espositivo, si ritiene maggiormente proficuo suddividere le disposizioni individuate per nuclei argomentativi tematici piuttosto che per tipologia di fonte da cui le norme promanano.

Infatti, esaminare prima tutte le disposizioni contenute nelle Convenzioni e, di seguito, quelle rinvenute all'interno delle Raccomandazioni avrebbe il pregio di far emergere più immediatamente, dal punto di vista grafico, quali siano le regole convenzionali, dotate della massima forza precettiva, e quali abbiano la più attenuata efficacia giuridica propria delle Raccomandazioni.

Tuttavia, così operando, la trattazione rischierebbe di risultare frammentata e disorganica, considerato che disposizioni relative alla protezione della riservatezza del lavoratore in un medesimo contesto si troverebbero separate e distanziate in diverse parti dell'elaborato a causa della diversa della fonte di provenienza.

Pertanto, considerato che l'obiettivo di ricerca proprio di questa parte della trattazione non è la sola ricognizione delle previsioni dell'Organizzazione in tema di protezione de lla riservatezza del lavoratore – attività che, comunque, a quanto consta, risulta inedita – ma anche verificare se sia possibile ricavare all'interno delle "fonti primarie" principi di applicazione generale *in subiecta materia*, si ritiene che procedere con la suddivisione

delle disposizioni adottate dall'ILO per nuclei tematici risulti maggiormente confacente al predetto scopo.

Sempre sotto il profilo metodologico, si precisa che l'oggetto di indagine non risulta limitato al solo trattamento dei dati personali, ma è altresì esteso alle fattispecie che rispondono a questioni ed esigenze di rispetto della vita privata dei lavoratori in senso ampio, ancorché manchi un trattamento di dati personali in senso tecnico.

Per tale ragione, si è prescelto di adottare nel titolo dell'elaborato l'espressione tutela della riservatezza del lavoratore in quanto capace di includere tutte le situazioni in cui sia in gioco la protezione dell'intimità privata dei lavoratori.

7. I trattamenti di dati personali effettuati dalle agenzie per l'impiego privato

L'ILO, all'interno della Convenzione n. 181 del 1997 e della relativa Raccomandazione n. 188 del 1997, si preoccupa di tutelare la privacy dei lavoratori rispetto ai trattamenti di dati personali effettuati dalle agenzie per l'impiego privato.

L'attuale Convenzione sulle agenzie per l'impiego privato n. 181/1997 sostituisce le precedenti Convenzioni n. 88 del 1948 e n. 96 del 1949[49], le quali esprimevano un approccio particolarmente restrittivo rispetto all'esercizio da parte dei privati di attività inerenti alla mediazione tra domanda e offerta di lavoro.

La ragione della diffidenza dell'ILO verso gli operatori privati deriva dalla convinzione secondo cui l'operatività di agenzie private con funzioni in tema di collocamento della manodopera si ponesse in contrasto con il principio fondamentale espresso dell'Organizzazione nella dichiarazione di Filadelfia del 1944 secondo cui "*il lavoro non è una merce*".

Infatti, l'ILO riteneva che, per prevenire fenomeni di sfruttamento delle vulnerabilità di lavoratori privi di occupazione in cerca di una (ri)collocazione all'interno del mercato del lavoro, le attività dirette a favorire l'incontro tra domanda e offerta di lavoro dovessero essere erogate da servizi pubblici e gratuiti di collocamento.

[49] Per un approfondimento delle fonti ILO relative alle agenzie per l'impiego privato si rinvia ai contributi di G. P. LIONTI, *Lavoro temporaneo: le istanze esogene dell'OIL e il camaleontismo dell'approccio italiano*, in L. MECHI, A. SITZIA (a cura di), *op. cit*. e di G. LINFANTE, *I servizi privati per l'impiego: il caso delle agenzie di collocamento*, in *Monografie sul Mercato del lavoro e le politiche per l'impiego*, n. 4/2002, ISFOL.

Con un evidente cambiamento di paradigma, la sessione n. 81 della Conferenza Internazionale del Lavoro ha preso atto del ruolo positivo che può essere svolto dalle agenzie per l'impiego private ai fini del buon funzionamento del mercato del lavoro, programmando l'adozione di una nuova Convenzione in materia.

Con l'adozione della Convenzione n. 181/1997, l'ILO, quindi, mira a favorire l'operatività delle agenzie per l'impiego private[50], occupandosi, al contempo, di prevenire abusi ai danni dei lavoratori e delle persone in cerca di occupazione[51].

---

[50] Ai sensi dell'art. 1, comma 1, Conv. ILO n. 181/1997, l'espressione "*agenzia d'impiego privata*" indica "*ogni persona fisica o morale, indipendente dalle autorità pubbliche, che fornisce uno o più dei seguenti servizi relativi al mercato del lavoro: a) servizi volti ad abbinare le offerte e le domande d'impiego senza tuttavia che l'agenzia d'impiego privata divenga parte delle relazioni di lavoro che potrebbero derivarne; b) servizi consistenti nell'assumere lavoratori allo scopo di metterli a disposizione di una terza persona fisica o morale («impresa utilizzatrice») che stabilisce i loro compiti e ne sorveglia l'esecuzione; c) altri servizi relativi alla ricerca di lavoro, determinati dall'autorità competente previa consultazione delle organizzazioni di datori di lavoro e di lavoratori più rappresentative, come ad esempio la fornitura d'informazioni, senza tuttavia che ciò implichi l'abbinamento di un'offerta e di una domanda specifiche*" (traduzione italiana pubblicata in Gazzetta Ufficiale della Repubblica italiana, 2 febbraio 2000, n. 26).
La Convenzione presenta un ambito applicativo tendenzialmente onnicomprensivo, coprendo sia tutte le categorie di lavoratori, inclusi i richiedenti lavoro (art. 1, par. 2), fermo restando che "*ogni Membro deve prendere misure per accertare che il lavoro minorile non sia né utilizzato né fornito da agenzie per l'impiego private*" (art. 9) sia tutti i rami di attività economica, ad eccezione del reclutamento e del collocamento della gente di mare (art. 2),
Tuttavia, ai sensi dell'art. 2, par. 4, gli Stati – previa consultazione delle organizzazioni più rappresentative di datori di lavoro e di lavoratori interessati – possono sia vietare, in determinate circostanze, alle agenzie per l'impiego private di trattare con talune categorie di lavoratori o in taluni rami dell'attività economica sia escludere, in determinate circostanze, i lavoratori di alcuni rami dell'attività economica o di settori di questi ultimi, dalla portata di applicazione della convenzione o di alcune sue disposizioni, ma a condizione che ai lavoratori interessati sia assicurata ad altro titolo un'adeguata protezione.
In ogni caso, ogni Stato che ratifica la Convenzione deve indicare gli eventuali divieti o esclusioni ed esplicitarne i motivi all'interno dei rapporti annuali contenente l'indicazione dei provvedimenti adottati allo scopo di porre in esecuzione le convenzioni alle quali lo Stato ha aderito redatti ai sensi dell'art. 22 della Costituzione dell'ILO.

[51] Al fine di proteggere le persone che si avvalgono dei servizi delle agenzie per l'impiego private, ogni Stato deve determinare, per mezzo della concessione di licenze o di abilitazioni, le condizioni di esercizio delle attività delle agenzie, salvo quando tali condizioni siano in altro modo regolamentate dalla legislazione e dalla prassi nazionali (art. 3, par. 2).
In questo modo, l'ILO mira ad assicurarsi che possano operare solamente gli operatori privati che presentino un sufficiente livello di affidabilità, essendo in possesso dei requisiti stabiliti dagli Stati membri dell'ILO al fine di operare nel mercato del lavoro.
Inoltre, per evitare che le agenzie private possano lucrare sulla posizione di debolezza delle persone in cerca di occupazione, viene confermato il principio di gratuità dei servizi per i lavoratori, prevedendosi che le agenzie per l'impiego private non devono far pagare ai lavoratori, direttamente o indirettamente, spese o altri costi (art. 7).
Questo, tuttavia, non significa che agli operatori privati del mercato del lavoro sia precluso il conseguimento di erogazioni economiche a fronte dei servizi erogati.
Infatti, il principio di gratuità dei servizi riguarda solamente i lavoratori, ben potendo le agenzie ricevere compensi dai datori di lavoro-committenti o usufruire di stanziamenti di risorse pubbliche.
Eccezionalmente e nell'interesse dei lavoratori, l'autorità competente, previa consultazione delle organizzazioni di datori di lavoro e di lavoratori maggiormente rappresentative, può autorizzare deroghe al principio di gratuità per alcune categorie di lavoratori, e per servizi specificamente identificati, forniti dalle

Una delle direttrici di tutela attraverso cui l'ILO mira a proteggere i lavoratori che entrano in contatto con le agenzie per l'impiego privato consiste, appunto, nella regolamentazione del trattamento dei loro dati personali.

Infatti, le agenzie per l'impiego privato potrebbero voler assumere quante più informazioni possibili sui prestatori allo scopo di aumentare l'efficienza dei propri servizi di selezione del personale in favore di datori di lavoro-committenti e/o di invio di personale in somministrazione presso imprese utilizzatrici.

Dunque, candidati all'assunzione e lavoratori corrono il rischio di vedere precluse o limitate le proprie prospettive occupazionali a causa di caratteristiche soggettive e private che potrebbero rappresentare fattori di discriminazione nel mercato del lavoro.

Per tale ragione, l'art. 6 della Convenzione n. 181/1997 prevede alcune cautele con riguardo all'elaborazione dei dati personali relativi ai lavoratori[52].

Malgrado la predetta disposizione utilizzi l'espressione "*elaborazione di dati personali*", l'ambito applicativo dell'art. 6 risulta particolarmente esteso in quanto con tale espressione si intende "*la raccolta, lo stoccaggio, la combinazione e la comunicazione di dati personali, o ogni altro uso*[53] *che potrebbe essere fatto di qualsiasi informazione relativa ad un lavoratore identificato o identificabile*" (art. 1, par. 3)[54].

---

agenzie per l'impiego private (art. 7, par. 2).
Considerata la ratifica della Convenzione n. 181/1997 (G.U. 2 febbraio 2000, n. 26), l'ordinamento italiano prevede il divieto di esigere o comunque di percepire, direttamente o indirettamente, compensi dal lavoratore, salvo che i contratti collettivi stipulati da associazioni dei datori di lavoro e dei prestatori di lavoro comparativamente più rappresentative a livello nazionale o territoriale stabiliscano che tale divieto non operi per specifiche categorie di lavoratori altamente professionalizzati o per specifici servizi offerti dalle agenzie per il lavoro (art. 11, d.lgs. n. 276/2003, c.d. decreto Biagi).

[52] Ai fini della Convenzione, il termine lavoratori include anche i richiedenti lavoro (art. 1, par. 2).

[53] L'espressione "*elaborazione*" risulta sostanzialmente corrispondente alla nozione di trattamento di dati personali adottata dall'art. 4, comma 1, lett. b), Reg. UE 2016/679 (c.d. GDPR), a norma della quale per trattamento si intende "*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*".
E, infatti, nel testo inglese è utilizzata l'espressione "*processing of personal data*", mentre nella versione francese quella di "*traitement des données personnelles".*

[54] Seppur la Convenzione n. 181 del 1997 non contenga una definizione espressa di dato personale del lavoratore, dalla nozione di "*elaborazione dei dati personali*" di cui all'art. 3 si ricava che per dato personale si intende "*qualsiasi informazione relativa ad un lavoratore identificato o identificabile*". Pertanto - proprio come nel Reg. UE 2016/679, art. 4, comma 1, lett. a) - costituiscono dati personali non solo le informazioni

Ai sensi dell'art. 6, "*l'elaborazione dei dati personali relativi ai lavoratori da parte delle agenzie per l'impiego private, deve: a) essere effettuato in condizioni tali da proteggere questi dati e rispettare la vita privata dei lavoratori, in conformità alla legislazione ed alla prassi nazionale; b) limitarsi alle questioni relative alle qualifiche ed all'esperienza professionale dei lavoratori, e ad ogni altra informazione direttamente pertinente*".

Vengono, quindi, individuati due distinti limiti ai trattamenti di dati personali dei lavoratori effettuati dagli operatori privati della mediazione tra domanda e offerta di lavoro.

Il primo limite, di carattere più generale, impone di proteggere i dati personali e rispettare la privacy dei lavoratori in conformità con quanto previsto dalla legislazione e dalla prassi nazionale.

Pertanto, l'art. 6 rinvia all'applicazione delle regole sulla *privacy* vigenti all'interno dell'ordinamento nazionale degli Stati.

Potrà trattarsi di normative di applicazione generale che riguardano tutti i cittadini compresi i lavoratori, di discipline specificatamente dedicate al trattamento dei dati dei lavoratori o di prescrizioni indirizzate proprio alle agenzie per l'impiego privato[55].

Il secondo limite, connotato da un maggiore livello di dettaglio, prevede che, in ogni caso, il trattamento dei dati personali deve *"limitarsi alle questioni relative alle qualifiche ed all'esperienza professionale dei lavoratori, e ad ogni altra informazione direttamente pertinente*[56]", ponendosi in linea di continuità con quanto previsto dall'art. 5, par. 1, del

---

direttamente identificative di una persona, ma anche quelle informazioni che presentano l'attitudine a renderla identificabile.

[55] A titolo di esempio, il legislatore nazionale, all'art. 10, comma 1, d.lgs. n. 276/2003, rubricato "*Divieto di indagini sulle opinioni e trattamenti discriminatori*" fa divieto alle agenzie per il lavoro – così come agli altri soggetti pubblici e privati autorizzati o accreditati – *"di effettuare qualsivoglia indagine o comunque trattamento di dati ovvero di preselezione di lavoratori, anche con il loro consenso, in base alle convinzioni personali, alla affiliazione sindacale o politica, al credo religioso, al sesso, all'orientamento sessuale, allo stato matrimoniale o di famiglia o di gravidanza, alla età, all'handicap, alla razza, all'origine etnica, al colore, alla ascendenza, all'origine nazionale, al gruppo linguistico, allo stato di salute nonché ad eventuali controversie con i precedenti datori di lavoro, a meno che non si tratti di caratteristiche che incidono sulle modalità di svolgimento della attività lavorativa o che costituiscono un requisito essenziale e determinante ai fini dello svolgimento dell'attività lavorativa".*

La medesima disposizione pone altresì il "*divieto di trattare dati personali dei lavoratori che non siano strettamente attinenti alle loro attitudini professionali e al loro inserimento lavorativo*".

L'art. 10 del c.d. decreto Biagi è espressamente richiamato all'interno dell'art. 113, d.lgs. n. 196/2003, come modificato dal d.lgs. n. 101/2018 (Codice Privacy).

[56] La formulazione utilizzata dall'ILO è simile a quella adottata dall'art. 8, l. n. 300/1970 (c.d. Statuto dei Lavoratori) che vieta al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo terzi, sulle opinioni politiche, religiose o sindacali

Code of practice del 1997 ai sensi del quale "*personal data should be processed* (…) *only for reasons directly relevant to the employment of the worker*".

In questo modo, l'ILO introduce una limitazione alle finalità per cui i dati personali dei lavoratori possono essere trattati dalle agenzie per l'impiego privato vincolante per tutti gli Stati membri dell'Organizzazione che hanno ratificato la Convenzione n. 181/1997.

Considerata l'ampia nozione di elaborazione dei dati adottata dalla Convenzione di cui si è dato conto, si ritiene che sia vietato non solo richiedere ai lavoratori dati che non siano strettamente attinenti alle loro attitudini professionali e al loro inserimento lavorativo, ma anche l'utilizzo di tali informazioni, pure se reperite *aliunde*[57].

Inoltre, si reputa che divieto posto dall'art. 6, par. 1, lett. b) non possa essere superato nemmeno con il consenso del lavoratore.

Infatti, l'art. 6 non prevede alcuna eccezione al divieto di trattamento, mentre, sotto il profilo sistematico, si rileva come le altre disposizioni convenzionali che introducono divieti in capo alle agenzie per l'impiego privato indichino espressamente la presenza di situazioni eccezionali in cui risulta possibile derogare a siffatti divieti (cfr. artt. 5[58] e 7[59]).

Tale interpretazione, del resto, risulta coerente con la considerazione per cui le persone che si affacciano al mercato del lavoro si trovano in una posizione di debolezza strutturale rispetto agli operatori che possono favorire il loro (re)inserimento occupazionale.

---

del lavoratore, nonché su "*fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore*".
Tuttavia, l'art. 8 St. Lav. riguarda i datori di lavoro, mentre l'art. 6 Conv. n. 181/1997 anticipa la tutela dei dati personali sin dalla fase in cui il (potenziale) lavoratore entra in contatto con gli operatori del mercato del lavoro.

[57] Ciò in quanto la definizione di elaborazione copre non solo la raccolta, ma anche "*ogni altro uso*" dei dati.

[58] L'art. 5, che pone il divieto di discriminazioni basate sulla razza, il colore, il sesso, la religione, l'opinione politica, l'ascendenza nazionale, l'origine sociale o ogni altra forma di discriminazione coperta dalla legislazione e dalle prassi nazionali, come l'età e l'invalidità (par. 1), con una previsione derogatoria esplicita, prevede che tale divieto di discriminazione non può operare in modo da impedire alle agenzie per l'impiego private di fornire determinati servizi o di realizzare programmi volti, in modo particolare, ad aiutare i lavoratori più sfavoriti nelle loro attività di ricerca di lavoro (par. 2).

[59] L'art. 7, dopo aver sancito, al par. 1, la gratuità per i lavoratori dei servizi per l'impiego, individua espressamente al par. 2 le possibili eccezioni al divieto di far sostenere ai lavoratori, direttamente o indirettamente, spese o altri costi.

Pertanto, a causa della posizione di squilibrio[60], tali soggetti potrebbero essere indotti a consentire a rivelare informazioni relative alla propria sfera personale, così vanificando la disposizione protettiva posta dall'art. 6.

Invece, come si ricava dall'art. 5, informazioni normalmente non rilevanti per la valutazione dell'attitudine professionale del lavoratore – quali la "*razza, il colore, il sesso, la religione, l'opinione politica, l'ascendenza nazionale, l'origine sociale o ogni altra forma di discriminazione coperta dalla legislazione e dalle prassi nazionali, come l'età e l'invalidità*" – possono essere trattati dalle agenzie private allo scopo di "*fornire determinati servizi o di realizzare programmi volti, in modo particolare, ad aiutare i lavoratori più sfavoriti nelle loro attività di ricerca di lavoro*".

Infatti, la partecipazione dei lavoratori più vulnerabili e distanti dal mercato del lavoro a servizi o iniziative finalizzate a favorirne la (ri)collocazione professionale potrebbe richiedere la (legittima) rivelazione di informazioni di natura sensibile inerenti alla persona del prestatore[61].

Infine, per bilanciare la riservatezza dei lavoratori con l'interesse pubblico alla valutazione della correttezza dell'operato delle agenzie private, alla trasparenza del mercato del lavoro e al monitoraggio statistico, l'art. 13, par. 3 e 4, della Convenzione prevede "*le agenzie per l'impiego private devono, ad intervalli determinati dalle autorità competenti, fornire a queste ultime le informazioni richieste, tenendo in debita considerazione il carattere riservato di tali informazioni: a) per consentire alle autorità competenti di conoscere la struttura e le attività delle agenzie per l'impiego private in conformità alle condizioni ed alle prassi nazionali; b) per fini statistici*", cosicché l'autorità competente possa elaborare le informazioni trasmesse per "*renderle disponibili al pubblico"*.

Le disposizioni convenzionali poste a tutela della privacy dei lavoratori sono ulteriormente specificate nella Raccomandazione n. 188 del 1997.

---

[60] Anche il considerando n. 43, Reg. UE 2016/679 indica che "*è opportuno che il consenso non costituisca un valido fondamento giuridico per il trattamento dei dati personali in un caso specifico, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento*" (sul punto, cfr. anche European Data Protection Board - EDPB, *Linee guida sul consenso*, 4 maggio 2020).

[61] Del resto, è lo stesso ILO, nella Raccomandazione sulle agenzie per l'impiego privato n. 188/1997, a incoraggiare le predette agenzie "*a promuovere la parità nel lavoro per mezzo di programmi di azione positivi*" (art. 10).

In particolare, l'art. 11 della citata Raccomandazione, in linea di continuità con l'art. 6 della Convenzione, indica che "*alle agenzie per l'impiego private dovrebbe essere vietato di trascrivere in schedari o registri i dati personali non necessari per valutare l'abilitazione dei candidati per gli impieghi per i quali sono o potrebbero essere presi in considerazione*"[62].

Inoltre, la Raccomandazione specifica i criteri in base ai quali determinare il periodo di conservazione dei dati personali dei lavoratori, così da evitare che i predetti dati, legittimamente raccolti e utilizzati, siano mantenuti dalle agenzie per l'impiego *sine die*.

A norma dell'art. 12, par. 1, "*le agenzie per l'impiego private possono conservare i dati personali di un lavoratore soltanto per il tempo richiesto dal fine specifico della raccolta di dati, oppure per tutto il tempo in cui il lavoratore desidera rimanere iscritto su una lista di candidati*".

Dunque, il periodo di conservazione dipende dalla finalità per la quale i dati sono trattati, ferma la possibilità che il lavoratore manifesti l'interesse alla conservazione dei propri dati personali all'interno di liste di candidati detenute dalle agenzie per l'impiego in modo da poter essere contattato per la promozione di occasioni di lavoro.

La Raccomandazione, poi, si preoccupa di dotare i lavoratori di strumenti volti a consentire la verifica della conformità dei trattamenti alle regole sulla privacy.

A tal fine, l'art. 12, par. 2, della Raccomandazione contempla diritti individuali[63] di accesso, rettifica e cancellazione dei dati, prevedendo che "*dovrebbero essere presi provvedimenti affinché i lavoratori possano consultare tutti i dati personali che li riguardano, a prescindere se elaborati automaticamente, per via informatica o manualmente. Tali provvedimenti dovrebbero includere il diritto per il lavoratore di ottenere ed esaminare una copia di tutti questi dati, nonché di esigere che i dati inesatti o incompleti siano eliminati o rettificati*".

---

[62] Quanto ai dati relativi alla salute, stante l'elevata potenzialità discriminatoria propria di tali informazioni, la Raccomandazione inserisce una sorta di presunzione relativa di inidoneità di tale tipologia di dati rispetto alla valutazione dell'attitudine professionale del lavoratore.
Infatti, ai sensi dell'art. 12, par. 3, "*salvo se i dati sono direttamente connessi alle condizioni richieste per l'esercizio di una determinata professione ed il lavoratore interessato lo autorizza espressamente, le agenzie d'impiego private non dovrebbero chiedere, conservare o utilizzare informazioni sullo stato di salute di un lavoratore o utilizzare queste informazioni per decidere circa la sua abilitazione all'impiego*".

[63] A differenza del Codice di condotta ILO del 1997, la Raccomandazione n. 188/1997 non contempla invece strumenti di tutela collettiva esercitabili dai rappresentanti dei lavoratori.

A conclusione dell'esame degli *standard* lavoristici in materia di protezioni dei dati personali nel contesto delle agenzie per l'impiego privato, si rileva che le predette agenzie rientrano anche nell'ambito di applicazione del *Code of practice on the protection of workers' personal data* del 1997[64].

Se ne ricava che l'Organizzazione Internazionale del Lavoro, a protezione dei dati personali trattati dalle agenzie per l'impiego privato, da un lato, attraverso il Codice di Condotta, predispone una regolamentazione organica e esaustiva, ma contenuta in uno strumento che non rientra nel novero delle fonti primarie dell'ILO; dall'altro, attraverso la Convenzione n. 181/1997 e la Raccomandazione n. 188/1997, pone regole di fonte primaria, ma che disciplinano solamente alcuni specifici profili della materia[65].

---

[64] Ciò è espressamente chiarito nel *Commentary on the code of practice*, redatto dallo stesso gruppo di esperti che ha realizzato il Codice di condotta al fine di meglio chiarire le disposizioni nello stesso contenute.
In particolare, nel commento all'art. 3, viene specificato come, dal momento che il Codice di condotta si applica anche agli *applicants for employment*, sono soggetti ai principi del Codice non solo i *direct employers*, ma anche le *employment agencies*.
Ancora più chiaramente, il commento all'art. 4, rubricato "*Scope of applications*", conferma che le regole a tutela della privacy dei prestatori sancite dal Codice di condotta sono indirizzate anche alle agenzie per l'impiego ("*the code applies to the processing of personal data whether by public or private employers, by workers' representatives or by employment agencies*").
Per tutelare la privacy dei lavoratori in caso di ricorso ad agenzie per l'impiego per il reclutamento di lavoratori, l'art. 13 del Codice ILO prevede che l'*employer* dovrebbe richiedere espressamente all'agenzia per l'impiego di raccogliere e trattare i dati personali dei prestatori in conformità alle previsioni del Codice.

[65] Si rivolgono alle agenzie per l'impiego privato anche i "*Principi generali e linee guida per il reclutamento equo*", uno strumento non vincolante di natura volontaristica che mira alla promozione di pratiche di *fair recruitment* adottato nel *Tripartite Meeting of Experts on Fair Recruitment* del 5–7 settembre 2016.
Tale documento, infatti, accoglie una definizione ampia di "*impresa*" che ricomprende al proprio interno non solo i datori di lavoro, ma anche i reclutatori di manodopera diversi dai servizi pubblici per l'impiego e gli altri fornitori di servizi nell'ambito del processo di reclutamento (v. sezione "*Definizioni e termini*").
Nell'ambito della sezione "*Responsabilità delle imprese e dei servizi pubblici per l'impiego*", al punto 19, viene indicato che le imprese - e, quindi, anche i reclutatori di manodopera - "*dovrebbero rispettare la riservatezza dei lavoratori e garantire la tutela dei loro dati personali*".
In particolare, "*le imprese dovrebbero astenersi dal registrare, in archivi o registri, dati personali che non siano necessari per valutare l'idoneità dei lavoratori, compresi i lavoratori migranti, ai lavori per i quali sono o potrebbero essere assunti o presi in considerazione, o che non siano necessari per facilitare il loro impiego"*.
Viene quindi ribadito anche per le agenzie per l'impiego privato l'*international labour standard* di cui all'art. 6 della Convenzione n. 181/1997, la quale, del resto, viene espressamente richiamata all'interno dell'elenco delle fonti internazionali del lavoro che hanno costituito il punto di riferimento per la redazione del documento.

8. La tutela dei workers' health data nella Raccomandazione n. 171/1985 sui servizi sanitari sul lavoro

Per quanto concerne la protezione riconosciuta dalle fonti primarie dell'ILO ai dati sanitari, la tematica risulta affrontata estensivamente all'interno di Raccomandazioni, e, in misura minore, di Convenzioni[66] aventi ad oggetto la tutela della salute e sicurezza dei lavoratori.

La regolamentazione del trattamento degli *health data* trova, infatti, il proprio "posizionamento naturale" all'interno della materia della salute e della sicurezza sul lavoro, giacché, al fine di assicurarsi che i lavoratori non presentino condizioni di salute tali da esporli a pericoli nell'esercizio della prestazione lavorativa, è necessario eseguire accertamenti che comportano il trattamento di dati di carattere medico-sanitario.

Tuttavia, tali trattamenti presentano rischi significativi in quanto la conoscenza dei dati sanitari del lavoratore può rappresentare un fattore di esposizione a trattamenti svantaggiosi e/o discriminatori[67].

Infatti, lo stato di salute può rappresentare un fattore dirimente nella decisione di procedere all'instaurazione o alla cessazione del rapporto con un determinato lavoratore,

---

[66] Si sta facendo riferimento, in particolare, alla Convenzione n. 124/1965 in tema di "*Medical Examination of Young Persons (Underground Work)*".
L'obiettivo perseguito dalla Convenzione consiste nella predisposizione di norme internazionali dirette a regolamentare gli esami medico-attitudinali a cui devono essere sottoposti gli adolescenti impiegati in lavori sotterranei in cave o miniere (art. 1).
Nello specifico, la Convenzione richiede che i minori di 21 anni siano sottoposti a un esame preventivo approfondito finalizzato a valutarne l'idoneità all'impiego, che deve necessariamente comprendere una radiografia dei polmoni, nonché ad esami periodici realizzati a intervalli non superiori all'anno (art. 2 e 3).
Come stabilito dall'art. 3, tali esami sono effettuati sotto la responsabilità e la sorveglianza di un medico qualificato a ciò autorizzato dall'autorità competente e adeguatamente certificati.
Per quanto più interessa, la citata Convenzione richiede al datore di lavoro di predisporre e conservare, per ciascun lavoratore, dei *records* contenenti gli esiti degli esami che, dietro richiesta, devono essere messi a disposizione degli ispettori del lavoro e dei rappresentanti dei lavoratori.
Tuttavia, per impedire la conoscibilità da parte del datore di lavoro dello stato di salute dei prestatori, nei *record* devono essere conservati solamente certificati che attestino l'idoneità del lavoratore allo svolgimento delle mansioni, ma che non devono riportare alcun dato idoneo a rivelarne lo stato di salute (art. 4).
La soluzione adottata dalla Convenzione n. 124/1965 per rispondere alle contrapposte esigenze di trattamento e di riservatezza degli *health data* è, quindi, quella di precludere al datore di lavoro l'accesso alle informazioni di natura sanitaria.

[67] A causa degli elevati rischi discendenti dal loro trattamento, l'art. 9 del GDPR classifica i dati relativi alla salute come categorie particolari di dati personali (*ex* dati sensibili).

considerato che il datore di lavoro potrebbe non volere la presenza all'interno della propria struttura organizzativa di persone con condizioni di salute non ottimali.

Pertanto, mentre la tutela della salute e sicurezza dei lavoratori presenta un'esigenza conoscitiva delle condizioni di salute dei lavoratori, viceversa, la protezione da trattamenti discriminatori e/o deteriori impone esigenze di riservatezza.

Proprio dalla necessità di comporre la tensione esistente tra le contrapposte esigenze di acquisizione e riservatezza dei dati sanitari discende l'interesse dell'ILO nella regolamentazione del trattamento degli *health data*.

Tale tematica è affrontata estensivamente nella Raccomandazione n. 171/1985 sui servizi sanitari sul lavoro[68], la quale, da un lato, richiede l'esecuzione di accertamenti sullo stato di salute dei lavoratori[69], dall'altro, l'adozione di "*disposizioni per proteggere la vita privata dei lavoratori ed assicurare che il controllo della loro salute non venga utilizzato a fini di discriminazione o in ogni altra maniera lesiva dei loro interessi"* (art. 11, par. 2).

Le modalità con cui la Raccomandazione intende proteggere i dati sanitari dei lavoratori sono diverse.

Innanzitutto, la Raccomandazione suggerisce misure organizzative volte a mantenere i dati sanitari nettamente separate dalle altre tipologie di dati, così da evitare che i terzi, quando ricercano altre informazioni relative al lavoratore possano imbattersi anche in notizie sul suo stato di salute.

---

[68] Ai sensi dell'art. 48, la Raccomandazione completa la Convenzione sui servizi sanitari sul lavoro del n. 161 del 1985, la quale, all'art. 1, definisce i "*servizi sanitari sul lavoro*" come "*un servizio preposto a funzioni essenzialmente preventive ed incaricato di consigliare il datore di lavoro, i lavoratori ed i loro rappresentanti nell'impresa" su: i) i requisiti per stabilire e mantenere un ambiente lavorativo sicuro e salubre, atto a favorire una salute fisica e mentale ottimale in relazione al lavoro; ii) l'adattamento del lavoro alle capacità dei lavoratori, tenuto conto del loro stato di salute fisica e mentale*".

[69] In particolare, secondo quanto precisato dall'art. 11, par. 1, le condizioni di salute dei lavoratori dovrebbero essere valutate: a) prima dell'assegnazione a posti specifici che possano comportare un pericolo per la salute propria o altrui; b) periodicamente, durante ogni impiego che comporti l'esposizione a rischi particolari per la salute; c) al momento della ripresa del lavoro dopo una assenza prolungata per motivi di salute, per determinarne le possibili origini professionali, raccomandare l'azione adeguata per proteggere i lavoratori e determinare se il lavoro sia adatto a loro, e determinare i bisogni di riqualificazione e di riabilitazione; d) al momento della cessazione e dopo la cessazione dell'assegnazione a posti che comportano rischi tali da provocare o da favorire ulteriori danni alla salute.
In ogni caso, il lavoratore deve essere sempre informato dei risultati degli esami sanitari e di valutazione della propria salute in modo da poter far correggere "*ogni dato erroneo o che potrebbe portare ad un errore*" (art. 22, par. 2).

A tal fine, la Raccomandazione richiede la registrazione da parte dei servizi sanitari dei dati relativi alla salute in cartelle sanitarie personali e confidenziali[70] (art. 14, par. 1).
L'ILO, poi, si preoccupa di limitare la possibilità di accedere e diffondere le informazioni sanitarie del lavoratore.
In tal senso, *in primis*, è previsto che il personale che fornisce servizi sanitari sul lavoro dovrebbe avere accesso alle cartelle sanitarie personali solo nella misura in cui l'informazione contenuta sia rilevante per l'esercizio delle sue funzioni e che, qualora le cartelle sanitarie contengano informazioni personali confidenziali di carattere medico, l'accesso alle cartelle andrebbe limitato al personale medico (art. 14, par. 2)[71].
In secondo luogo, per limitare la circolazione dei dati relativi alle valutazioni sanitarie, viene indicato che tali dati andrebbero comunicati a terzi solo con il consenso informato del lavoratore interessato (art. 14, par. 3).
Infatti - seppur, in specifiche circostanze, il lavoratore potrebbe avere interesse a che i risultati delle proprie valutazioni mediche siano resi noti all'esterno del perimetro dei servizi sanitari, ad esempio per poter fruire di eventuali prestazioni, misure o iniziative dirette a sostenere i cittadini-lavoratori in relazione al proprio stato di salute - le decisioni circa la comunicazione delle proprie valutazioni sanitarie, in ossequio al principio di autodeterminazione informativa, dovrebbero essere assunte in modo cosciente e informato dal lavoratore stesso[72].

---

[70] Queste cartelle dovrebbero comprendere informazioni sugli impieghi svolti dai lavoratori, sull'esposizione ai rischi professionali inerenti al loro lavoro e sui risultati di ogni valutazione della loro esposizione a questi rischi.

[71] La Raccomandazione in esame non fornisce, invece, indicazioni precise in merito alle condizioni e alla durata di conservazione delle cartelle sanitarie personali, alle condizioni di trasferimento e di comunicazione nonché alle misure richieste per preservarne il carattere confidenziale, in particolare qualora le informazioni contenute nelle cartelle sanitarie vengano informatizzate, richiedendo che tali aspetti siano stabiliti dalla legislazione nazionale o dall'autorità competente, o disciplinati da direttive etiche riconosciute, conformemente alla prassi nazionale (art. 15).
L'unica indicazione che si rinviene nella Raccomandazione è quella secondo cui i dati personali relativi alle valutazioni della salute andrebbero comunicati a terzi solo con il consenso informato del lavoratore interessato (art. 14, par. 3).

[72] Anche se, in specifiche ipotesi, è la stessa Raccomandazione a prevedere che determinate informazioni inerenti alla salute del lavoratore dovrebbero essere comunicate all'autorità competente prescindendo dal consenso del lavoratore interessato.
A titolo di esempio, qualora il controllo della salute abbia portato a individuare una malattia professionale, questa malattia andrebbe notificata all'autorità competente, conformemente alla legislazione e alla prassi nazionale.
In questo caso, i lavoratori – oltre ai loro rappresentanti e il datore di lavoro - dovrebbero essere solamente informati a titolo conoscitivo dell'avvenuta notifica (art. 18).

Indicazioni ancora più stringenti sono stabilite per quanto riguarda l'accesso alle informazioni sanitarie da parte del datore di lavoratore.

Per contrastare il rischio di utilizzo improprio delle informazioni, il medico che effettuato un esame prescritto per determinare l'attitudine di un lavoratore ad un lavoro che comporti l'esposizione ad un rischio particolare dovrebbe comunicarne per iscritto al datore di lavoro solamente le relative conclusioni (art. 16, par. 1).

Le conclusioni comunicate al datore di lavoro non dovrebbero riportare alcun dato di natura medica, ma, a seconda dei casi, potrebbe indicare l'attitudine del lavoratore per l'assegnazione prevista oppure specificare i tipi di lavoro e le condizioni lavorative medicalmente controindicate, in modo temporaneo o permanente (art. 16, par. 2)[73].

La soluzione raccomandata dall'ILO è, quindi, quella di rendere edotto il datore di lavoro solamente delle ricadute sulle modalità di svolgimento dell'attività lavorativa derivanti dalle risultanze dell'accertamento, precludendogli, invece, l'acquisizione delle risultanze sanitarie sulla base delle quali il medico ha adottato le proprie conclusioni.

In questo modo, il datore di lavoro non viene a conoscenza di dati di natura medica, ma di sole informazioni rilevanti ai fini dell'organizzazione della struttura produttiva.

A garanzia della riservatezza dei dati sanitari, la Raccomandazione introduce due ulteriori principi: la salvaguardia dell'indipendenza professionale (art. 37, par. 1) e la soggezione al segreto professionale del personale che fornisce servizi sanitari sul lavoro (art. 38).

Quanto all'indipendenza professionale dei servizi sanitari, questa risulta funzionale non solo a garantire la correttezza e l'obiettività delle funzioni svolte, ma anche ad assicurare che il personale possa godere dell'autonomia necessaria a resistere di fronte a richieste del datore di lavoro volte a reperire indebitamente informazioni sullo stato di salute dei prestatori[74].

In questo modo, risulta rafforzata l'ulteriore garanzia rappresentata dal segreto professionale rispetto ai dati medici e tecnici conosciuti nello svolgimento delle proprie

[73] Qualora, poi, dovesse emergere che il mantenimento di un lavoratore in un posto di lavoro particolare sia controindicato, i servizi sanitari sul lavoro dovrebbero contribuire all'individuazione di un altro posto di lavoro nella stessa impresa, o ad ogni altra soluzione adeguata (art. 17).

[74] A tale scopo, l'autorità competente, se necessario e conformemente alla legislazione e alla prassi nazionale, dovrebbe specificare le condizioni relative all'assunzione ed al licenziamento del personale dei servizi sanitari sul lavoro, in consultazione con le organizzazioni rappresentative dei datori di lavoro e dei lavoratori interessate (art. 37, par. 2).

funzioni, al quale tutto il personale del servizio sanitario sul lavoro dovrebbe essere soggetta, salve deroghe previste dalla legislazione nazionale.

8.1. Altre Raccomandazioni inerenti al trattamento dei dati sanitari dei lavoratori

Sebbene sia solamente la Raccomandazione n. 171/1985 a presentare un quadro regolatorio approfondito di tutela dei dati sanitari dei lavoratori, vi sono anche altre Raccomandazioni che contengono disposizioni rilevanti.

Si tratta di Raccomandazioni che contengono previsioni di approfondimento e adattamento delle regole generali relative agli esami sanitari in ragione della sussistenza di particolari rischi ambientali (quali l'esposizione ad amianto, a prodotti chimici, inquinamento atmosferico, rumore e vibrazioni), di speciali condizioni di vulnerabilità psico-fisica (minori) o delle peculiarità proprie dell'attività svolta (lavoratori portuali, infermieri e *domestic workers*).

Ai fini dell'esposizione si partirà dall'esame delle disposizioni rilevanti ai fini della tutela dei dati sanitari contenute in Raccomandazioni dedicate alla protezione dei lavoratori esposti a particolari rischi ambientali (Raccomandazione n. 172/1986 sulla sicurezza nell'utilizzo dell'amianto, Raccomandazione n. 177/1990 sulla sicurezza nell'utilizzo dei prodotti chimici e Raccomandazione n. 156/1997 sull'ambiente di lavoro – inquinamento atmosferico, rumore e vibrazioni).

Cominciando dalla Raccomandazione n. 172/1986, questa richiede l'adozione di test e esami medici specifici finalizzati a rivelare l'esistenza di effetti clinici o preclinici derivanti dall'esposizione dei lavoratori all'amianto (sezione IV - Controllo dell'ambiente di lavoro e della salute dei lavoratori)[75].

---

[75] A fini di controllo dell'ambiente di lavoro e della salute dei lavoratori, "*nei casi decisi dall'autorità competente, il datore di lavoro prenderà disposizioni per il controllo sistematico delle concentrazioni di polveri di amianto in sospensione nell'aria dei luoghi di lavoro, per il controllo sistematico della durata e del livello di esposizioni dei lavoratori all'amianto, e per il controllo della salute dei lavoratori*" (art. 29). In particolare, ai sensi dell'art. 31, par. 1 e 2, "*per la prevenzione delle malattie e dei danni funzionali in relazione all'esposizione all'amianto, tutti i lavoratori assegnati ad un lavoro che comporti l'esposizione all'amianto dovrebbero beneficiare, a seconda dei casi: a) di un esame medico preliminare all'assegnazione; b) di esami medici periodici ad intervallo adeguato; c) di altri test e esami, in particolare la radiografia del torace e le prove di funzione respiratoria, che potrebbero essere necessarie per controllare lo stato di salute in relazione al rischio professionale, e per identificare i segni precoci di una malattia causata dall'amianto.*
Gli intervalli tra gli esami medici andrebbero determinati dall'autorità competente, tenuto conto del livello di esposizione e dello stato di salute del lavoratore in relazione al rischio professionale".

Tale Raccomandazione prevede espressamente che i lavoratori sottoposti a controllo dello stato di salute dovrebbero avere "*il diritto al rispetto della riservatezza delle informazioni personali e mediche*" (art. 38, par. 1, lett. a)[76], dovendo i risultati degli esami medici essere utilizzati con l'esclusiva finalità di determinare lo stato di salute in relazione all'esposizione all'amianto (art. 31, par. 6) e, eventualmente, a seconda dei casi, di prevenire o ridurre l'esposizione dei lavoratori interessati (art. 31, par. 7) e/o di facilitare l'assegnazione del lavoratore ad un lavoro compatibile con le condizioni mediche (art. 31, par. 7)[77].

La Raccomandazione, inoltre, richiede la conservazione di dati sanitari del lavoratore per un lungo periodo di tempo.

È infatti indicato che, "*i registri del controllo dell'esposizione dei lavoratori, insieme agli elementi delle loro cartelle sanitarie relativi ai rischi di danni alla salute dovuti all'esposizione all'amianto e alle radiografie del torace, andrebbero conservati per almeno trent'anni dopo la cessazione di un incarico che comporti l'esposizione all'amianto*" (art. 36).

In caso di chiusura di una impresa o dopo la cessazione del rapporto di lavoro, tali registri e informazioni "*andrebbero depositati, conformemente alle direttive dell'autorità competente*" (art. 38).

Prima facie, la scelta di legittimare il mantenimento di informazioni relative ai lavoratori per un significativo arco temporale, anziché procedere alla loro cancellazione o

---

Oltre ai predetti esami, considerato che alcune malattie legate all'amianto si caratterizzano per la lungo-latenza, "*l'autorità competente dovrebbe garantire che, conformemente alla legislazione e alla prassi nazionale, vengano prese disposizioni perché i lavoratori possano continuare a beneficiare di esami medici adeguati dopo la cessazione di una attività che comporti l'esposizione all'amianto*" (art. 31, par. 3).
In ogni caso, al lavoratore dovrebbe essere riconosciuto il diritto a rifiutare l'applicazione di procedure mediche invadenti che potrebbero danneggiarne integrità fisica (art. 31, par. 8, lett. c).

[76] Dal punto di vista pratico, tuttavia, garantire il diritto alla riservatezza delle informazioni mediche potrebbe risultare difficoltoso in quanto la valutazione di inidoneità allo svolgimento di mansioni che implicano l'esposizione ad amianto può, seppur indirettamente, far presumere l'esistenza o il rischio di insorgenza di una patologia absesto correlata.
Inoltre, l'art. 36 prevede che l'insorgenza di una malattia professionale causata dall'amianto andrebbe notificata all'autorità competente, conformemente alla legislazione e alla prassi nazionale. Seppur nulla venga specificato sul punto, si ritiene che, per meglio garantire il diritto alla riservatezza, siffatta segnalazione, ove comporti la rivelazione di informazioni sanitarie del lavoratore, dovrebbe essere effettuata dal personale medico.

[77] Qualora ciò non sia possibile, dovrebbero essere riconosciuti "*mezzi alternativi per conservare il reddito*" (art. 34) e "*un risarcimento per i lavoratori che contraggano una malattia o presentino una invalidità funzionale dovuta all'esposizione professionale all'amianto*" (art. 35).

anonimizzazione, potrebbe apparire una soluzione meno favorevole per i lavoratori.
Tuttavia, a ben vedere, la richiesta di conservazione dei dati personali trova la propria giustificazione nella circostanza che, come noto, le patologie absesto correlate possono presentare lunghi periodi latenza.
Pertanto, la possibilità di reperire informazioni mediche anche a lunga distanza di tempo può risultare utile ai fini dell'accertamento dell'eziologia professionale della patologia insorta.
Un altro strumento che contiene previsioni relative alla tutela dei dati sanitari di lavoratori sottoposti a particolari rischi ambientali è la Raccomandazione n. 177/1990 sulla sicurezza nell'utilizzo dei prodotti chimici.
L'art. 18 della Raccomandazione, infatti, si occupa della gestione delle cartelle mediche personali redatte all'esito degli accertamenti sanitari finalizzati alla valutazione dello stato di salute dei lavoratori in relazione all'esposizione ai prodotti chimici pericolosi[78].
A tal riguardo, l'art. 18, par. 6, richiede il rispetto "*del carattere confidenziale delle cartelle mediche personali … secondo i principi generalmente accettati dell'etica medica*".
Una deroga espressa alla riservatezza dei risultati contenuti nelle cartelle mediche è, tuttavia, contenuta nell'art. 18, par. 8, il quale prevede che i predetti risultati "*andrebbero resi disponibili per preparare statistiche sanitarie e studi epidemiologici*" utili a favorire l'identificazione e il controllo delle malattie professionali.
In tal caso, vi è comunque un recupero della privacy del lavoratore "a valle", essendo previsto che gli studi statistici e epidemiologici eventualmente svolti a partire dai contenuti delle cartelle mediche devono garantire l'anonimato dei lavoratori.
Pertanto, gli studi devono essere realizzati e diffusi in modo da non consentire in alcun modo di poter risalire alle condizioni di salute di singoli lavoratori.

---

[78] Ai sensi dell'art. 18, "*il datore di lavoro o l'istituzione competente in virtù della legislazione e della prassi nazionale dovrebbero essere tenuti a prendere disposizioni, secondo un metodo conforme alla legislazione e alla prassi nazionale, per il controllo medico dei lavoratori qualora necessario: a) per la valutazione dello stato di salute dei lavoratori in relazione ai rischi risultanti dall'esposizione ai prodotti chimici; b) per la valutazione delle malattie e delle lesioni legate al lavoro risultanti dall'esposizione ai prodotti chimici pericolosi*" (par. 1).
"*Qualora i risultati dei test o degli esami medici rivelino l'esistenza di effetti clinici o preclinici, andrebbero prese misure per prevenire o per ridurre l'esposizione dei lavoratori interessati e per impedire un ulteriore deterioramento della loro salute*" (par. 2).
"*I risultati degli esami medici andrebbero utilizzati per determinare lo stato di salute in relazione all'esposizione ai prodotti chimici, e non andrebbero utilizzati per discriminare il lavoratore*" (par. 3).

A differenza della Raccomandazione n. 172/1986 sull'amianto, non vengono fornite indicazioni specifiche sulla conservazione delle cartelle, essendo rimesso all'autorità competente il compito di stabilire il periodo e i soggetti tenuti alla conservazione. In ogni caso, dovrebbe essere garantito ai lavoratori il diritto di accesso alla propria cartella medica, esercitabile "*di persona o tramite il proprio medico*" (art. 18, par. 5). Da ultimo, disposizioni sulla tutela dei dati sanitari contenute in Raccomandazioni finalizzate alla tutela dei lavoratori esposti a particolari rischi ambientali si rinvengono anche nella Raccomandazione n. 156/1997 *on Working Environment (Air Pollution, Noise and Vibration)*.

L'art. 18 - contenuto nella sezione III della Raccomandazione dedicata al controllo della salute dei lavoratori – richiede all'autorità competente di sviluppare e determinare le modalità di funzionamento del sistema di registrazione delle informazioni mediche ricavate dalla sottoposizione dei lavoratori alla sorveglianza sanitaria[79].

In particolare, l'autorità competente dovrebbe prevedere la conservazione dei registri sanitari per un appropriato periodo di tempo per la realizzazione di studi epidemiologici e altre attività di ricerca.

Per coniugare le finalità di ricerca con la tutela della riservatezza dei dati sanitari dei lavoratori, l'art. 18 richiede che i singoli lavoratori a cui si riferiscono le informazioni mediche dovrebbero essere identificabili "*by the competent autorithy only*".

Inoltre, come si ricava dall'art. 16, par. 2, l'accesso ai risultati degli esami e dei test andrebbe riconosciuto anche ai lavoratori interessati e, su loro richiesta, al loro medico personale.

Disposizioni rilevanti si ritrovano anche all'interno della Raccomandazione n. 79 del 1946, la quale dedica una apposita regolamentazione agli esami medici di bambini e adolescenti, richiedendo, in ragione della loro speciale vulnerabilità psico-fisica, l'esecuzione di approfonditi accertamenti[80].

---

[79] L'art. 16 della Raccomandazione richiede che la supervisione della salute dei lavoratori dovrebbe includere, secondo quanto stabilito dall'autorità competente: a) una visita medica preassuntiva; b) visite mediche periodiche a intervalli adeguati; c) test o indagini biologiche o di altro tipo che potrebbero essere necessarie per controllare il grado di esposizione e lo stato di salute del lavoratore interessato; d) visite mediche o test o indagini biologiche dopo la cessazione dell'incarico che, se indicato dal punto di vista medico, dovrebbero essere resi disponibili regolarmente e per un periodo prolungato.

[80] Tali esami - individuati approfonditamente nella sezione II della Raccomandazione - dovrebbero essere svolti da un corpo di medici esaminatori specializzati in igiene industriale e in possesso di comprovata esperienza rispetto alle problematiche di salute proprie di bambini e adolescenti (art. 11).

Questa opera una distinzione tra i servizi di medicina esecutori degli esami e il datore di lavoro per quanto riguarda il grado di conoscenza dei dati personali dei lavoratori.
Infatti, da un lato, viene richiesto che gli esiti integrali degli esami siano riportati all'interno di una scheda da conservare negli archivi dei servizi di medicina responsabili della conduzione degli esami (art. 6, par. 1); dall'altro, viene richiesta la redazione di un certificato medico destinato al datore di lavoro, il quale dovrebbe indicare in maniera sufficientemente esplicita i limiti all'idoneità al lavoro rilevati nelle visite e le misure di precauzione che, alla luce delle risultanze degli esami, dovrebbero essere adottate con riguardo alle condizioni di lavoro.
Tuttavia, nel certificato non dovrebbero essere in nessun caso riportate informazioni confidenziali quali la diagnosi di difetti congeniti o malattie (art. 6, par. 2).
Pertanto, la Raccomandazione distingue tra documentazione completa sullo stato di salute del datore di lavoro, conservata dai servizi sanitari, e documentazione "parziale" priva di informazioni confidenziali di natura medica destinata al datore di lavoro.
Passando all'analisi del contenuto di Raccomandazioni dedicate alla protezione delle particolari categorie di lavoratori, disposizioni rilevanti in merito alla protezione dei dati sanitari si rinvengono nelle Raccomandazioni n. 157/1977 sul personale infermieristico, n. 160/1979 sulla salute e sicurezza dei lavoratori portuali e n. 201/2011 sui lavoratori domestici.
La Raccomandazione sul personale infermieristico[81] contiene cenni sulla tutela degli *health data* all'interno dell'art. 47, contenuto nella sezione IX dedicata alla tutela della salute sul lavoro.
Ai sensi del citato articolo, deve essere assicurata la "*confidentiality*" degli esami svolti dal personale infermieristico (par. 3)[82], fermo restando che, come previsto dall'art. 48, par. 2, l'insorgenza di malattie professionali o che potrebbero essere tali dovrebbe essere

[81] Il personale che fornisce assistenza e servizi infermieristici dovrebbe essere sottoposto a *medical examinations* al momento dell'assunzione, ad intervalli regolari durante l'impiego e alla cessazione dello stesso (art. 47, par. 1).
Se, poi, il personale infermieristico lavora regolarmente in circostanze che comportano rischi concreti per la loro salute o per quella delle persone con cui entrano in contatto, la sottoposizione agli esami dovrebbe avvenire regolarmente ad intervalli appropriati rispetto alla tipologia del rischio implicato (art. 47, par. 2).

[82] L'art. 55, contenuto nella sezione X – *Social security*, prevede anche che, laddove il sistema di sicurezza sociale attribuisca la libera scelta del medico e dell'istituzione sanitaria, anche il personale infermieristico dovrebbe godere della stessa facoltà di scelta, fermo restando che le loro cartelle cliniche dovrebbero rimanere riservate.

oggetto di notifica all'autorità competente.

È inoltre previsto che, al fine di assicurare l'oggettività e l'indipendenza degli accertamenti, il personale che conduce gli esami non dovrebbero essere eseguiti "*by doctors with whom the person examined have a close working relationship*" (art. 47, par. 3).

Quanto alla Raccomandazione n. 160/1979 sulla tutela della salute e sicurezza nel lavoro portuale[83], l'art. 26 prevede che i risultati delle *medical examinations and investigations* prescritte dall'art. 36 della relativa Convenzione[84] dovrebbero essere comunicati al lavoratore interessato (par. 1).

Invece, al datore di lavoro dovrebbe essere comunitato se il lavoratore sia "*fit for the work to be carried out and whether he may constitute a risk to other persons on the condition that, subject to Article 39 of the Convention, the confidential character of the information is respected*". La Raccomandazione, quindi, ribadisce il carattere confidenziale dei dati sanitari, fatta eccezione per quanto previsto dall'art. 39 della Convenzione n. 152/1979 sul lavoro portuale, il quale richiede che gli infortuni e le malattie professionali che colpiscono i lavoratori portuali vengano notificati all'autorità competente.

Particolarmente significative sono anche le previsioni della Raccomandazione n. 201/2011 relativa al lavoro dignitoso di lavoratrici e i lavoratori domestici.

Tale Raccomandazione tutela la riservatezza dei dati sanitari dei *domestic workers*[85] attraverso una tecnica regolativa che costituisce un *unicum* all'interno delle fonti dell'ILO.

---

[83] I lavoratori portuali sono definiti come i lavoratori impegnati in qualsivoglia fase dell'attività di carico o scarico di qualsiasi nave o in lavori collegati (art. 1).

[84] L'art. 36 della Convenzione n. 152/1979 sul lavoro portuale richiede che ciascuno Stato determini, mediante leggi, regolamenti nazionali o altri metodi appropriati coerenti con le pratiche e le condizioni nazionali, previa consultazione con le organizzazioni dei datori di lavoro e dei lavoratori interessate: a) per quali rischi lavorativi deve essere condotta una visita medica iniziale o visite mediche periodiche, o entrambe tali tipologie di visite; b) tenuto conto della natura e del grado del rischio e delle particolari circostanze, gli intervalli massimi entro i quali devono essere effettuate le visite mediche periodiche; c) nel caso di lavoratori esposti a particolari rischi per la salute sul lavoro, la gamma di indagini speciali ritenute necessarie; d) misure adeguate per la fornitura di servizi di medicina del lavoro (par. 1).
I *records* delle visite e degli accertamenti medici devono rimanere confidenziali (par. 3).

[85] Ai sensi dell'art. 1 della Raccomandazione, le relative disposizioni completano quelle della Convenzione sulle lavoratrici e i lavoratori domestici n. 189/2011, la quale precisa che con "*lavoro domestico*" si intende "*il lavoro svolto in o per una o più famiglie*, mentre l'espressione "*lavoratore domestico*" indica "*ogni persona che svolge un lavoro domestico nel quadro di una relazione di lavoro*", mentre "*una persona che svolga un lavoro domestico in maniera occasionale o sporadica, senza farne la propria professione, non è da considerarsi lavoratore domestico*" (art. 1 della Convenzione).

Infatti, la Raccomandazione, all'art. 3[86], non individua specifiche misure tecniche e organizzative preordinate alla protezione della confidenzialità dei sanitari, ma richiede il rispetto delle pertinenti norme internazionali del lavoro, e, *in primis*, del *Code of practice on the protection of workers' personal data*.

Considerato il richiamo espresso operato dall'art. 3, si ritiene rilevante approfondire le disposizioni del Codice di condotta ILO dedicate al trattamento dei *medical data*, in parte già accennate nelle sezioni 1.3 e 1.4. dell'elaborato.

Tali previsioni, in parte, ricalcano quanto previsto dalla precedente Raccomandazione sui servizi sanitari sul lavoro n. 171/1985, la quale, del resto, è stata tenuta in considerazione dal gruppo di esperti che ha elaborato il Codice ILO come si evince dai numerosi riferimenti alla stessa contenuti nel Commentario (pagg. 16, 18, 20 e 23).

Il Codice di condotta stabilisce cautele particolari in merito alla raccolta, conservazione e comunicazione dei dati sanitari.

Ai sensi dell'art. 6, par. 7, la raccolta dei dati sanitari dovrebbe essere vietata, a meno che non ricorrano tre basi giuridiche alternative: a) necessità di determinare se il lavoratore è idoneo a un particolare impiego; b) necessità di adempiere ad obblighi in materia di salute e sicurezza sul lavoro; c) necessità di determinare se il lavoratore è in possesso dei requisiti richiesti per accedere a *social benefits*.

In presenza di tali condizioni di liceità del trattamento, la raccolta dei dati dovrebbe comunque avvenire in conformità alla legislazione nazionale, al segreto medico e ai principi generali in materia di salute e sicurezza sul lavoro.

Quanto alla conservazione, i dati personali coperti da segreto medico dovrebbero essere conservati esclusivamente da personale vincolato al rispetto delle norme sul segreto medico e separatamente da tutti gli altri dati personali (art. 8, par. 2)[87].

---

[86] Per la precisione, l'art. 3 prevede che "*i Membri, conformemente alle norme internazionali del lavoro, dovrebbero fra l'altro: a) garantire che il sistema degli esami medici relativo al lavoro rispetti il principio della confidenzialità dei dati personali e della vita privata dei lavoratori domestici e che sia conforme al Codice di condotta dell'ILO sulla tutela dei dati personali dei lavoratori del 1997 e alle altre norme internazionali rilevanti in materia di protezione dei dati; b) prevenire qualsiasi forma di discriminazione legata a tali esami; c) garantire che i lavoratori domestici non siano in nessun caso tenuti a sottoporsi ad un test sull'HIV o ad un test di gravidanza, o a divulgare il proprio stato sierologico o di gravidanza*" (traduzione a cura dell'Ufficio ILO di Roma).

[87] Il Commentario al Codice ILO, a pag. 19, chiarisce che "*medical data should, as is already done in most countries, be kept separately from all other information related to workers … Their storage should be handled exclusively by specialized personnel bound by the rules of medical secrecy. To eliminate possible misunderstanding, section 6.7 clarifies that the reference to medical data applies only to those data which have been collected by persons acting under medical confidentiality*".

Da ultimo, rispetto alla comunicazione dei dati sanitari, il Codice del 1997 nella sostanza riprende quanto già stabilito dall'art. 16 della Raccomandazione n. 171/1975, prevedendo che, qualora i lavoratori siano sottoposti a una visita medica, il datore di lavoro dovrebbe essere informato soltanto delle conclusioni rilevanti per la specifica decisione da assumere (art. 10, par. 8).

Tali conclusioni non dovrebbero contenere informazioni di natura medica, ma queste, a seconda dei casi, potrebbero indicare l'idoneità all'incarico proposto o specificare i tipi di lavoro e le condizioni di lavoro che sono controindicate dal punto di vista medico, sia temporaneamente che permanentemente (art. 10, par. 9).

Invece, il lavoratore interessato dovrebbe sempre avere il diritto di accedere ai dati medici che lo riguardano anche attraverso un medico di propria fiducia (art. 11, par. 6).

8.2. Gli standards di tutela dei dati sanitari dei lavoratori ricavabili dalle fonti dell'ILO

Esaurita la trattazione delle disposizioni rilevanti in tema di riservatezza dei dati sanitari dei lavoratori, risulta possibile provare ad enucleare gli *standards* internazionali di tutela dei dati sanitari dei lavoratori ricavabili "dall'intreccio" delle fonti dell'ILO.

Gli *standards* minimali di protezione richiesti dall'ILO che sembra potersi rinvenire sono i seguenti:

- il trattamento dei dati sanitari dei lavoratori dovrebbe essere limitato al ricorrere di finalità specifiche ed eccezionali quali accertamento dell'idoneità a uno specifico impiego, valutazione dell'esposizione a specifici fattori di rischio occupazionali, adempimento di obblighi in materia di salute e sicurezza, accesso a benefici e prestazioni sociali, informazione alle autorità pubbliche competenti

Per prevenire i rischi connessi all'informatizzazione dei dati sanitari, viene specificato che "*while the code does not prohibit computerizing certain particularly sensitive data, such as medical and psychological data, problems can arise if the entire record is not included. Special attention, therefore, must be paid to the computerized storage of personal data which presents several dangers: the record on computer may be incomplete, the use of key words to characterize data may be misleading, selected data may be transferred from one file to another, and access to the data may not be as easily controlled as with manual files. These risks can only be avoided if computerized storage is not limited to the data but comprises the entire context in which they are mentioned*".

circa l'insorgenza di malattie professionali, realizzazione di studi statistici e epidemiologici generali ed anonimi;

- i dati relativi alla salute non possono essere utilizzati per fini di discriminazione o, comunque, in ogni altra maniera lesiva dei loro interessi;
- nei casi in cui è ammesso, il trattamento dei dati sanitari dovrebbe essere eseguito da parte di personale facente parte dei servizi sanitari per il lavoro specializzato, indipendente e vincolato alla riservatezza dal segreto medico;
- i servizi sanitari sul lavoro dovrebbero conservare i dati personali in cartelle individuali e separate rispetto agli altri dati del lavoratore;
- i dati devono essere conservati per un periodo congruo rispetto alle finalità per cui sono stati raccolti, ma in determinati casi possono essere richiesti periodi di conservazione più lunghi, come per l'utilizzo in studi epidemiologici;
- l'accesso alle cartelle sanitarie dovrebbe essere sempre consentito al lavoratore, eventualmente tramite suoi rappresentanti;
- l'accesso alle cartelle sanitarie è consentito al personale specializzato dei servizi sanitari sul lavoro se necessario allo svolgimento delle loro funzioni;
- il datore di lavoro non dovrebbe venire a conoscenza delle condizioni di salute del lavoratore;
- la comunicazione e circolazione dei dati sanitari dovrebbero essere limitate e avvenire solo previo consenso informato e libero del lavoratore, salvo al ricorrere di specifiche circostanze quali la necessità di notificare infortuni e malattie professionali all'autorità competente.

8.3. HIV/AIDS e tutela della privacy dei lavoratori

La Raccomandazione n. 200/2010 richiede la predisposizione in favore dei lavoratori[88] di misure di prevenzione, trattamento e assistenza finalizzate a contrastare lo sviluppo

[88] La Raccomandazione presenta un ambito applicativo particolarmente ampio, trovando applicazione in sede di accesso, svolgimento e cessazione di qualsivoglia prestazione *lato sensu* lavorativa (cfr. artt. 10 e 11). Infatti, la Raccomandazione si applica "*a) a tutti i lavoratori che prestano la loro opera in qualunque forma, a seguito di qualunque genere di accordo e in qualunque luogo di lavoro, vale a dire: i) le persone che svolgono qualunque tipo di impiego o esercitano qualunque professione; ii) le persone in corso di formazione professionale, quali tirocinanti, apprendisti e stagisti; iii) i volontari; iv) le persone che sono in cerca di lavoro o presentano domanda d'impiego; v) i lavoratori in mobilità o cassa integrazione; b) a*

dell'HIV/AIDS[89], epidemia particolarmente diffusa tra persone in età lavorativa già svantaggiate o emarginate, con danni significativi anche per l'economia degli Stati maggiormente colpiti.

La Raccomandazione contiene un ampio apparato regolativo dedicato alla tutela della riservatezza[90].

---

tutti i settori dell'attività economica, pubblica e privata, formale e informale; c) agli appartenenti alle forze armate e a tutti i servizi in uniforme" (art. 2).

[89] Come noto, con la sigla HIV si identifica l'agente virale che determina l'insorgenza della sindrome da immunodeficienza acquisita (AIDS), ossia la fase conclamata dell'infezione da HIV.

[90] La Raccomandazione è stata adottata a quasi dieci anni dall'elaborazione del *Code of practice on HIV/AIDS and the world of work* del 2001, funzionale a fornire linee guida e orientamenti pratici per la prevenzione, gestione e mitigazione dell'impatto dell'HIV/AIDS sul mondo del lavoro, l'assistenza dei lavoratori colpiti e l'eliminazione dello stigma e della discriminazione connessi allo stato di sieropositività reale o percepito (art. 1).
Già il Codice di condotta individua la tutela della riservatezza dello stato sierologico del lavoratore come uno dei propri *key principles*, indicando che "*non esiste alcuna giustificazione per la richiesta ad un lavoratore o a chi fa domanda di assunzione di rivelare informazioni personali in materia di HIV; né si possono obbligare i lavoratori a rivelare dette informazioni personali a proposito di un collega. L'accesso ai dati personali legati alla condizione di sieropositività di un lavoratore deve essere vincolato alle disposizioni in materia di riservatezza, in conformità al codice di condotta dell'ILO sulla tutela dei dati personali dei lavoratori, 1997*" (sez. 4, par. 7).
Il *key principle* di tutela della riservatezza è ripreso e sviluppato in più parti del *Code of practice*.
In primo luogo, il Codice afferma la centralità del ruolo ricoperto dai servizi sanitari sul lavoro, richiedendo che le informazioni sui lavoratori attinenti all'HIV/AIDS siano "*strettamente confidenziali e conservate solamente nelle cartelle cliniche che consentono un accesso alle informazioni conforme alla Raccomandazione sui servizi sanitari sul lavoro, 1985 (n.171), nonché alla legislazione e alla prassi nazionale. L'accesso a dette informazioni deve essere limitato al personale sanitario e tali informazioni devono essere svelate solo in presenza di un mandato legale o con il consenso della persona interessata*" (sez. 5 "*Diritti e responsabilità generali*", par 2 "*i datori di lavoro e le loro organizzazioni*", lett. g).
Per favorire l'effettività della confidenzialità delle informazioni è richiesta la predisposizione di apposite iniziative formative in materia di privacy. In tal senso, "*gli addetti alla salute e la sicurezza devono ricevere una formazione specialistica al fine di … garantire che le informazioni in materia di HIV/AIDS, se esistenti, vengano conservate in condizioni di stretta riservatezza, come nel caso degli altri dati clinici riguardanti i lavoratori, e che vengano svelate solo in conformità con il codice di condotta ILO sulla protezione dei dati personali dei lavoratori*" (sez. 7 "*Formazione mirata*", par. 4 "*Formazione mirata per gli addetti alla salute e la sicurezza*"). Anche i rappresentanti dei lavoratori "*devono ricevere una formazione durante l'orario lavorativo, dunque retribuita, finalizzata a … garantire la riservatezza delle informazioni che possono acquisire sui lavoratori affetti da HIV/AIDS nel corso dello svolgimento delle loro funzioni di rappresentanza*" (sez. 7, "*Formazione mirata*", par. 3 "*Formazione mirata per i rappresentanti dei lavoratori*").
Viene, poi, specificata la diversa ampiezza del diritto di accesso, a seconda che sia esercitato dal lavoratore o dalle rappresentanze dei lavoratori. Mentre i lavoratori godono di un diritto di accesso pieno ai propri dati personali e alle proprie cartelle cliniche, le organizzazioni dei lavoratori, nell'esercizio delle proprie responsabilità e delle funzioni sindacali, possono avere accesso ai dati relativi alla condizione di sieropositività di un lavoratore solamente rispettando le "*regole di riservatezza e il requisito del consenso della persona interessata, come sanciti nella Raccomandazione sui servizi sanitari sul lavoro, 1985 (n. 171)*" (sezione 5 "*Diritti e responsabilità generali*", par. 3 "*I lavoratori e le loro organizzazioni*", lett. j).
Il dovere di mantenere la riservatezza dei dati clinici è esteso anche ai soggetti terzi, come gli enti di sicurezza sociale generali, aziendali e di categoria, ai quali viene richiesto di conformare il proprio operato

In tale contesto, la protezione della privacy è funzionale a prevenire fenomeni di stigmatizzazione sociale e/o discriminazione occupazionale[91] connessi allo stato, reale o presunto, di soggetto affetto da HIV/AIDS.

Inoltre, in assenza di siffatte tutele, i lavoratori potrebbero rinunciare a effettuare i test sierologici o a partecipare ad altre iniziative a causa del timore di subire ripercussioni negative in caso di emersione del proprio stato di sieropositività. In questo modo, l'efficacia delle misure predisposte in favore dei lavoratori finirebbe per diminuire, se non per essere vanificata.

Passando all'esame delle disposizioni rilevanti, la Raccomandazione - nell'enunciare i principi generali che devono guidare le azioni intraprese dagli Stati nell'ambito della risposta nazionale di contrasto all'HIV/AIDS nel mondo del lavoro - stabilisce che "*occorre tutelare la privacy dei lavoratori, delle loro famiglie e delle persone a loro carico, e garantire la riservatezza delle informazioni su HIV/AIDS, in particolare quelle relative allo stato sierologico*" (art. 3, par. 1, lett. h)[92], non dovendosi imporre ai lavoratori "*di effettuare il test HIV o rivelare il proprio stato sierologico*" (art. 3, par. 1, lett. i). L'ampiezza dei soggetti a cui viene riconosciuto il diritto alla riservatezza, esteso anche alla famiglia e alle persone a carico, ben testimonia come l'ILO affronti il tema dell'HIV/AIDS nel mondo del lavoro come un problema non solo individuale del singolo lavoratore, ma anche del relativo nucleo familiare. Infatti, la conoscenza dello stato di sieropositività di un lavoratore può portare effetti negativi anche per i familiari. Tali effetti negativi potrebbero consistere sia nella stigmatizzazione e emarginazione

---

a quanto indicato nel codice di condotta dell'ILO sulla tutela dei dati personali dei lavoratori (sez. 9 "*Assistenza e sostegno*", par. 7 "*Privacy e riservatezza*", lett. b).
In ogni caso, la partecipazione del lavoratore alle iniziative in materia di contrasto all'HIV/AIDS - le quali possono comportare trattamenti di dati personali - devono avvenire su base autenticamente volontaria e previo consenso informato del lavoratore (sez. 5, par. 2, lett. l). Il lavoratore, quindi, deve poter si determinare in piena libertà, conoscendo preventivamente tutti gli elementi e tutte le possibili implicazioni della partecipazione alle iniziative.
Infine, è richiesto che i test devono siano effettuati in condizioni di estrema riservatezza da personale adeguatamente qualificato e, di norma, al di fuori del luogo di lavoro. Ciò in quanto, diversamente, risulterebbe accresciuto il rischio che i risultati del test possano essere conosciuti all'interno dell'ambiente lavorativo e utilizzati per scopi discriminatori.

[91] Il termine "*stigma*" indica "*il pregiudizio sociale che, associato ad una persona affetta da HIV, solitamente ne determina l'emarginazione o ne pregiudica la possibilità di godere appieno della vita sociale*" (art. 1, par. 1, lett. d); mentre per "*discriminazione*" si intende "*qualsiasi forma di distinzione, esclusione o preferenza che ha per effetto di negare o di alterare l'uguaglianza di possibilità o di trattamento in materia d'impiego o di professione*" (art. 1, par. 1, lett. e).

[92] Traduzione italiana a cura della Lega Italiana per la Lotta contro l'AIDS (LILA).

dell'intero gruppo sociale sia nella perpetrazione di discriminazioni lavorative ai danni dei familiari del lavoratore a causa del timore che siano anch'essi sieropositivi[93]. Il che può determinare un peggioramento delle condizioni economico-sociali e dell'esposizione all'HIV/AIDS dell'intero nucleo familiare[94].

Il principio generale di tutela di riservatezza enunciato nell'art. 3 della Raccomandazione è maggiormente specificato all'interno degli artt. 24-27 contenuti nella sezione "*Testing, privacy and confidentiality*". Tali disposizioni, infatti, prevedono che: i test devono essere autenticamente volontari e svolti senza coercizione alcuna nel rispetto delle linee guida internazionali su riservatezza e consenso (art. 24); ai lavoratori, alle persone in cerca di occupazione e ai candidati a un impiego non dovrebbe imporsi né l'effettuazione di test né altre forme di *screening* (art. 25); ai medesimi soggetti non dovrebbe nemmeno imporsi la rivelazione di informazioni relative allo stato sierologico proprio o altrui[95] (artt. 25 e 27); i risultati dei test dovrebbero rimanere riservati e non pregiudicare l'accesso al lavoro, la possibilità di ottenere un posto fisso, la sicurezza sul lavoro o le opportunità di carriera (art. 26); l'accesso alle informazioni sullo stato sierologico dovrebbe essere regolato da norme di riservatezza coerenti con il Codice di condotta dell'ILO sulla protezione dei dati personali dei lavoratori del 1997 e agli altri *standard* internazionali pertinenti sulla protezione dei dati personali (art. 27).

Per favorire l'effettività delle tutele, è infine richiesto agli Stati membri la predisposizione di procedure facilmente accessibili di risoluzione delle controversie che garantiscano il risarcimento dei lavoratori in caso di violazione del diritto alla riservatezza (art. 29) nonché l'integrazione all'interno di leggi e normative nazionali delle misure concernenti le violazioni della privacy e della riservatezza (art. 37, par. c).

---

[93] Questo rischio è accresciuto anche dalla scarsa conoscenza circa le modalità di trasmissione della malattia che la Raccomandazione si propone di contrastare richiedendo l'adozione di programmi di informazione e sensibilizzazione su HIV/AIDS rivolti ai lavoratori (art. 15).

[94] Coerentemente, la Raccomandazione richiede che l'accesso ai servizi di prevenzione, trattamento, assistenza e sostegno venga esteso anche alle famiglie dei lavoratori e alle persone a loro carico (art. 3, par. 1, lett. e).

[95] Data l'ampiezza della formulazione, pare ricavarsi che la Raccomandazione precluda non solo di svolgere indagini o domande sullo stato sierologico del lavoratore, ma anche di richiedere al lavoratore di rivelare informazioni relative alla condizione di terzi, come propri familiari o colleghi.

9. Altre disposizioni contenute in Convenzioni e Raccomandazione connesse alla tutela della riservatezza dei lavoratori

Nella presente sezione dell'elaborato si darà conto di un nucleo di previsioni contenute in Convenzioni e Raccomandazioni adottate dall'ILO che mirano a proteggere l'identità e/o la riservatezza dei lavoratori in circostanze in cui la rivelazione dell'identità o l'assenza di riservatezza potrebbe esporli a conseguenze negative.
Nello specifico, verranno analizzate le previsioni contenute nelle Convenzioni dedicate alle ispezioni sul lavoro dirette a tutelare l'identità dei lavoratori che effettuino segnalazioni di irregolarità delle condizioni di lavoro agli organismi ispettivi nazionali (Convenzioni n. 81/1947, n. 129/1969, n. 110/1958).
Successivamente, si affronteranno le disposizioni rilevanti rispetto al tema oggetto dell'elaborato contenute nella Convenzione sull'eliminazione delle violenze e delle molestie sul luogo di lavoro n. 190/2019 e nella relativa Raccomandazione n. 206 del 2019.

9.1. La tutela della riservatezza dei lavoratori che effettuano segnalazioni agli organismi ispettivi

Il livello di efficacia dei servizi nazionali di ispezione risulta essenziale per assicurare l'effettività delle regole poste a tutela delle condizioni di lavoro, comprese le norme lavoristiche internazionali adottate dall'ILO[96].

[96] Le principali fonti OIL dedicate alle ispezioni del lavoro sono la Convenzione n. 81/1947 relativa all'ispezione del lavoro nell'industria e nel commercio; la Raccomandazione n. 81/1947 sull'ispezione del lavoro; la Raccomandazione n. 82/1947 sull'ispezione del lavoro (attività mineraria e trasporti); la Convenzione n. 129/1969 concernente l'ispezione del lavoro in agricoltura; la Raccomandazione n. 133/1969 relativa all'ispezione del lavoro in agricoltura; il Protocollo n. 81/1995 alla Convenzione sull'ispezione del lavoro n. 81/1947. Inoltre, la Convenzione n. 110/1958 sulle condizioni di impiego dei lavoratori delle piantagioni si occupa in modo esteso delle ispezioni (sezione XI).
L'essenzialità del buon funzionamento dei sistemi ispettivi per contrastare gli abusi ai danni dei lavoratori è stata più volte affermata anche nelle dichiarazioni dell'Organizzazione Internazionale del Lavoro.
La *Dichiarazione sulla giustizia sociale per una globalizzazione equa*, adottata alla 97ª sessione della Conferenza internazionale del lavoro (2008) e modificata alla 110ª sessione (2022) include "*la promozione del dialogo sociale e del tripartitismo come strumenti più adeguati … alla creazione di sistemi efficaci di ispezione del lavoro*" tra "*gli obiettivi strategico dell'OIL … attorno ai quali si articola l'Agenda del lavoro dignitoso*" (sezione I "*Portata e principi*"). Inoltre, la Dichiarazione classifica le Convenzioni sulle ispezioni del lavoro nn. 81/1947 e 129/1969 come convenzioni di *governance*, evidenziandone l'essenzialità per il funzionamento del sistema delle norme internazionali del lavoro nel suo complesso (Allegato alla Dichiarazione, sez. II, par. A, punto vi).

I controlli diretti ad accertare la regolarità delle condizioni lavorative dei prestatori possono avvenire sia a fronte di iniziative autonome degli ispettori sul lavoro sia in risposta alla ricezione di segnalazioni circa la sussistenza di irregolarità[97].

L'art. 15, par. 1, lett. c), Convenzione n. 81/1947 relativa all'ispezione del lavoro nell'industria e nel commercio si occupa di tutelare l'identità dei segnalanti, prevedendo che "*fatta riserva delle eccezioni che la legislazione nazionale potrebbe prevedere, gli ispettori del lavoro … dovranno considerare assolutamente confidenziale l'origine di qualsiasi reclamo che segnali loro un difetto nelle installazioni o un'infrazione alle disposizioni di legge e dovranno astenersi dal rivelare al datore di lavoro o al suo rappresentante che la visita di ispezione è stata effettuata in seguito ad un reclamo*"[98].

Infatti, il mantenimento della riservatezza circa l'identità dei lavoratori segnalanti consente di raggiungere una duplice utilità, tutelando al contempo sia i singoli lavoratori sia l'interesse collettivo alla rimozione delle situazioni di irregolarità lavorativa.

L'utilità per i singoli lavoratori si ravvisa nella circostanza che il datore di lavoro, ove a conoscenza dell'esistenza di una segnalazione di irregolarità proveniente da un lavoratore, potrebbe adottare condotte ritorsive nei confronti dell'autore dell'esposto. Ma l'utilità individuale è strettamente connessa a quella collettiva giacché la predisposizione di misure di tutela della riservatezza dei lavoratori segnalanti aumenta le *chances* che i prestatori segnalino all'autorità competente la (presunta) situazione di irregolarità. In

---

Anche nella *Dichiarazione del Centenario per il Futuro del Lavoro* del 2019 viene ribadito che l'ILO, al fine di adempiere al proprio mandato costituzionale*, "deve orientare i propri sforzi per … rafforzare l'amministrazione e l'ispezione del lavoro*".

[97] Nello specifico, le funzioni dell'ispezione del lavoro identificate dall'art. 3, par. 1, Convenzione n. 81/1947 e dall'art. 6, par. 1, Convenzione n. 129/1969 consistono nel: (i) garantire l'applicazione delle disposizioni di legge relative alle condizioni di lavoro ed alla protezione dei lavoratori nell'esercizio della loro professione, quali le disposizioni relative alla durata del lavoro, ai salari, alla sicurezza, all'igiene ed al benessere, all'impiego dei fanciulli e degli adolescenti, e ad altre materie connesse, nella misura in cui gli ispettori del lavoro sono incaricati di garantire l'applicazione di dette disposizioni; (ii) fornire informazioni e consigli tecnici ai datori di lavoro ed ai lavoratori sui mezzi più efficaci per osservare le disposizioni di legge; (iii) sottoporre all'attenzione dell'autorità competente le insufficienze o gli abusi che non sono specificamente coperti dalle disposizioni di legge esistenti e le proposte per un miglioramento della legislazione vigente.

[98] Fonte della traduzione: G. KOJANEC, *Convenzioni e raccomandazioni della Organizzazione internazionale del lavoro 1919–1968*, Padova, CEDAM, 1969.
La medesima disposizione è presente anche in altre Convenzioni dedicate alle ispezioni del lavoro. Infatti, presentano una formulazione identica all'art. 15, par. 1, lett. c), Convenzione n. 81/1947 anche l'art. 20, par. 1, lett. c), Convenzione n. 129/1969 concernente l'ispezione del lavoro in agricoltura e l'art. 79, par. 1, lett. c), Convenzione n. 110/1958 sulle condizioni di impiego dei lavoratori delle piantagioni.

questo modo, ad essere favorita è l'efficacia complessiva dei sistemi di ispezione del lavoro.

Passando all'analisi della disposizione, questa richiede ai servizi ispettivi non solo di trattare in modo confidenziale la fonte all'origine del reclamo, ma anche di non rivelare al datore di lavoro e ai suoi rappresentanti la stessa esistenza del reclamo che ha portato all'attivazione dell'ispezione. Infatti, l'informazione circa l'esistenza di un esposto fornisce al datore di lavoro la certezza che l'accertamento non è stato attivato "autonomamente" dagli organismi ispettivi, potendo indurlo a porre in essere indagini dirette a scoprire, a scopo ritorsivo, se l'esposto proviene da un proprio lavoratore.

Tuttavia, la tutela della confidenzialità della fonte della segnalazione non presenta carattere assoluto, essendo espressamente fatta salva la possibilità che la legislazione nazionale possa introdurre eccezioni.

Considerato che la Convenzione n. 81/1947 è stata ratificata a livello nazionale con la legge 2 agosto 1952, n. 1305 (G.U., Serie Generale n. 242 del 17 ottobre 1952 - Suppl. Ordinario), si ritiene rilevante verificare se, all'interno dell'ordinamento interno, il diritto alla riservatezza del lavoratore autore dell'esposto sia suscettibile di subire eccezioni. Per rispondere a questo quesito, occorre analizzare la portata del c.d. diritto di accesso agli atti previsto dagli artt. 22 ss., l. 7 agosto 1990, n. 241 allo scopo di favorire l'imparzialità e la trasparenza dell'attività amministrativa. In particolare, si dovrà verificare se al datore di lavoro sia riconosciuto il diritto di accedere all'esposto alla base di un accertamento ispettivo, ove questo sia riconducibile a un lavoratore[99].

In tal senso, innanzitutto bisogna verificare se l'esposto costituisca un documento amministrativo in senso proprio, considerato che il c.d. diritto di accesso agli atti consiste nella possibilità di "*prendere visione e di estrarre copia di documenti amministrativi*" (art. 22, comma 1, lett. a). A tale prima questione deve essere fornita risposta affermativa in quanto la l. n. 241/1990 non richiede che i documenti per i quali si richiede l'accesso siano formati ad opera della pubblica amministrazione, essendo sufficiente che gli stessi siano "*detenuti da una pubblica amministrazione e concernenti attività di pubblico*

[99] Considerato che l'oggetto di ricerca consiste nella protezione della riservatezza del lavoratore, l'ambito dell'indagine è delimitato all'ipotesi in cui la richiesta datoriale sia diretta ad accedere a un esposto riconducibile a un lavoratore.

interesse"[100].

In secondo luogo, occorre verificare se il datore di lavoro abbia la legittimazione a richiedere l'accesso all'esposto riconducibile a un lavoratore.

In generale, il diritto di accesso è riconosciuto agli interessati, ossia "*tutti i soggetti privati … che abbiano un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso*" (art. 22, comma 1, lett. b). Pertanto, risulta necessaria l'individuazione di un interesse qualificato in capo al datore di lavoro che possa giustificare l'accesso all'esposto. In astratto, tale interesse potrebbe essere ravvisato nell'interesse alla difesa in giudizio tutelato dall'art. 24, comma 7, l. n. 241/1990 in forza del quale "*deve comunque essere garantito ai richiedenti l'accesso ai documenti amministrativi la cui conoscenza sia necessaria per curare o per difendere i propri interessi giuridici*" (c.d. accesso difensivo). Infatti, sempre ragionando in termini astratti, l'accesso del datore di lavoro all'esposto potrebbe essere funzionale, da un lato, a contestare i provvedimenti adottati dagli organi ispettivi che abbiano riscontrato irregolarità, dall'altro, a difendere in giudizio l'immagine e la reputazione dell'organizzazione qualora l'ispezione si concluda senza che vengano ravvisate violazioni.

Quanto alla prima esigenza difensiva rappresentata, quella di contrastare il contenuto degli accertamenti ispettivi di irregolarità, si ritiene insussistente l'interesse qualificato del datore di lavoro idoneo a giustificare il c.d. accesso difensivo all'esposto. Infatti, la segnalazione costituisce un atto meramente sollecitatorio dell'esercizio della funzione amministrativa di controllo che compete agli organismi ispettivi e, pertanto, la conoscenza dei fatti e delle condotte contestate risulta assicurata dall'accesso ai documenti formati dall'organismo ispettivo, senza che sia necessario al datore di lavoro risalire al precedente esposto per predisporre la propria difesa[101].

---

[100] Per la precisione, l'ampia nozione di documento amministrativo individuata dall'art. 22, comma 1, lett. d), l. n. 241/1990 è la seguente: "*ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale*".

[101] A tal riguardo, il Consiglio di Stato, sez. III, 1° marzo 2021, n.1717, ha affermato come, di regola, la soddisfazione dell'interesse difensivo dell'impresa a cui siano contestate irregolarità non richiede l'accesso alla segnalazione che ha originato l'attività di controllo. Infatti, "*allorquando l'accertamento di un illecito amministrativo sia fondato su autonomi atti di ispezione dell'Autorità amministrativa, l'esposto del privato ha il solo effetto di sollecitare il promovimento d'ufficio del procedimento, senza acquisire efficacia*

Invece, nel secondo caso, quello in cui l'attività ispettiva si concluda senza che siano ravvisate violazioni, effettivamente l'accesso all'esposto potrebbe ravvisarsi un interesse qualificato alla tutela in giudizio della lesione all'onore, all'immagine e alla reputazione dell'azienda causata dal contenuto potenzialmente diffamatorio e/o calunnioso dell'esposto.

Però, a tali esigenze conoscitive datoriali si contrappone l'esigenza di tutela della riservatezza del lavoratore autore della segnalazione - indispensabile per la prevenzione di azioni ritorsive e/o discriminatorie - che verrebbe compromessa dall'accesso datoriale all'esposto.

A questo punto, occorre, quindi, verificare se, all'interno dell'ordinamento giuridico nazionale, sia prevalente il principio di trasparenza, alla base del c.d. diritto di accesso difensivo o l'interesse alla riservatezza del lavoratore-controinteressato[102].

A livello normativo, il sistema sembra propendere per la preminenza del diritto alla riservatezza dei lavoratori rispetto a quello datoriale di accesso all'esposto.

Infatti, l'art. 24 comma 6, l. n. 241/90 stabilisce che "*il Governo può prevedere casi di sottrazione all'accesso di documenti amministrativi … quando i documenti riguardino la vita privata o la riservatezza di persone fisiche…, con particolare riferimento all'interesse professionale … ancorché i relativi dati siano forniti all'amministrazione dagli stessi soggetti cui si riferiscono*".

In attuazione della predetta disposizione, il Decreto del Ministero del lavoro n. 757/1994 ha disposto la sottrazione dall'accesso agli atti dei "*documenti contenenti le richieste di intervento dell'Ispettorato del lavoro*" (art. 2) "*per cinque anni, o finché perduri il*

probatoria, con la conseguenza che in tali evenienze, di regola, per il destinatario del provvedimento finale non sussiste la necessità di conoscere gli esposti al fine di difendere i propri interessi giuridici, a meno che non siano rappresentate particolari esigenze; ciò, del resto, corrisponde al fatto che, di fronte al diritto alla riservatezza del terzo, la pretesa di conoscenza dell'esposto da parte del richiedente, se svincolata dalla preordinazione all'esercizio del diritto di difesa, acquista un obiettivo connotato ritorsivo che l'ordinamento non può tutelare".

[102] Con il termine "*controinteressati*" si definiscono "*tutti i soggetti, individuati o facilmente individuabili in base alla natura del documento richiesto, che dall'esercizio dell'accesso vedrebbero compromesso il loro diritto alla riservatezza*" (art. 22, comma 1, lett. c), l. n. 241/1990).

rapporto di lavoro nella ipotesi che la richiesta di intervento provenga da un lavoratore o abbia comunque ad oggetto un rapporto di lavoro" (art. 3)[103].

Si ritiene che la prevalenza che l'ordinamento sembra attribuire alle esigenze di tutela del lavoratore rispetto a quelle datoriali di ostensione dell'esposto dovrebbe valere anche qualora il datore di lavoro si limiti a richiedere l'accesso al solo contenuto dell'esposto e non anche al nominativo del segnalante. Infatti, specie nelle aziende di minori dimensioni, dal contenuto dell'esposto, ove proveniente da un lavoratore, potrebbero trarsi elementi utili all'identificazione del segnalante quali indicazioni di tempo (da cui potrebbe desumersi da quanto tempo il lavoratore è in forza), dettagli in ordine alla posizione ricoperta o alla prestazione svolta, riferimento informazioni o eventi noti solo a specifici lavoratori.

Sempre al fine di contrastare il predetto rischio di identificazione del lavoratore, si ritiene che l'accesso dovrebbe essere negato anche qualora l'esposto sia anonimo, ma, dall'esame del suo contenuto, sia certo o comunque probabile che lo stesso provenga da un lavoratore.

Tuttavia, la prevalenza che l'ordinamento sembra attribuire alla tutela della riservatezza del lavoratore potrebbe risultare parzialmente incisa nella prassi.

Infatti, l'art. 25, comma 3, l. n. 241/90 richiede all'amministrazione di motivare l'eventuale rifiuto, differimento o limitazione dell'istanza di accesso proposta dall'interessato. Ebbene, qualora il datore di lavoro faccia richiesta di accesso all'esposto che ha dato avvio all'ispezione (ove esistente), l'amministrazione, per giustificare il proprio rifiuto, potrebbe dover fare riferimento alla necessità di tutelare l'identità e la riservatezza del lavoratore segnalante.

---

[103] Similmente, il previgente Codice di comportamento ad uso del personale ispettivo del Ministero del Lavoro e delle Politiche Sociali del 20 aprile 2006 prevedeva che "*nel corso dell'ispezione, nonché delle fasi successive, il personale ispettivo garantisce la segretezza della fonte della denuncia e/o degli atti che hanno dato origine all'accertamento*" (art. 23, comma 3). Anche la versione aggiornata del Codice di comportamento ribadisce il dovere del personale ispettivo di "*garantire la segretezza della fonte della denuncia*", ma aggiunge "*nei limiti indicati dall'Amministrazione*" (art. 22, comma 3, Decreto del Ministero del lavoro del 15 gennaio 2014).

Quanto al Codice di comportamento dei dipendenti dell'Ispettorato Nazionale del Lavoro (INL) adottato con decreto direttoriale n. 4 del 24 gennaio 2022, questo prevede che "*nelle fasi precedenti l'ispezione, nel corso della stessa e nelle fasi successive, ivi compresa la verbalizzazione conclusiva, il personale ispettivo garantisce la segretezza delle ragioni che hanno dato origine all'accertamento, secondo quanto indicato dalla legge e dall'Amministrazione*" (art. 21, comma 3).

È vero che l'amministrazione potrebbe anche decidere di non pronunciarsi lasciando decorre inutilmente il termine di trenta giorni dalla richiesta che equivale a diniego tacito dell'istanza datoriale (art. 25, comma 4).

Tuttavia, qualora l'interessato si opponga al differimento o al diniego dell'accesso, sia esso espresso o tacito (art. 25, commi 4 e 5), l'amministrazione, seppur in un secondo momento[104], dovrà comunque motivare le ragioni sottese al rifiuto, ossia la circostanza che l'esposto è riferibile a un lavoratore.

Pertanto, l'interesse a evitare condotte ritorsive che si intendeva tutelare potrebbe risultare quantomeno inciso dalla prassi procedimentale giacché il datore di lavoro, pur non accedendo né al contenuto né al nominativo dell'autore dell'esposto (ove sottoscritto), potrebbe acquisire la certezza che la segnalazione provenga da uno dei propri lavoratori, esponendo questi ultimi ad una possibile attività di "ricerca del colpevole".

[104] In realtà, anche in caso di provvedimento espresso di diniego la rivelazione della circostanza che l'esposto proviene da un prestatore di lavoro potrebbe essere posticipata. Infatti, il diniego espresso all'istanza di accesso datoriale potrebbe non far riferimento alcuno a tale informazione qualora sussistano motivazioni diverse che comunque impongano il rigetto della richiesta (come, ad esempio, il difetto di specificità della motivazione dell'istanza di accesso agli atti *ex* art. 25, comma 2, l. 241/1990). Inoltre, il rifiuto potrebbe basarsi solamente su altre argomentazioni che potenzialmente potrebbero giustificare il rigetto (come il difetto di un interesse qualificato alla conoscenza dell'esposto).
Questo perché, secondo il consolidato orientamento della giurisprudenza amministrativa, nel giudizio instaurato a seguito del ricorso avverso il diniego della richiesta accesso agli atti, è possibile aggiungere nuove argomentazioni non "spese" nel provvedimento di rigetto. Questo perché "*il giudizio di accesso - anche se si atteggia come impugnatorio, essendo rivolto avverso il provvedimento di diniego o avverso il silenzio-rigetto formatosi sulla relativa istanza - ha per oggetto l'accertamento della spettanza o meno del diritto medesimo, piuttosto che la verifica della sussistenza di vizi di legittimità dell'eventuale diniego opposto dall'Amministrazione" (Consiglio di Stato, sez. IV, 06/02/2019, n. 906; Consiglio di Stato sez. III, 05/03/2018, n. 1396) il che implica la dequotazione della problematica relativa alla contestata motivazione postuma*" (Cons. St., sez. III, 28 ottobre 2020, n. 6570). Quindi, il fatto che sia rivelata al datore la riferibilità dell'esposto a un lavoratore per la prima volta nel corso del giudizio "*non è censurabile in termini di inammissibile motivazione postuma, dovendo valutare il Giudice tutti gli elementi che, anche se non individuati nel contestato provvedimento di diniego, possono influire sull'ostensibilità del documento. Ovviamente, per converso, a tutela del diritto di difesa del soggetto ricorrente (n.d.r. datore di lavoro), deve essere data la possibilità allo stesso di modificare e integrare le deduzioni, censure e argomentazioni contenute nel ricorso*" (T.A.R. Veneto, sez. III, 29 marzo 2021).
Un'ulteriore opzione per tutelare pienamente la riservatezza del lavoratore autore dell'esposto potrebbe consistere nell'argomentare il rifiuto di ostensione dell'esposto facendo genericamente riferimento all'esistenza di un prevalente interesse alla riservatezza di un terzo, senza specificare che si tratta di un lavoratore. In questo modo, però, si corre il rischio che il giudice ritenga prevalente l'interesse alla difesa in giudizio del datore di lavoro rispetto a un interesse alla riservatezza di terzi così genericamente espresso. Il che potrebbe condurre alla condanna dell'organismo ispettivo all'esibizione dell'intero esposto, circostanza che arrecherebbe maggiore *vulnus* alla posizione del lavoratore segnalante.

9.2. La tutela della riservatezza dei lavoratori coinvolti in episodi di violenza o molestia sul lavoro

Le Convenzione n. 190/2019 sull'eliminazione della violenza e delle molestie nel mondo del lavoro, così come la Raccomandazione n. 206/2019 che ne approfondisce i contenuti[105], hanno lo scopo di prevenire e contrastare "*un insieme di pratiche e di comportamenti inaccettabili, o la minaccia di porli in essere, sia in un'unica occasione, sia ripetutamente, che si prefiggano, causino o possano comportare un danno fisico, psicologico, sessuale o economico*" [106] (art. 1, par. 1, lett. a), Convenzione n. 190/2019) "*che si verifichino in occasione di lavoro, in connessione con il lavoro o che scaturiscano dal lavoro*" (art. 3, Convenzione n. 190/2019), con una particolare attenzione per la violenza e le molestie di genere[107].

Tali strumenti contengono anche disposizioni inerenti alla protezione della vita privata e della riservatezza dei lavoratori.

In particolare, al fine di conformarsi alla Convenzione, agli Stati ratificanti è richiesta l'adozione a livello interno di "*misure adeguate al fine di … proteggere la vita privata dei soggetti coinvolti e la riservatezza, nella misura massima possibile e a seconda dei casi, e garantire che le esigenze di protezione della vita privata e della riservatezza non vengano utilizzate impropriamente, evitandone qualsivoglia utilizzo inopportuno*" (art. 10, par. 1, lett. c)[108].

---

[105] Tali strumenti sono stati simbolicamente approvati nel contesto del centenario dell'ILO (sessione n. 108 della Conferenza Internazionale sul Lavoro il 21 giugno 2019).
Per un commento generale sugli strumenti cfr., tra gli altri, S. SCARPONI, *La convenzione OIL 190/2019 su violenza e molestie nel lavoro e i riflessi sul diritto interno*, in *Rivista giuridica del lavoro*, 1/2021, pp. 23-39; C. ALESSI, *La Convenzione Ilo sulla violenza e le molestie sul lavoro*, in Lavoro e diritto, 3/2023, pp. 577-594; L. CALAFÀ, *Molestie e violenza sul lavoro: la questione debitoria rinnovata dalla ratifica della Convenzione OIL*, in ISL -IGIENE & SICUREZZA DEL LAVORO, 8-9/2023, pp. 16-19; M. SAHAN "*The First International Standard on Violence and Harassment in the World of Work*", Cambridge University Press, 2020.

[106] Traduzione in italiano a cura dell'Ufficio ILO per l'Italia e San Marino.

[107] L'espressione "*violenza e molestie di genere*" indica "*la violenza e le molestie nei confronti di persone in ragione del loro sesso o genere, o che colpiscano in modo sproporzionato persone di un sesso o genere specifico, ivi comprese le molestie sessuali*" (art. 1, par. 1, lett. b, Convenzione n. 190/2019).

[108] A titolo di esempio, gli Stati devono assicurarsi che i *non-disclosure agreements* (c.d. NDAs) non siano utilizzati "*to silence victims or whistle-blowers, irrespective of their contractual status, who allege any misconduct, particularly sexual harassment and other forms of discrimination-based harassment. In this regard, Article 10(c) of Convention No. 190 states that ratifying States should ensure that requirements for privacy and confidentiality are not misused* (v. *Violence and harassment in the world of work: A guide on*

Tale disposizione è meglio specificata all'interno della Raccomandazione n. 206/2019, le cui disposizioni, integrando quelle della Convenzione, dovrebbero essere considerate congiuntamente (v. Preambolo). In particolare, ai sensi dall'art. 7, par. 1, lett. f), della Raccomandazione, "*i Membri dovrebbero specificare nella legislazione che le lavoratrici e lavoratori e i loro rappresentanti dovrebbero partecipare allo sviluppo, all'attuazione e al monitoraggio della politica a livello aziendale*" in materia di violenza e molestie sul lavoro[109]. Politica aziendale che dovrebbe prevedere anche "*il diritto delle persone alla vita privata e alla riservatezza, secondo quanto indicato nell'articolo 10 c) della Convenzione, conciliandolo con il diritto delle lavoratrici e lavoratori a essere informati di qualsivoglia pericolo*"[110].

Pertanto, l'ILO non delinea regole e misure specifiche in materia di tutela della vita privata e della riservatezza, ma si limita a fornire indicazioni di massima che necessitano di essere implementate e specificate secondo le direttrici fornite dall'ILO attraverso l'adozione di politiche nazionali e aziendali sul tema.

Sono quindi le politiche nazionale e aziendali a doversi fare carico di regolamentare più nello specifico come la privacy dei soggetti coinvolti debba essere garantita in concreto. Innanzitutto, si pone l'esigenza di proteggere la privacy della vittima (in caso di condotta accertata) o della presunta vittima (in caso di denuncia, segnalazione o indagine in corso). In questo caso, la tutela della riservatezza costituisce il presupposto per il perseguimento di obiettivi meritevoli connessi alla tutela della stessa dignità della persona: rispettare la volontà, ove sia tale, della vittima di mantenere il riserbo sulla circostanza di aver subito violenza e/o molestie sul luogo di lavoro; prevenire possibili valutazioni moralistiche e/o

---

Convention No. 190 and Recommendation No. 206, *International Labour Office*, Ginevra, 2021, Box 25 *Violence and harassment and non-disclosure agreements*).

[109] Il richiamo della Raccomandazione è alla politica aziendale di cui all'art. 9, par. 1, lett. a) della Convenzione n. 190/2019, ai sensi del quale "*ciascun Membro dovrà adottare leggi e regolamenti che richiedano ai datori di lavoro di intraprendere misure adeguate e proporzionate al rispettivo livello di controllo in materia di prevenzione della violenza e delle molestie nel mondo del lavoro, ivi compresi la violenza e le molestie di genere, e in particolare, nella misura in cui sia ragionevolmente fattibile, attraverso … l'adozione e l'attuazione, in consultazione con le lavoratrici e i lavoratori e i loro rappresentanti, di una politica in materia di violenza e di molestie a livello aziendale*".

[110] A proposito dell'art. 7 della Raccomndazione, il documento "*Violence and harassment in the world of work: A guide on Convention No. 190 and Recommendation No. 206*", *International Labour Office*, Ginevra, 2021, sezione 5.2. "*Adopting and implementing a workplace policy on violence and harassment*" sottolinea come "*it would be important that employers commit to protecting individuals' right to privacy and confidentiality while balancing the right of workers to be made aware of all hazards, as well as their right not to be victimized or retaliated against*".

episodi di stigmatizzazione ai danni della vittima, specie in caso di violenza e molestie di natura sessuale; evitare possibili ritorsioni nei confronti della vittima, ad esempio ad opera di colleghi vicini all'autore/presunto autore della violenza e/o molestia; qualora, per qualsiasi motivo, l'identità della vittima sia nota, mantenere strettamente riservati i dettagli sull'episodio/sugli episodi così da contrastare il fenomeno della c.d. vittimizzazione secondaria o, comunque, la "morbosa attenzione" verso la vicenda da parte di colleghi e/o terzi[111]. In questo senso, la predisposizione di regole a tutela della riservatezza della vittima risulta altresì funzionale alla rimozione di fattori ostativi che possono scoraggiarla dal denunciare le condotte subite.

Sussistono anche esigenze di protezione della riservatezza anche in capo ai c.d. *whistle-blowers*, così da prevenire possibili condotte ritorsive idonee a disincentivarli segnalare condotte di violenza e/o molestia sul luogo di lavoro.

Inoltre, si ravvisano istanze di riservatezza anche con riferimento ai testimoni giacché la pubblicità delle dichiarazioni rese potrebbe scoraggiarli dal riferire le informazioni rilevanti di cui siano a conoscenza. Esigenza che, a sua volta, può collidere con l'interesse della persona indicata come autore della violenza e della molestia ad accedere a tali dichiarazioni al fine di predisporre un'idonea difesa.

Inoltre, può porsi anche l'esigenza di tutelare la privacy del soggetto indicato come autore della violenza/molestia, specie ove anch'esso sia un lavoratore, almeno fino a quando l'accertamento dei fatti sia ancora in corso, senza che però la privacy possa tradursi in uno strumento funzionale a ostacolare la conduzione di seri accertamenti[112].

Sono, quindi, numerosi i profili suscettibili di essere tenuti in considerazione dalle politiche nazionali e aziendali al fine di declinare in concreto la configurazione, l'estensione e le modalità di esercizio delle prerogative relative alla riservatezza.

---

[111] Ai sensi della Raccomandazione n. 8 del 2006 del Consiglio d'Europa "*secondary victimisation means the victimisation that occurs not as a direct result of the criminal act but through the response of institutions and individuals to the victim*" (par. 1.3). La vittima, infatti, può subire ulteriore violenza da parte di soggetti che non sono gli autori della violenza primaria, ad esempio attraverso commenti atti a spostare l'attenzione e la responsabilità dalla persona che ha commesso la violenza alla persona che l'ha subita.

[112] Nel documento *Violence and harassment,* cit., par. 6.1.2. "*Protection before, during and after reporting or making a complaint*" è indicato che anche la riservatezza del presunto responsabile ("*alleged perpetrator*") deve essere tutelata, senza che però ciò impedisca lo svolgimento dell'indagine. Nello specifico, si legge che "*throughout the reporting, investigation and dispute resolution process, Convention No. 190 calls for the protection of privacy and confidentiality, to the extent possible and as appropriate (Art. 10(c)). The confidentiality of complaints is essential to protecting the privacy of both the complainant and the alleged perpetrator. However, privacy and confidentiality should not impede an investigation*".

10. Le più recenti iniziative dell'Organizzazione Internazionale del Lavoro sulla protezione della privacy dei lavoratori

Nella *Centenary Declaration for the Future of Work*, approvata dalla Conferenza Internazionale del Lavoro in data 21 giugno 2019, l'ILO ha incoraggiato gli Stati a promuovere "*politiche e misure che garantiscano un adeguato rispetto della vita privata e la protezione dei dati personali, e che reagiscano alle sfide e colgano le opportunità che si presentano nel mondo del lavoro in relazione alla trasformazione digitale del lavoro, ivi compreso il lavoro su piattaforma*" (art. 3).

La direzione indicata nella Dichiarazione del Centenario sta venendo percorsa lungo due diversi direttrici: da un lato, attraverso iniziative generali, all'interno delle quali, tra i profili affrontati, vi è anche la protezione della privacy dei lavoratori; dall'altro, mediante iniziative specificatamente rivolte ad affrontare le sfide poste dell'evoluzione tecnologica con riguardo alla riservatezza dei prestatori.

Partendo dal primo tipo di iniziative, il Consiglio d'Amministrazione, nella sessione n. 341 del marzo 2021, ha richiesto all'Ufficio Internazionale del Lavoro di convocare nel corso del 2022 una riunione tripartita di esperti sul tema del lavoro dignitoso nell'economia delle piattaforme (GB.341/PV, par. 50c). L'obiettivo era quello di utilizzare i risultati del *meeting of experts on decent work in the platform econom* per una discussione generale o per intraprendere un percorso di *standard-setting* su questo tema in seno alla Conferenza Internazionale del lavoro (GB.341/INS/3/1(Rev.2), par. 26).

Nell'ordine del giorno del *meeting* tripartito, approvato dal Consiglio di Amministrazione nella sessione n. 344 del marzo 2022, è stato inserito anche l'esame delle misure inerenti alla protezione dei dati personali e all'utilizzo della tecnologia per organizzare e monitorare il lavoro dei *platform workers* (GB.344/INS/18(Rev.1), par. 3).

In preparazione della predetta riunione, l'Ufficio Internazionale del Lavoro ha elaborato il *Reference document for the Meeting of experts on decent work in the platform economy*, funzionale ad agevolare lo svolgimento *meeting* attraverso la ricostruzione del contesto generale e del quadro regolatorio in cui si inserisce il lavoro tramite piattaforme digitali[113]

[113] Per uno studio comparativo delle condizioni di lavoro dei lavoratori nelle *microtask platforms* si rinvia a J. BERG, M. FURRER, E. HARMON, U. RANI, M. SIX SILBERMAN, *Digital labour platforms and the future of work, International Labour Office, ILO,* Ginevra, 2018.

(MEDWPE/2022). Il rapporto dell'Ufficio individua anche gli *standard* dell'ILO che potrebbero essere rilevanti in tema di protezione dei dati personali e uso della tecnologia per organizzare e monitorare il lavoro su piattaforma.

A tal proposito, la sezione 6.3 "*Data protection and algorithmic management*" evidenzia come i progressi compiuti dalle piattaforme digitali rispetto alla capacità di acquisire dati suscitino crescenti preoccupazioni per la protezione dei dati personali dei lavoratori.

Nell'ambito degli strumenti giuridici esistenti, l'Ufficio ritiene che il Codice di condotta dell'ILO sulla protezione dei dati personali dei lavoratori del 1997 potrebbe guidare le azioni delle piattaforme nell'applicazione di alcuni diritti e garanzie fondamentali quali: il diritto di essere informati sui dati personali in possesso della piattaforma e sul loro trattamento; il diritto di accesso ai dati personali, indipendentemente dal fatto che siano sottoposti a trattamento automatizzato; il diritto di richiedere la cancellazione o la correzione di dati personali inesatti o incompleti; la garanzia che le decisioni riguardanti un lavoratore non dovrebbero basarsi esclusivamente su un trattamento automatizzato dei dati personali di quel lavoratore; la garanzia che il trattamento dei dati personali non dovrebbe condurre a discriminazioni (par. 96). Tuttavia, viene evidenziato come nel Codice di condotta ILO manchi il riconoscimento del diritto alla portabilità dei dati[114], il quale consentirebbe il trasferimento del *ranking* del lavoratore da una piattaforma all'altra (par. 97)[115].

---

[114] Il diritto alla portabilità è invece riconosciuto da altri strumenti normativi in materia di dati personali. Infatti, l'art. 20 del Reg. UE 679/2016 (c.d GDPR) e l'art. 30 degli *Standards for Personal Data Protection for Ibero-American States* disciplinano il diritto alla portabilità dei dati personali, inteso come diritto dell'interessato alla trasmissione dei propri dati personali da un titolare del trattamento all'altro.

[115] Pertanto, mentre, per un verso, costituisce motivo di preoccupazione per l'ILO l'equità dei sistemi di *ranking* algoritmico e il loro utilizzo per la valutazione automatizzata delle prestazioni dei lavoratori, che può comportare anche l'impossibilità di continuare a svolgere l'attività lavorativa in caso di disattivazione dell'*account*; per un altro, l'ILO si preoccupa di favorire il trasferimento del *ranking* del lavoratore tra piattaforme.
Presumibilmente, quello a cui l'ILO mira è consentire al lavoratore che lo desideri la possibilità di trasferire il proprio punteggio ad un'altra piattaforma. Diversamente, un lavoratore potrebbe essere disincentivato a cambiare piattaforma, finendo per rimanere "ostaggio" della stessa, per la preoccupazione di dover ricostruire dall'inizio la propria reputazione digitale. Inoltre, l'esercizio di tale diritto sembra presupporre la trasparenza delle piattaforme su come venga calcolato e quale sia il *ranking* assegnato al lavoratore.
Tuttavia, a parere dello scrivente, il diritto alla portabilità della reputazione digitale non potrebbe essere riconosciuto in modo assoluto, richiedendo come presupposto logico (quantomeno) la vicinanza dei criteri con cui viene calcolato il *ranking* tra la piattaforma di partenza e quella di destinazione nonché una certa comunanza tra le attività delle stesse. Infatti, a titolo di esempio, sembrerebbe irragionevole il trasferimento del *ranking* da una piattaforma di *food delivery* a una piattaforma inerente un'attività relativa a prestazioni di natura completamente diversa.

Inoltre, il documento rileva l'esistenza di una lacuna normativa all'interno degli strumenti adottati dall'ILO per quanto riguarda la tutela dei lavoratori rispetto all'*algorithmic management*[116], fenomeno caratterizzante il lavoro tramite piattaforme digitali decritto nei seguenti termini: "*it is an algorithm that offers and grants services or tasks to workers, defines their time slots, calculates the rankings on which their activities and income depend, and decides whether they will continue to provide services for the platform or remain deselected from it*" (par. 101). In particolare, il rapporto sottolinea come i lavoratori su piattaforma non conoscano affatto o non conoscano sufficientemente il funzionamento dell'algoritmo perché opaco e, a volte, per loro del tutto incomprensibile e come le decisioni algoritmiche non siano sempre neutrali in quanto i dati che alimentano gli algoritmi possono contenere pregiudizi che si traducono in decisioni discriminatorie[117].

Il *meeting of experts on decent work in the platform economy* si è tenuto a Ginevra tra il 10 e il 14 ottobre del 2022 tra ventiquattro esperti, nominati a seguito della consultazione con il gruppo dei Governi, dei Datori di Lavoro e dei Lavoratori del Consiglio di Amministrazione[118].

Sulla base delle diverse proposte e posizioni espresse dagli esperti durante le giornate dedicate alla discussione generale, l'Ufficio Internazionale del Lavoro ha preparato un insieme di conclusioni provvisorie da sottoporre al *meeting* tripartito (v. *Summary record of proceedings,* MEDWPE/2022/8, Allegato I).

Nelle predette conclusioni provvisorie viene indicato che dovrebbero essere messe in atto o rafforzate misure per garantire un lavoro dignitoso a tutti i lavoratori delle piattaforme attraverso la protezione dei loro dati personali e la regolamentazione dell'*algorithmic management*. In particolare, viene segnalata l'opportunità di istruire un quadro normativo strutturato e meccanismi di conformità per garantire adeguata protezione dei dati

[116] Per la precisione, la sezione 6.3 "*Data protection and algorithmic management*" del rapporto dell'Ufficio si conclude evidenziando che "*there is a regulatory vacuum within the ILO on this matter*".

[117] Tra gli esempi di discriminazioni algoritmiche, il rapporto dell'Ufficio riporta anche l'ordinanza del Tribunale di Bologna del 31 dicembre 2020, già citata nel Capitolo I, par. 1.2 dell'elaborato, che ha rilevato come l'algoritmo utilizzato dalla piattaforma di consegna Deliveroo causi discriminazioni tra i *riders* perché non tiene conto che i motivi per cui i lavoratori potrebbero non lavorare in uno *slot* temporale precedentemente selezionato o cancellarsi da tale *slot* con un preavviso inferiore a 24 ore potrebbero consistere nell'esercizio del diritto di sciopero o nello stato di malattia.

[118] La composizione della riunione tripartita è stata approvata dal Consiglio di Amministrazione nella sessione n. 343 del novembre 2021 (GB.343/INS/15, paragrafi 1–7)

personali dei *platform workers* e il loro diritto alla privacy, specialmente regolamentando la sorveglianza tecnologica nonchè l'accesso, il controllo e la portabilità dei dati. Inoltre, viene rilevato che dovrebbe essere regolamentato e controllato l'uso di algoritmi in sostituzione dei decisori umani, specie per assegnare i compiti, valutare le prestazioni lavorative e sanzionare i lavoratori, anche per quanto concerne il diritto dei lavoratori a una revisione umana delle decisioni automatizzate e la garanzia che gli algoritmi siano equi, trasparenti e privi di pregiudizi discriminatori (*Draft conclusions*, par. 16h).

Sempre nelle conclusioni provvisorie, si legge che alcuni aspetti del lavoro su piattaforma non sarebbero adeguatamente coperti dalle norme internazionali sul lavoro, tra cui la protezione dei dati personali e il diritto alla privacy dei lavoratori, compresa la portabilità della reputazione digitale, nonché la *governance* dell'*algorithmic management*, inclusa l'equità e la trasparenza delle decisioni automatizzate quali quelle relative al *rating* e alla disattivazione dell'a*ccount* (par. 18, *"Recommendation for future action by the International Labour Organization*", punti nn. 2 e 3).

Tuttavia, a causa della distanza tra le posizioni e dell'ostruzionismo degli esperti datoriali, il *meeting* si è concluso senza l'approvazione di nessuna delle conclusioni provvisorie.

Malgrado l'incapacità del *meeting of experts* di raggiungere conclusioni condivise che potessero orientare l'azione degli organi dell'ILO, il Consiglio di Amministrazione, nella sessione n. 346 (ottobre-novembre 2022), ha deciso di inserire comunque nella sessione n. 113 del 2025 della Conferenza Internazionale del Lavoro un punto all'ordine del giorno sul lavoro dignitoso nell'economia delle piattaforme. A tal fine, il Consiglio di Amministrazione ha richiesto all'Ufficio Internazionale del Lavoro di presentare nella sessione n. 347 del marzo 2023 un'analisi sulle lacune normative relative al lavoro su piattaforma al fine di guidare il processo decisionale circa la natura del punto da inserire (GB.346/INS/PV, par. 92b).

In attuazione di quanto stabilito, per fornire al Consiglio di Amministrazione una base informativa più completa per decidere le azioni più opportune da intraprendere per la tutela del lavoro dignitoso dei lavoratori tramite piattaforma, è stato elaborato il documento denominato "*A normative gap analysis on decent work in the platform economy*" (GB.347/POL/1).

Il documento individua due tipi di *gap* regolativi: lacune nel campo di applicazione soggettivo delle norme internazionali del lavoro (*gaps in the personal scope of*

application of international labour standards)[119] e lacune tematiche, ossia questioni rilevanti per il lavoro tramite piattaforme che non sembrano essere completamente affrontate negli strumenti regolativi dell'ILO (*thematic gaps*)[120].

Particolarmente rilevanti ai fini del presente elaborato sono le sezioni nn. 17 "*The protection of workers' personal data*" e 18 "*Algorithmic management*".

Nella sezione 17, dedicata alle possibili lacune normative in materia di protezione dei dati personali dei lavoratori, viene evidenziato come nessuno standard internazionale regoli la protezione dei dati personali dei lavoratori come il Codice di condotta ILO del 1997 e che numerosi partecipanti al *meeting* di esperti e componenti del Consiglio di Amministrazione abbiano menzionato la *data protection* come un ambito non coperto da *standards* esistenti, sebbene alcune questioni, come la sorveglianza digitale e il diritto di accesso ai dati personali, risultino, almeno in parte, coperti dal Codice di Condotta. A tal proposito, è rilevato come il Codice ILO, pur privo di forza vincolante e dello *status* di *international labour standard*, potrebbe guidare le azioni delle piattaforme in diversi ambiti, così come indicato anche nel *Reference document for the meeting of experts on decent work in the platform economy* predisposto dall'Ufficio Internazionale del Lavoro (v. *supra*)[121].

---

[119] In particolare, sono individuati gli strumenti regolativi dell'ILO rilevanti che non trovano applicazione nei confronti dei lavoratori autonomi, considerato che, come noto, spesso i *platform workers* sono classificati come lavoratori autonomi.

[120] Il documento presenta una suddivisione per argomenti, presentando, per ciascuno di essi, una valutazione della relativa copertura negli *standard* dell'Organizzazione Internazionale del Lavoro. Le venti tematiche affrontate sono: 1) *employment relationship*; 2) *freedom of association and collective bargaining*; 3) *forced labour*; 4) *elimination of child labour*; 5) *equality and opportunity of treatment*; 6) *labour inspection*; 7) *employment policy and promotion*; 8) *employment security*; 9) *wages*; 10) *working time*; 11) *occupational safety and health*; 12) *social security*; 13) *maternity protection*; 14) *migrant workers*; 15) *specific categories of workers*; 16) *transition from the informal to the formal economy*; 17) *protection of workers' personal data*; 18) *algorithmic management*; 19) *resolution of labour disputes*; 20) *cross-border nature of the platform economy*.

[121] In particolare, il par. 97 del rapporto preliminare al *meeting* di esperti dedicato al *decent work in the platform economy* (MEDWPE/2022) rileva che "*the ILO code of practice on protection of workers' personal data (1997) … could guide the actions of platforms in this regard, especially the application of the following basic rights: (i) to be informed about personal data being held and about its processing; (ii) having access to personal data regardless of whether it undergoes automated processing; (iii) the possibility to request the deletion or correction of inaccurate or incomplete personal data; (iv) a guarantee that decisions concerning a worker should not be based solely on the automated processing of that worker's personal data; and (v) a guarantee that the processing of personal data should not lead to any discrimination*".

Invece, il rapporto considera limitati altri *standard* dell'ILO che contengono disposizioni sulla protezione dei dati personali dei lavoratori in quanto si applicano esclusivamente alle agenzie di collocamento private (Convenzione n. 181/1997 e Raccomandazione n. 188/1997 sulle agenzie per il lavoro private), ai *domestic workers* (Convenzione n. 189/2011) o solo ai dati sanitari (Raccomandazione sui servizi sanitari del lavoro n. 171/1985 e Raccomandazione su HIV e AIDS n. 200/2010).

Quanto al tema dell'*algorithmic management*, affrontato nella sezione 18, l'analisi rileva che le norme internazionali del lavoro non affrontano specificamente la gestione algoritmica o, più in generale, l'uso dell'intelligenza artificiale nel mondo del lavoro, sebbene risultino rilevanti in tale contesto alcuni strumenti dell'ILO, come la Convenzione n. 111/1958 per quanto concerne la prevenzione di *discriminatory biases* nella progettazione degli algoritmi[122].

Particolarmente rilevante, è anche la rilevazione dell'intrinseco legame intercorrente tra la protezione dei dati personali e *algorithmic management*. Tale nesso consiste nella circostanza che la gestione algoritmica del lavoro si caratterizza per un ampio ricorso al trattamento dei dati personali.

Preso atto dell'analisi sulle lacune normative individuate elaborato dall'Ufficio Internazionale del Lavoro, il Consiglio di Amministrazione ha deciso che il punto all'ordine del giorno sul lavoro dignitoso dei lavoratori tramite piattaforma della sessione n. 113 della Conferenza Internazionale del Lavoro del 2025 sarà dedicato all'attività di *standard setting* sul tema attraverso una procedura a doppia discussione (GB.347/POL/1, par. 65, come emendato dal Consiglio di Amministrazione).

Pertanto, l'Organizzazione Internazionale del Lavoro ha mosso il primo passo necessario per l'approvazione di uno strumento che, ove il procedimento andasse a buon fine, dovrebbe regolamentare anche la protezione dei dati personali dei lavoratori tramite piattaforma, con particolare attenzione ai rischi per la privacy legati al *management* algoritmico[123].

---

[122] Altre criticità evidenziate riguardano l'accesso dei governi ai codici sorgente degli algoritmi al fine di regolarli; la trasparenza nella gestione algoritmica per supportare la corretta classificazione dei lavoratori; l'equità delle decisioni automatizzate come le valutazioni, la disattivazione dalla piattaforma e altre penalità ; la sorveglianza dei lavoratori.

[123] I passaggi successivi previsti in vista dell'adozione di norme internazionali dell'ILO relative al lavoro tramite piattaforma consistono: nella preparazione da parte dell'Ufficio Internazionale del Lavoro di un rapporto che analizzi la legislazione e la prassi degli Stati rispetto al lavoro su piattaforma; la trasmissione

Passando al secondo ordine di iniziative, quelle riguardanti le "sfide generali" poste dall'evoluzione tecnologica in materia di dati personali dei lavoratori, l'ILO ha proceduto alla calendarizzazione di un *meeting of experts on protection of workers' personal data in the digital era*.

Infatti, nella sessione n. 346 (ottobre-novembre 2022), il Consiglio di Amministrazione ha chiesto all'Ufficio Internazionale del Lavoro la preparazione di proposte per una riunione di esperti sulla protezione dei dati personali dei lavoratori nell'era digitale da sottoporre nella sessione n. 349 (ottobre-novembre 2023) del Consiglio di Amministrazione (GB.346/PV, par. 93g).

Nella sessione successiva del Consiglio di Amministrazione n. 347 del marzo 2023, è stato indicato che il *meeting* di esperti potrebbe esaminare le sfide che emergono riguardo alla protezione dei dati personali dei lavoratori alla luce della crescente digitalizzazione del lavoro e che la riunione potrebbe coprire la raccolta, l'archiviazione, l'uso e la comunicazione dei dati a terzi, il monitoraggio digitale e la gestione algoritmica dei lavoratori. A tal fine, è richiesto all'Ufficio di fornire al Consiglio di Amministrazione, nella sessione 349ª sessione (ottobre-novembre 2023), ulteriori informazioni, comprese considerazioni in merito alla permanente rilevanza e attualità del Codice di condotta dell'ILO sulla protezione dei dati personali dei lavoratori, affinché possa prendere una decisione definitiva sulle modalità e sull'ordine del giorno dell'incontro (GB.347/INS/2/1, sezione "*Subjects under consideration for possible inclusion in the agenda of future sessions of the Conference*", par. 19). Nel citato documento, viene anche evidenziato come per contrastare il pericolo che il trattamento di dati personali possa violare il diritto alla privacy dei lavoratori e, in alcuni casi, dar luogo a fenomeni discriminatori - intensificatosi con l'aumento dell'uso delle tecnologie dell'informazione e della comunicazione a fini lavorativi – sia necessaria la definizione di una *governance* chiara e solida sull'uso dei dati personali dei lavoratori. In particolare, vengono identificati

---

di tale rapporto agli Stati membri e alle organizzazioni dei lavoratori e dei datori di lavoro affinché esprimano i propri commenti; nell'analisi dei commenti e nella formulazione di una proposta di conclusioni da parte dell'Ufficio Internazionale del Lavoro; nella presentazione delle conclusioni alla Conferenza internazionale del lavoro del 2025 per una prima discussione; nella elaborazione da parte dell'Ufficio di un secondo rapporto contenente la sintesi della discussione e un progetto di strumento regolativo sul lavoro su piattaforma; nella trasmissione del secondo rapporto a governi, datori di lavoro e lavoratori per commenti; nella eventuale preparazione da parte dell'Ufficio della revisione del progetto di strumento; nella presentazione del progetto di strumento alla successiva sessione della Conferenza Internazionale del Lavoro (quella del 2026) dove verrà discusso, eventualmente modificato e ne verrà proposta l'adozione (v. artt. 19-22 della Costituzione dell'ILO).

come elementi di particolare preoccupazione, da un lato, l'utilizzo dei dati personali nel contesto dell'*algorithmic management*, dall'altro, le possibili implicazioni sulla sorveglianza tecnologica e il trattamento dei dati dei lavoratori discendenti dal passaggio massivo a forme di lavoro da remoto ("*telework*") accelerato dalla pandemia di Covid-19 (GB.347/INS/2/1, sez. 5b, paragrafi 62-64).

Nell'ultima sessione del Consiglio di Amministrazione (ottobre-novembre 2023) è stato indicato che il *meeting of experts* potrebbe verificare il grado di rilevanza dell'*ILO Code of practice on the protection of workers' personal data* alla luce degli sviluppi tecnologici e, se necessario, aggiornarlo[124]. In alternativa, l'ordine del giorno del *meeting* potrebbe anche affrontare questioni più ampie riguardanti la protezione dei dati personali dei lavoratori nell'era digitale (GB.349/INS/2, paragrafi 38-41, "*Protection of workers' personal data in the digital era*").

Le tempistiche e l'oggetto definitivo della riunione saranno decise dal Consiglio di Amministrazione nella sessione n. 350 del marzo 2024 (GB.349/Decisions, par. 2e)[125].

Alla luce di quanto riportato, non si può non evidenziare come la tutela della privacy del lavoratore, specie nel contesto del *management* algoritmico, stia acquisendo sempre più centralità all'interno degli organi istituzionali dell'Organizzazione Internazionale del Lavoro. Le indicazioni programmatiche contenute nella Dichiarazione del Centenario hanno dato impulso a nuove iniziative che, seppur (ad ora) non si siano tradotte nell'adozione di nuovi strumenti regolativi, potrebbero condurre in un prossimo futuro alla revisione e al rafforzamento degli *standards* di tutela della riservatezza riconosciuti dalle fonti dell'Organizzazione Internazionale del Lavoro.

[124] A tal proposito, nell'allegato I, sez. 3b "*Protection of workers' personal data in the digital era*", è rilevato come "*a preliminary analysis of the Code of practice suggests that the principles underpinning it remain relevant due to its alignment with general data protection standards that have developed over many years. Nevertheless, the development of new technologies brings new dimensions to the interpretation and application of these principles*".

[125] Si riportano le conclusioni adottate dal Consiglio di Amministrazione sul punto: "*the Governing Body … requested the Office to present further proposals on the scope, timing and resourcing of a meeting of experts on the protection of personal data in the digital era to its 350th Session (March 2024)*".

Capitolo III

Digitalizzazione, algorithmic management of work e rischi per la privacy del lavoratore

11. Premessa

Come evidenziato *supra*, l'ILO ha individuato nella gestione algoritmica del lavoro tramite piattaforma uno degli ambiti che pone le principali sfide per la tutela della privacy dei lavoratori. Tale tematica dovrebbe essere affrontata dall'ILO nella sessione n. 113 della Conferenza Internazionale del Lavoro del 2025 nell'ambito della più ampia iniziativa di *standard setting* dedicata al lavoro dignitoso nell'ambito del lavoro tramite piattaforma (v. GB.347/POL/1, par. 65, come emendato dal Consiglio di Amministrazione).

Parallelamente, l'ILO sta programmando la convocazione di un *meeting* di esperti sulla protezione dei dati personali dei lavoratori nell'era digitale a quasi trent'anni di distanza dalla riunione di esperti sulla privacy che ha elaborato il *Code of practice on the protection of workers' personal data* del 1997. Sebbene l'ordine del giorno non sia stato ancora fissato definitivamente, è stata paventata la possibilità di consentire al gruppo di esperti, ove lo ritenga opportuno, di procedere all'aggiornamento del Codice di condotta (v. GB.349/INS/2, paragrafi 38-41 e GB.349/Decisions, par. 2e).

Essendo questo il contesto in cui si inserisce il presente elaborato, in questa sezione si cercherà di fornire una panoramica generale dei principali rischi per la privacy dei lavoratori derivanti dall'evoluzione tecnologica e dalla diffusione della gestione algoritmica del lavoro.

Si ritiene che tale ricostruzione risulti utile a stabilire in che misura il contenuto degli strumenti regolativi di cui l'ILO dispone risulti ancora attuale nonché ad individuare alcuni possibili ambiti di rafforzamento delle tutele.

12. Algorithmic management of work e impatto sulla privacy dei lavoratori

Per esaminare le sfide per la privacy dei lavoratori poste dall'*algorithm management of work* occorre individuare una definizione del fenomeno.

Nel presente elaborato si è prescelto di adottare una nozione ampia del fenomeno, che viene definito come un approccio gestionale che sfrutta l'analisi dei dati e algoritmi per supportare o sostituire il decisore umano nell'esercizio delle funzioni manageriali[126].

L'ambito in cui la gestione algoritmica del lavoro si manifesta con maggiore evidenza è il lavoro tramite piattaforma.

Infatti, nelle piattaforme digitali è diffuso il ricorso a sistemi basati sull'elaborazione algoritmica di dati per l'allocazione delle commesse; il controllo dell'esecuzione della prestazione; la valutazione della *performance* tramite l'assegnazione di un *ranking* che può incidere sull'assegnazione dei turni e sulle occasioni di lavoro nonché, in caso di abbassamento del punteggio al di sotto una soglia prestabilita, determinare la disconnessione dell'*account* con cui il lavoratore ha accesso alla piattaforma[127]. Il

[126] Nel contesto dell'Organizzazione Internazionale del Lavoro, lo studio congiunto condotto dall'ILO e dall'*European Commission's Joint Research Centre* (JRC) relativo all'impatto della gestione algoritmica sull'organizzazione e sulla qualità del lavoro si riferisce al fenomeno come l'utilizzo di algoritmi *"which are digitally encoded and implemented by computers, and which process data*" nell'ambito del *management*, inteso come "*a set of tasks which are necessary for the administration of an organisation … normally implemented by a specialised position which is at the top of the organisational hierarchy: the manager(s) … summarised in five functions: planning (i.e. deciding in advance), staffing, commanding, coordinating and controlling … With algorithmic management, all these functions can be supported or at least partly implemented with computer algorithms, if the associated managerial problems can be numerically encoded in a more or less unambiguous way*" (S. BAIOCCO (JRC), E. FERNANDEZ-MACÍAS (JRC), U. RANI (ILO), A. PESOLE (JRC), *The Algorithmic Management of work and its implications in different context*s, Background paper Series, 21 giugno 2022, pp. 5-6).
S. BAIOCCO e E. FERNÁNDEZ-MACÍAS, *Algorithmic management: A basic compass*, *JRC Science for Policy Brief on Labour, Education and Employment*, 2022, p. 1, definiscono il fenomeno come "*the use of computer programmed procedures, which can be AI or non-AI powered, to coordinate labour input in an organisation. It involves, for example, the definition and assignment of work shifts, the development and delivery of job-related instructions, the assessment of workers' performance and the assignment of rewards or penalties*".

[127] Come visto *supra*, l'analisi dell'Ufficio Internazionale sul Lavoro sui *normative gaps* inerenti al lavoro tramite piattaforma contiene la seguente definizione di *management* algoritmico dei *platform workers*: "*it is an algorithm that offers and grants services or tasks to workers, defines their time slots, calculates the rankings on which their activities and income depend, and decides whether they will continue to provide services for the platform or remain deselected from it*" (GB.347/POL/1, par. 18).

descritto assetto gestionale principalmente prescinde dall'intervento di personale della piattaforma, essendo tali processi altamente automatizzati[128].

In tale contesto, i dati personali dei lavoratori sono "il carburante" che consente il funzionamento delle pratiche di gestione algoritmica che trasformano gli *input* in suggerimenti, raccomandazioni o decisioni che hanno un impatto sul rapporto di lavoro.

Una prima questione impattante sulla privacy dei lavoratori consiste nella circostanza che la costante raccolta di informazioni accresce la possibilità di esercitare un controllo continuativo sulla prestazione. Ciò, ad esempio, è reso possibile dal ricorso a tecnologie quali sistemi di GPS, incorporati nelle applicazioni di *taxi o food delivery*, capaci di raccogliere informazioni come la velocità e sullo stile di guida, la posizione del lavoratore, il percorso eseguito e il tempo impiegato per completare l'ordine o il viaggio[129]. Talvolta, lo stato di avanzamento della consegna può essere tracciato in tempo reale anche dai clienti, ai quali viene comunicato un tempo di attesa approssimativo e consentito di verificare in tempo reale la percentuale di completamento dell'ordine[130].

Il potere di controllo delle piattaforme digitali è altresì accresciuto dal ricorso a forme di "valutazione esterna", riconducibili all'ambito della c.d. *customer o client's satisfaction*, rappresentate dai *feedback* rilasciati dagli utenti sul livello di gradimento del servizio reso dal lavoratore[131].

Se i *feedback*, da un lato, possono risultare utili ad individuare i lavoratori più affidabili, dall'altro lato, consentono al datore di lavoro di sommare le informazioni ricavate dall'esercizio del potere di controllo "ordinario" con quelle provenienti dal "controllo" della clientela, così "duplicando" i fronti del monitoraggio sui lavoratori.

---

[128] Per una ricostruzione del funzionamento dell'algoritmo utilizzato da alcune piattaforme digitali cfr. L. STARK, *Algorithmic Labor and information asymmetries. A case study of Uber's Drivers*, in *IJC*, n. 10, v. 27, 2016 nonché A. INGRAO, *La protezione dei dati personali dei lavoratori nel diritto vivente al tempo degli algoritmi*, in A. BELLAVISTA, R. SANTUCCI (a cura di), *Tecnologie digitali, poteri datoriali e diritti dei lavoratori*, Giappichelli, 2022.

[129] V. S. BAIOCCO (JRC), E. FERNANDEZ-MACÍAS (JRC), U. RANI (ILO), A. PESOLE (JRC), *The Algorithmic Management of work and its implications in different context*s, *cit.*, p. 15.

[130] Cfr. *World Employment and Social Outlook 2021: The Role of Digital Labour Platforms in Transforming the World of Work*, ILO, Ginevra, 2021, p. 75, dove si riporta che "*customers are updated at every step, provided with an approximate waiting time, an estimated fare and ride duration, and have the ability to track their driver and their ride in real time through their mobile application*".

[131] Sul tema cfr., *ex multis*, V. NUZZO, *Customer satisfaction e contratto di lavoro subordinato*, in *DRI*, 1/2020, 27 ss. e Q. WU, H. ZHANG, Z. LI e K. LIU, *Labor Control in the Gig Economy: Evidence from Uber in China*, in *Journal of Industrial Relations*, vol. 61(4), 2019, pp. 574 ss.

Inoltre, le valutazioni richieste ai clienti potrebbero trascendere il giudizio sulla mera abilità/capacità oggettiva di portare a termine correttamente e con competenza il compito assegnato, estendendosi a giudizi sulle qualità soggettive del prestatore quali il grado di cortesia rilevato.

Si corre, poi, il rischio di sovrapposizione tra valutazione della *performance* del singolo lavoratore e livello di soddisfazione rispetto al servizio complessivamente fornito dall'organizzazione datoriale. Infatti, il lavoratore potrebbe rimanere penalizzato per disfunzioni organizzative non direttamente imputabili allo stesso che hanno inciso sul grado di soddisfazione dell'utente[132].

L'utilizzo dei dati per valutare/controllare la prestazione dei lavoratori non rappresenta certo una novità propria della gestione algoritmica della prestazione: già semplici macchinari industriali consentono di calcolare il numero di unità di prodotto realizzate in un determinato lasso di tempo e, quindi, di ricavare il livello di produttività dei singoli lavoratori. Così come la richiesta di *feedback* e giudizi sui lavoratori rappresenta un fenomeno diffuso anche presso le organizzazioni datoriali "tradizionali" come nel caso delle richieste di valutazione del servizio reso dagli operatori dei *call-center* o dagli impiegati delle concessionarie di autovetture.

Tuttavia, tradizionalmente, le informazioni sui lavoratori sono "filtrate" da parte di un valutatore umano, il quale può fornire una lettura interpretativa dei dati che tenga in considerazione tutte le circostanze del caso concreto. A titolo di esempio, un basso livello di produttività potrebbe dipendere da circostanze estranee alla sfera di controllo del lavoratore come problematiche di funzionamento dei macchinari o ritardi nella fornitura

[132] Per minimizzare tale rischio, potrebbe considerarsi l'adozione di alcuni accorgimenti tecnici come la richiesta al cliente di fornire una breve giustificazione della valutazione, tenendo in considerazione solo i giudizi negativi che presentino motivazioni adeguate e pertinenti. In alternativa, al cliente che intenda esprimere un giudizio negativo potrebbe essere richiesto di indicare una specifica motivazione all'interno di un elenco di opzioni predisposto a priori contenente ragioni oggettive quali, a titolo di esempio, la mancata esecuzione del servizio.
Sembrerebbe, poi, opportuno che i giudizi espressi siano comunicati o accessibili al lavoratore: da un lato, ciò consentirebbe al lavoratore di contestare fatti riferiti dal cliente non corrispondenti al vero o, comunque, di esprimere il proprio punto di vista; dall'altro, il lavoratore potrebbe acquisire conoscenza degli specifici aspetti oggetto di valutazione negativamente, così da poter adeguare la propria condotta *pro futuro*. Tuttavia, potrebbero porsi esigenze di tutela della riservatezza del soggetto che ha espresso il giudizio, specie ove il lavoratore, per la tipologia del servizio reso, possegga o possa agevolmente ottenere informazioni quali l'indirizzo del cliente. In questi casi, i giudizi potrebbero essere comunicati al lavoratore in forma anonima, rendendo, però, più difficile per il lavoratore contestare la valutazione o esprimere la propria opinione.

dei materiali oppure potrebbe essere compensato da altre qualità non registrate dai dati come la disponibilità ad aiutare i colleghi. Allo stesso modo, un giudizio negativo potrebbe dipendere dalla circostanza che l'operatore ha dovuto interfacciarsi con un cliente scontroso o che presentava un problema oggettivamente non risolvibile.

Invece, nell'*algorithmic management* in senso stretto, le informazioni e i dati sul lavoratore sono elaborati per generare "decisioni algoritmiche automatiche" che incidono sulle condizioni di lavoro e, quindi, sulla capacità di generare reddito.

Infatti, le informazioni acquisite sul lavoratore – che possono essere le valutazioni fornite da clienti e/o esercenti, la revoca della disponibilità a fornire il servizio in uno *slot* temporale precedentemente selezionato, il numero di ordini accettati e rifiutati, la tempestività nel completare il servizio – sono elaborate per formare graduatorie tra i lavoratori. Il *ranking* calcolato dall'algoritmo può incidere sotto diversi aspetti: sull'allocazione delle offerte di lavoro che vengono indirizzate verso coloro che presentano un punteggio più elevato; sull'ordine di prenotazione degli *slot* di svolgimento della prestazione e, quindi, sulla possibilità di lavorare nei turni ad alta intensità che presentano maggiore richiesta di servizi e/o offerte di lavoro più remunerative[133]; sulla stessa possibilità di accedere all'*account* che può essere sospeso o, financo, disattivato automaticamente se il lavoratore scende al di sotto di un punteggio minimo[134].

Ciò pone ulteriori profili rilevanti sotto il profilo della tutela della privacy dei lavoratori, in particolare sotto il profilo della trasparenza e delle informazioni rese all'interessato. Infatti, spesso, i lavoratori non sono informati/adeguatamente informati né su come vengono trattati i loro dati personali né sulle modalità e sulle logiche di funzionamento dei sistemi che li utilizzano, in tutto o in parte, per assumere decisioni impattanti sulle loro condizioni lavorative.

Emblematico in tal senso è un provvedimento del Garante per la protezione dei dati personali che - pur emesso nello specifico contesto italiano in cui trovano applicazione la l. 20 maggio 1970, n. 300 (c.d. Statuto dei lavoratori), il Regolamento UE 2016/679 (c.d.

---

[133] Si pensi, per quanto riguarda i *riders*, alla scelta degli orari di pranzo/cena di giornate festive dove, normalmente, pervengono maggiori ordini e le piattaforme, spesso, riconoscono maggiorazioni al fine di incentivare i lavoratori a rendersi disponibili a effettuare le consegne.

[134] È stata ampiamente riportata, anche nei *media* generalisti, la vicenda del *rider* fiorentino deceduto durante una consegna che ha ricevuto un messaggio preimpostato e automatico di disattivazione dell'*account*.

GDPR) e il d.lgs. 30 giugno 2003, n.196 (c.d. Codice Privacy) - ha rilevato la commissione di diverse infrazioni della disciplina in materia di protezione dei dati personali da parte di una nota piattaforma di *food delivery* sotto il profilo della trasparenza[135].

Infatti, è stato riscontrato che i lavoratori non erano stati messi nelle condizioni di conoscere con precisione le modalità con cui i loro dati personali erano trattati, essendo le informazioni fornite poco trasparenti e inidonee a consentire di comprendere con pienezza le modalità di utilizzo dei propri dati personali.

In particolare, è stato accertato che ai *riders* non erano state comunicate le effettive modalità di trattamento dei dati relativi alla propria posizione geografica - consistenti nella visualizzazione su mappa del percorso effettuato e nella raccolta sistematica del dato ogni quindici secondi - ma soltanto generiche informazioni sul ricorso alla geolocalizzazione. Inoltre, il Garante per la protezione dei dati personali ha ravvisato omissioni informative circa la "*effettuazione di trattamenti automatizzati compresa l'attività di profilazione ... preordinati all'assegnazione di un punteggio al rider al dichiarato fine di determinare la priorità nella prenotazione degli slot"* nonché sulle *"informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato*"[136].

Tuttavia, il fenomeno della gestione algoritmica trascende l'ambito del lavoro tramite piattaforma, essendo diffuso anche in settori produttivi tradizionali.

Un esempio particolarmente significativo riguarda l'utilizzo di sistemi di gestione algoritmica del personale nel settore della logistica, dove, a titolo di esempio, spesso gli addetti al c.d. *picking* e/o i carrellisti ricevono indicazioni sulla localizzazione dei prodotti da sistemare e/o spostare e sulle relative tempistiche tramite applicazioni incorporate in

---

[135] Garante per la protezione dei dati personali, ordinanza di ingiunzione 10 giugno 2021 n. 234.

[136] *Ibidem*, p. 16. Il riferimento è all'art. 13 "*Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato*", comma 2, lett. f), Reg. UE 2016/679. Ai sensi della predetta disposizione, il titolare del trattamento (la piattaforma) deve fornire all'interessato (il lavoratore) adeguata informazione circa "*l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1* (processo decisionale automatizzato, compresa la profilazione, basato su "dati comuni") *e 4* (processo decisionale automatizzato, compresa la profilazione, basato su categorie particolari di dati personali)*, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato*".

wearables o strumenti di lavoro[137].

Vi sono testimonianze giurisprudenziali di utilizzo di questa modalità di organizzazione del lavoro anche nel settore logistico nazionale[138].

In particolare, Trib. di Padova, Sez. Lav., sentenza 3 marzo 2023 n. 126, ha ravvisato l'esistenza di forme di gestione algoritmica in una controversia avente ad oggetto l'accertamento della genuinità o meno di contratti di appalto con cui l'impresa committente aveva demandato specifiche lavorazioni a terzi fornendo "*il programma informatico che dice al lavoratore cosa deve essere spostato, dove si trova e dove deve essere portato*" (p. 5)[139]. La sentenza ha ritenuto che, dietro lo schema del contratto di appalto, in realtà, fosse celata una prestazione di mera fornitura di manodopera da parte dell'impresa appaltatrice in quanto il sistema che consentiva di dirigere e controllare l'attività dei lavoratori faceva capo all'impresa committente. Tale elemento è stato ritenuto elemento dirimente ai fini dell'imputazione in capo alla committente (datore di lavoro sostanziale) del rapporto di lavoro formalmente intercorrente tra il dipendente e l'impresa appaltatrice (datore di lavoro formale).

Tuttavia, mentre le piattaforme sono "ontologicamente" strutturate su pratiche di gestione algoritmica, nei settori "standard" i sistemi di gestione algoritmica sono incorporati

---

[137] In dottrina, il fenomeno è esaminato, tra gli altri, da A. DELFANTI, *Machinic Dispossession and Augmented Despotism: Digital Work in an Amazon Warehouse*", in *New Media & Society*, vol. 23/2019, 39 ss., A. WOOD, *Algorithmic Management: Consequences for Work Organisation and Working Conditions*, in *JRC Working Papers Series on Labour, Education and Technology*, European Commission, 2021, K. C. KELLOGG, M.A. VALENTINE, A. CHRISTIN, *Algorithms at Work: The New Contested Terrain of Control*, in *Academy of Management Annals*, vol. 14, 2020, pp. 366 ss.

[138] Al di fuori del settore della logistica, un altro caso noto di utilizzo di algoritmi ai fini di assumere decisioni relative al rapporto di lavoro riguarda l'utilizzo di un sistema automatizzato da parte del MIUR per disporre i trasferimenti e le assegnazioni dei docenti nell'ambito del piano straordinario di assunzione previsto dalle L. 107/2015 (c.d. "Buona Scuola").
La vicenda è stata affrontata da Cons. Stato, sez. VI, 8 aprile 2019, n. 2270 e da Cons. Stato, sez. VI, sent. del 4 febbraio 2020, n. 881. Quest'ultima pronuncia ha ritenuto la procedura viziata per difetto di trasparenza data "*l'impossibilità di comprendere le modalità con le quali, attraverso il citato algoritmo, siano stati assegnati i posti disponibili*".
Per una ricostruzione più approfondita della vicenda v. F. LAUS, *La tecnologia nella pubblica amministrazione: algoritmi e processi decisionali nei procedimenti amministrativi. Il caso della procedura di mobilità*, in *Il lavoro nelle pubbliche amministrazioni*, 3/2020, pp. 49 ss.

[139] Per un commento della pronuncia si rinvia a G. SANFILIPPO, *La verifica della genuinità dell'appalto nelle organizzazioni d'impresa (ultra)digitalizzate. Nota a Tribunale di Padova, Sez. Lav., sentenza 3 marzo 2023 n. 126*, in *Lavoro Diritti Europa*, 22 giugno 2023 e L. NANNIPIERI, *Eterodirezione "algoritmica" negli appalti della logistica. Verso un quadro giurisprudenziale in mutamento*, in *Rivista Italia di Informatica e Diritto*, 1/2023, 205 ss.

all'interno di un'organizzazione di lavoro preesistente[140]. Il che può rendere più difficile identificare l'utilizzo di tali pratiche, specie qualora i sistemi siano utilizzati come supporto a decisioni assunte e comunicate ai lavoratori da personale dell'impresa quali determinazioni su quali candidati assumere o quali lavoratori promuovere[141].

13. Nuove frontiere del controllo tecnologico sul lavoratore…

La sempre maggiore capacità degli strumenti tecnologici di immagazzinare, conservare e elaborare grandi quantità di dati personali hanno reso le potenzialità di sorveglianza dei lavoratori ancora più intense e pervasive.

Già la stabile introduzione nei sistemi produttivi aziendali dei computer comporta la raccolta e la conservazione di una grande quantità di informazioni potenzialmente idonea a ricostruire minuziosamente lo svolgimento dell'attività lavorativa. Basti pensare a come l'esame della cronologia dei siti *web* visitati e l'accesso alla posta elettronica possano permettere al datore di lavoro di ricostruire l'attività svolta dal prestatore.

La situazione si è ulteriormente complicata con la diffusione di pratiche di utilizzo promiscuo degli strumenti di lavoro, utilizzati sia per scopi privati sia per svolgere la prestazione lavorativa.

Emblematica in tal senso è la pratica del c.d. BYOD (*Bring Your Own Device*) consistente nell'utilizzo da parte dei lavoratori di dispositivi personali - quali *smartphone*, *personal computer*, *tablet* - per accedere alle applicazioni e ai dati aziendali e/o svolgere la prestazione lavorativa. All'opposto, le imprese sempre più di frequente consentono, a titolo di *fringe benefit*, di utilizzare anche a fini personali strumenti di lavoro e apparecchiature aziendali.

In questo modo, vengono conservate all'interno del dispositivo sia informazioni relative alla vita privata del dipendente sia dati aziendali, accrescendo il rischio che il datore di lavoro possa accedere a informazioni sensibili relative alla sfera privata del lavoratore quali fotografie, messaggi, chiamate e siti web visitati al di fuori dall'orario di lavoro.

---

[140] S. BAIOCCO (JRC), E. FERNANDEZ-MACÍAS (JRC), U. RANI (ILO), A. PESOLE (JRC), *The Algorithmic Management of work and its implications in different context*s, *cit.*, p. 17.

[141] V. F. BORDONI, *Il processo di selezione del personale e la sua automazione in Italia*, in *Labour & Law Issues*, vol. 9, n. 1, 2023.

Inoltre, gli strumenti di lavoro aziendali possono contenere sistemi di geolocalizzazione, incorporati o appositamente installati, idonei a raccogliere informazioni sulla posizione del lavoratore e a memorizzare i luoghi in cui questo si è recato anche al termine dell'orario di lavoro. Il che potrebbe rivelare informazioni su abitudini, interessi, frequentazioni abituali e, financo, sullo stato di salute del lavoratore (ad esempio, nel caso in cui il prestatore si sia recato presso strutture sanitarie destinate alla cura di particolari patologie)[142].

Questioni di privacy sono poste anche dall'ingresso nei luoghi di lavoro nell'ambito di programmi di *wellbeing* aziendale dei c.d. dispositivi indossabili o *wearebles* come braccialetti di *fitness tracker* che tengono traccia di dati personali come il numero di passi compiuti durante la giornata e la frequenza del battito cardiaco del lavoratore[143]. Con questi strumenti, il datore di lavoro potrebbe avere accesso a un flusso continuativo e significativo di informazioni sensibili, compresi i dati biometrici. Queste informazioni potrebbero costituire la base - magari inconscia o non dichiarata - per assumere decisioni sui lavoratori basate sul loro stato di salute. Inoltre, sebbene tali programmi potrebbero essere ad adesione volontaria, i lavoratori potrebbero sentirsi costretti a partecipare per timore che ciò possa pregiudicare lo sviluppo della loro carriera, se non la stessa permanenza nel posto di lavoro nel caso di vigenza di regimi di licenziamento *ad nutum*. Ciò può, quindi, porre criticità sulla effettiva libertà del consenso eventualmente prestato dal lavoratore.

---

[142] A tal proposito, si ritiene rilevante segnalare la sentenza della Corte Europea dei Diritti dell'Uomo, Sez. IV, 13 dicembre 2022, Florindo de Almeida Vasconcelos Gramaxo c. Portogallo, ricorso n. 26968/2016. Il caso riguarda un'azienda farmaceutica portoghese che aveva autorizzato un proprio rappresentante a utilizzare il veicolo aziendale anche a scopi privati, a patto che i chilometri percorsi per finalità non connesse all'espletamento della prestazione lavorativa fossero rimborsati secondo una tariffa agevolata predeterminata. L'azienda, per controllare la veridicità del chilometraggio dichiarato ai fini del rimborso spese, aveva installato all'interno dell'autovettura un sistema GPS, il quale, aveva registrato ogni spostamento del dipendente, compresi quelli compiuti al di fuori dell'orario lavorativo.
Per un commento della pronuncia si rinvia a M. NOGUEIRA GUASTAVINO, *Geolocalización lícita, probablemente desproporcionada. La necesidad de una vigilancia cualitativa, no cuantitativa*, in Revista de jurisprudencia laboral, 2/2023 e a D. TARDIVO, *Controlli tramite l'(ab)uso di dispositivi di geolocalizzazione alla luce dell'art. 8 Cedu*, in *Arg. Dir. Lav.*, 3/2023.

[143] V. K. MALTSEVA, *Wearables in the workplace: The brave new world of employee engagement*, in *Business Horizons*, Vol. 63, Issue 4, 2020, p. 493 ss. Ad esempio, i programmi di *wellbeing* possono essere progettati per consentire al lavoratore di usufruire di sconti sulle spese mediche previste dal piano assicurativo sanitario stipulato dal datore di lavoro.

Inoltre, i lavoratori coinvolti nel programma potrebbero sentirsi costretti a raggiungere o superare gli *standard* richiesti per timore che ciò possa influenzare la loro considerazione da parte del datore di lavoro. Questo timore può avere riflessi sulla vita privata del lavoratore, intesa come libertà di autodeterminarsi al di fuori dell'orario di lavoro: così, al termine di una giornata di lavoro, magari intensa e abbastanza sedentaria, il prestatore potrebbe sentirsi tenuto a effettuare attività fisica per aumentare il numero di passi giornaliero invece che dedicarsi ad altre attività.

I *wearables*, poi, possono essere anche utilizzati per analizzare lo stato emotivo dei lavoratori come nel caso di incorporazione di sensori diretti alla misurazione del livello di *stress* del prestatore sulla base dell'analisi di dati come il cambiamento della frequenza cardiaca o il livello di sudorazione[144].

In questo modo, però, si assiste a una crescente invasione delle sfere più intime della persona-lavoratore, il suo stesso corpo e le sue emozioni.

13.1. … e sul telelavoratore

Con la crescita esponenziale del lavoro da remoto durante la pandemia di Covid-19, è accresciuto anche l'utilizzo di sistemi di tracciamento e di monitoraggio dell'attività dei lavoratori a distanza. Infatti, le imprese, preoccupate per l'impossibilità di verificare "visivamente" se un lavoratore stia effettivamente svolgendo o meno la prestazione, stanno ricorrendo a sistemi di monitoraggio che accrescono notevolmente le potenzialità di controllo già insite negli strumenti di lavoro[145].

Si sta facendo riferimento a sistemi capaci di registrare ogni tasto premuto dal lavoratore sulla tastiera (c.d. *keyloggers*), i movimenti del *mouse*, i siti web visitati e lo schermo del computer, effettuare *screenshot* del *monitor* e fotografare il lavoratore a intervalli casuali[146].

---

[144] V. ibidem, p. 494 e J. FULLERTON, *'Mind-reading' tech being used to monitor Chinese workers' emotions*, in *The Telegraph*, 30 aprile 2018.

[145] Cfr. A. SATRIANO, *How my boss monitor me while I work from home*, in *The New York Times*, 6 maggio 2020.

[146] Cfr. F. HENDRICKS, *Privacy e workplace monitoring in global legal perspective*, in C. PISANI, G. PROIA, A. TOPO (a cura di), *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Milano, Giuffrè, 2022.

Oltre a questioni relative alla proporzionalità del monitoraggio, questi sistemi pongono rischi sotto il profilo della trasparenza del trattamento in quanto, ove non informati, i lavoratori potrebbero anche non rendersi conto di essere sottoposti a sorveglianza[147].

14. Tutela della riservatezza del lavoratore e social network

Un ulteriore aspetto problematico è dovuto alla presenza sul web di una miriade di "tracce" relative alla propria persona lasciate, più o meno consapevolmente, dal lavoratore.

In particolare, negli ultimi decenni, è diventato di uso comune la condivisione nei *social network* di momenti di vita quotidiana, opinioni personali, gusti e abitudini. Pertanto, il profilo di un lavoratore può rivelare numerose informazioni private non strettamente attinenti alla valutazione dell'attitudine professionale come lo stato di famiglia, la presenza di figli minori a carico, le opinioni del lavoratore rispetto a tematiche politico-sociali e le abitudini extra-lavorative. Queste informazioni possono essere utilizzate per la ricostruzione della personalità e dello stile di vita del candidato all'impiego/lavoratore, per prevedere l'andamento professionale del lavoratore e per assumere decisioni inerenti al rapporto di lavoro[148].

D'altro canto, i *social network* potrebbero anche contenere informazioni rilevanti ai fini della valutazione della professionalità del lavoratore sia in fase di assunzione sia in costanza di rapporto di lavoro.

Quanto alla fase di instaurazione del rapporto, le informazioni contenute sui *social* potrebbero risultare rilevanti per escludere l'idoneità professionale di un candidato

---

[147] Cfr. S. MORRISON, *Just because you're working from home doesn't mean your boss isn't watching you*, Vox, 2 aprile 2020. L'articolo descrive il funzionamento di strumenti di tracciamento delle attività dei lavoratori da remoto come *TeamViewer* che consente al datore di lavoro di guardare in tempo reale il *monitor* dei dipendenti dal proprio computer nonché di "software dell'attenzione" come la funzione di *Zoom* che consentiva di individuare i partecipanti che, presumibilmente, non stavano seguendo la riunione. Tale funzione, che doveva servire per valutare l'efficacia degli eventi di informazione, ma che avrebbe potuto avere uno sviluppo nei *meeting on line* di lavoro, è stata in seguito disabilitata a seguito delle proteste provenienti dagli utenti (v. la nota di *Zoom* consultabile al seguente link: https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0069153).

[148] Peraltro, tali ricostruzioni potrebbero rivelarsi non aderenti alla realtà. Infatti, come noto, i *social network* sono spesso utilizzati per veicolare all'esterno una determinata immagine sociale che potrebbe non essere totalmente aderente all'effettiva personalità dell'individuo. Così una persona in realtà laboriosa e introversa potrebbe volersi mostrare ai *follower* di *Facebook* o *Instagram* come dotata di una intensa vita sociale, condividendo esclusivamente serate in discoteca o altri momenti di conviviali tà.

rispetto a una posizione lavorativa vacante. Si pensi all'ipotesi di un lavoratore che abbia postato contenuti di incitamento all'odio o alla violenza che testimonino la sua inattitudine a svolgere una mansione in cui si troverebbe a contatto con il pubblico.
Tuttavia, dal punto di vista pratico, a meno che non si tratti di *social network* dedicati alla ricerca di un'occupazione come *LinkedIn*, può risultare complicato per un *recruiter* sapere a priori in quale tipologia di informazioni si imbatterà. In altri termini, la ricerca sui *social network* di informazioni oggettivamente rilevanti ai fini dell'instaurazione del rapporto potrebbe comportare anche l'accesso a informazioni relative alla vita privata del candidato che - magari inconsapevolmente - possono portare a "scartarlo" per aspetti della sua vita privata e/o familiare che non dovrebbero essere oggetto di considerazione. In tale circostanza, si pone la questione se sia sufficiente o meno informare il candidato della possibilità di controllo dei *social network* e/o l'ottenimento del suo consenso. Ciò non tanto per la circostanza che l'asimmetria di potere caratterizzante il rapporto di lavoro dovrebbe rendere il consenso una base giuridica per il trattamento dei dati personali recessiva e residuale; quanto piuttosto per la circostanza che è discutibile che il consenso del lavoratore possa consentire al datore di lavoro di accedere anche a informazioni personali non attinenti ai fini della valutazione dell'idoneità professionale. Invece, nel momento in cui il rapporto lavorativo risulta già instaurato, i *social network* potrebbero assumere rilevanza sotto diversi profili.
Innanzitutto, il datore di lavoro ha interesse a controllare e sanzionare l'utilizzo improprio dei *social network* durante l'orario di lavoro.
In secondo luogo, il profilo del lavoratore potrebbe contenere informazioni su condotte extra-lavorative potenzialmente rilevanti ai fini dell'adempimento della prestazione lavorativa. Così, il titolare di un'azienda deputata al trasporto di persone potrebbe ravvisare l'inidoneità allo svolgimento della prestazione di un autista qualora questi, in una storia *Instagram* pubblicata da lui o da un conoscente, risulti in stato di apparente alterazione alcolica poche ore prima dell'inizio del turno. Oppure i *social network* potrebbero rivelare che un lavoratore assente per malattia sta svolgendo attività potenzialmente incompatibili con la sussistenza di un effettivo stato morboso o idonee a ritardarne la guarigione. Così come il lavoratore potrebbe postare nella propria bacheca personale o all'interno di gruppi chiusi commenti lesivi della reputazione e dell'immagine dell'azienda.

Altre sfide per la vita privata del lavoratore possono riguardare il ricorso da parte delle aziende e delle pubbliche amministrazioni di *social media policy* o codici di condotta che regolamentino l'attività *social* del lavoratore al di fuori dall'orario lavorativo[149]. Se, da un lato, queste *policy* potrebbero risultare utili per rendere edotti i lavoratori della possibile rilevanza, anche disciplinare, dell'utilizzo dei *social media* fuori dall'orario di lavoro, queste, ove non si limitino a ribadire regole di buon senso generale - come il divieto di nuocere al prestigio, al decoro o all'immagine dell'impresa o della pubblica amministrazione - potrebbero incidere sulla libertà di autodeterminarsi nella propria vita privata extra-lavorativa[150].

15. Considerazioni riassuntive

La ricostruzione generale svolta dimostra come il rispetto dei diritti del lavoratore alla privacy e alla protezione dei dati personali siano sempre più messi in discussione dall'evoluzione tecnologica e dalla gestione algoritmica del lavoro.

Questo è dovuto a diverse ragioni quali il crescente numero di informazioni sulla persona-lavoratore disponibili sul *web* e sui *social media*; l'ingresso nelle organizzazioni aziendali di pratiche di raccolta di *feedback* e valutazioni sui lavoratori; la diffusione sul luogo di lavoro di strumenti e sistemi capaci di raccogliere in modo continuativo dati personali del lavoratore anche altamente sensibili; la diffusione di nuove applicazioni e modalità di utilizzo dei dati personali come per la "lettura della sfera interiore" del lavoratore allo scopo di misurarne, ad esempio, lo stato emotivo e la resistenza allo *stress*; l'accresciuta potenzialità di utilizzo, anche non intenzionale, delle informazioni raccolte sul lavoratore - sempre più numerose, dettagliate e sensibili - per utilizzi discriminatori o comunque

[149] A tal proposito cfr. E. DAGNINO, *Dalla fisica all'algoritmo: una prospettiva di analisi giuslavoristica*, Adapt University Press, 2019, p 156.

[150] Queste pratiche, poi, pongono criticità anche sotto il profilo di libertà di espressione e di critica. Ad esempio, l'articolo 11 *ter*, comma 2, del Codice di comportamento dei dipendenti pubblici (D.P.R. n. 16 aprile 2013, n. 62), inserito dall'articolo 1, comma 1, lettera a) del D.P.R. 13 giugno 2023, n. 81, regola "*l'utilizzo dei mezzi di informazione e dei social media*", prevedendo che il dipendente pubblico debba "*astenersi da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro o all'immagine*" non solo "*dell'amministrazione di appartenenza*", ma anche "*della pubblica amministrazione in generale*". Ciò pone possibili frizioni con il diritto di critica, riconosciuto a ogni cittadino, circa l'operato dei pubblici servizi.

impropri; la crescente complessità delle tecnologie utilizzate per il trattamento dei dati personali che incrementano l'asimmetria informativa tra le parti del rapporto di lavoro; la mancanza di trasparenza circa le logiche di funzionamento dei sistemi decisionali automatizzati o semi-automatizzati che utilizzano, in tutto o in parte, dati personali dei lavoratori.

Lo scenario delineato dimostra la centralità del ruolo ricoperto dalla privacy anche come strumento in grado di rinforzare la protezione del lavoratore in ambiti ulteriori. Infatti, le regole sull'acquisizione dei dati personali nel contesto lavorativo possono prevenire l'utilizzo delle informazioni per scopi discriminatori.

Inoltre, la protezione della privacy può incidere positivamente sotto il profilo della salute e sicurezza sul lavoro. Infatti, un eccessivo livello di monitoraggio e la mancanza di trasparenza circa l'utilizzo dei propri dati personali può incidere sul benessere psicologico del lavoratore nonché indurlo a incrementare il ritmo della propria prestazione, rendendo più probabile la commissione di errori e il verificarsi di incidenti legati al lavoro. Pertanto, è da valutarsi positivamente la "rinnovata" attenzione che l'Organizzazione Internazionale del Lavoro sta dimostrando per assicurare un adeguato livello di tutela della *privacy* nel contesto occupazionale.

Capitolo IV

Considerazioni sulle fonti dell'Organizzazione Internazionale del Lavoro sulla tutela della privacy dei lavoratori

16. Premesse

Nella presente sezione verranno svolte alcune considerazioni sulle fonti che tutelano la riservatezza del lavoratore adottate dall'Organizzazione Internazionale del Lavoro, per come ricostruite nella prima parte dell'elaborato.

Tali considerazioni riguarderanno due ambiti distinti. In primo luogo, sarà svolta una valutazione di tipo contenutistico finalizzata ad evidenziare alcune possibilità di adattamento e di sviluppo del Codice di Condotta del 1997 per far fronte alle sfide poste dall'evoluzione tecnologica e dalla gestione algoritmica del lavoro in considerazione della circostanza che questo strumento potrebbe essere prossimamente aggiornato (v. *supra*).

Di seguito, saranno svolte considerazioni sulla tipologia delle fonti da cui promanano le previsioni inerenti alla tutela della riservatezza del lavoratore, anche alla luce delle iniziative che si stanno sviluppando nell'ambito dell'ILO a seguito della Dichiarazione del Centenario del 2019.

17. Code of practice on the protection of workers' personal data: ambito di applicazione e destinatari delle previsioni

Il Codice di Condotta contiene previsioni rivolte non solo al datore di lavoro, ma anche alle agenzie per l'impiego privato e alle rappresentanze sindacali dei lavoratori.

Queste disposizioni sono dirette a tutelare i *workers*, intesi come "*any current or former worker or applicant for employment*" (art. 3, par. 4), sia nel settore pubblico che privato (art. 4, par. 1, lett. a). Nel Commentario allegato al Codice si legge che "*ILO instruments generally do not define "worker", leaving it to national law and practice*".

Tuttavia, potrebbe essere opportuno valutare se questa scelta risulti ancora adeguata rispetto all'attuale contesto. Infatti, potrebbe accadere che alcuni soggetti che prestano

attività di lavoro, in alcuni contesti nazionali, siano esclusi dall'ambito di applicazione del Codice di condotta.

Inoltre, il Codice di Condotta non fa riferimento alcuno ai soggetti che producono, sviluppano e forniscono i sistemi che trattano i dati dei lavoratori.

Con lo sviluppo informatico, i sistemi che comportano maggiore compressione della privacy dei lavoratori hanno raggiunto un livello di complessità tale che lo stesso datore di lavoro potrebbe non avere completa contezza di come questi trattino i dati personali dei lavoratori. Inoltre, spesso, sono tali soggetti a detenere le competenze necessarie per progettare gli strumenti nel rispetto dei principi e delle regole poste dal Codice di Condotta, minimizzando la raccolta e l'utilizzo di dati non necessari o adottando soluzioni tecnologicamente avanzate per ridurre l'impatto sulla privacy dei lavoratori.

È vero che il datore di lavoro, quando intenda utilizzare sistemi tecnologici realizzati da terzi, potrà informarsi sulle modalità con cui sono trattati i dati personali nonché chiedere adattamenti o la disattivazione di determinate funzioni per rendere il sistema compatibile con le regole poste a tutela della privacy dei lavoratori. Tuttavia, considerare esplicitamente all'interno del Codice ILO la "catena di sviluppo e fornitura" dei sistemi potrebbe favorire l'adozione di *default* di misure adeguate alla protezione dei dati personali dei lavoratori piuttosto che basarsi sull'attivazione - rimediale, eventuale ed *ex post* - del datore di lavoro. Oppure lo sviluppatore, nella progettazione del sistema, potrebbe "mantenere del margine di manovra" per modificare senza particolari "sforzi tecnici" alcune funzioni particolarmente lesive della privacy.

Per tali ragioni, potrebbe essere oggetto di valutazione l'introduzione di previsioni *ad hoc* quali l'obbligo di fornire informazioni chiare ed esaustive sul funzionamento dei sistemi di trattamento dei dati personali e sulle misure adottate per salvaguardare la privacy dei lavoratori. I destinatari di tali informazioni potrebbero essere - oltre al datore di lavoro o l'agenzia per l'impiego che intende avvalersi del sistema - anche i lavoratori e/o le rappresentanze sindacali, così da agevolarne la valutazione sulla *compliance* rispetto alle previsioni del Codice di condotta.

17.1. Code of practice on the protection of workers' personal data: processi decisionali automatizzati

Con riguardo ai processi decisionali automatizzati, il Codice di condotta prevede che "*decisions concerning a worker should not be based solely on the automated processing of that worker's personal data*" (art. 5, par. 5) e, in particolare, che "*personal data collected by electronic monitoring should not be the only factors in evaluating worker performance*" (art. 5, par. 6).

Il Codice ILO, quindi, preclude l'adozione di decisioni relative ai lavoratori basate esclusivamente su un'elaborazione informatizzata di dati personali. Questa, quindi, può, tutt'al più, costituire un ausilio per la decisione del datore di lavoro, il quale, però, non può esimersi dall'esaminare tutte le circostanze del caso concreto al fine di valutare correttamente l'*output* fornito dal trattamento automatizzato.

Sotto tale profilo, il Codice ILO si differenzia da altri strumenti di *data protection* che, invece, ammettono il ricorso a decisioni automatizzate, ancorché in specifiche circostanze e a fronte di apposite garanzie. Il GDPR, all'art. 22, in linea di principio, prevede il diritto dell'interessato di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato di dati personali, compresa la profilazione[151], che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. Tuttavia, lo stesso art. 22 del GDPR ammette il ricorso a processi decisionali automatizzati qualora la decisione "*sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento* (art. 22, comma 1, lett. a) o "*vi sia il consenso dell'interessato*"[152]. In questo caso, però, il GDPR prevede alcune garanzie in favore dell'interessato. In primo luogo, il titolare del trattamento (la piattaforma) deve

[151] Ai sensi dell'art. 4, comma 1, n. 4, GDPR per profilazione si intende "*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*".

[152] Nell'ordinanza-ingiunzione irrogata alla piattaforma di *food delivery* Foodinho s.r.l. (provv. n. 234 del 10 giugno 2021), il Garante italiano per la protezione dei dati personali ha ritenuto che, nel contesto della gestione algoritmica dei *platform workers*, "*risulta applicabile una delle esenzioni previste dall'art. 22 rispetto al diritto di non essere sottoposti a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici o che incida in modo significativo sull'interessato e che, in particolare, risulta che il trattamento è necessario per l'esecuzione di un contratto stipulato tra le parti (v. art. 22, par. 2, lett. a) del Regolamento)".*

preavvertire l'interessato (il lavoratore) circa "*l'esistenza di un processo decisionale automatizzato, compresa la profilazione*" nonché fornire "*informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato*" (art. 13, comma 2, lett. f) e art. 14, comma 2, lett. g).

In secondo luogo, "*il titolare del trattamento deve attuare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione*" (art. 22, comma 3)[153].

Il GDPR è stato individuato da parte della dottrina come possibile rimedio alla opacità delle decisioni algoritmiche[154] e, in effetti, alcune decisioni rilevanti ne hanno fatto applicazione per accrescere la trasparenza e ridurre l'asimmetria informativa esistente che caratterizza l'*algorithmic management*[155]. D'altro canto, come rilevato nella relazione

[153] Sotto tale profilo, il GDPR sembra differenziarsi rispetto alla Raccomandazione CM/Rec(2015)5 sul trattamento di dati personali nel contesto occupazionale. Infatti, la Raccomandazione – precisato che "*an employee should not be subject to a decision significantly affecting him or her, based solely on an automated processing of data without having his or her views taken into consideration"* (art. 11, par. 5) – prevede che l'interessato dovrebbe ottenere, dietro propria richiesta ("*upon request*"), "*information on the reasoning underlying the data processing, the results of which are applied to him or her"*. Invece, il GDPR impone che le informazioni sulla logica sottostante al trattamento siano fornite preventivamente al lavoratore-interessato, senza bisogno che venga avanzata una specifica richiesta in tal senso.

[154] In ordine al dibattito dottrinale interno sulla rilevanza dell'art. 22 GDPR in tema di trasparenza algoritmica cfr. G. PELUSO, *Obbligo informativo e sistemi integralmente automatizzati*, in *Labour & Law Issues*, vol. 9, n. 2, 2023, p. 111, nota 34: "*sull'inesistenza nel GDPR di un diritto ad avere una spiegazione in relazione al processo decisionale automatizzato, v: G. Gaudio, Algorithmic management, poteri datoriali e oneri della prova: alla ricerca della verità materiale che si cela dietro l'algoritmo, LLI, 2020, 2, 29 ss.; G. Fioriglio, Intelligenza artificiale, privacy e rapporto di lavoro: una prospettiva informatico-giuridica, LDE, 2022, 3, 10. Sottolinea, invece, come «In relazione al funzionamento degli algoritmi, i principi di prevenzione e della trasparenza impongono, a favore dell'interessato, gli obblighi di informazione preventiva e di spiegazione delle operazioni che si avvalgono dell'A.I (c.d. right of explaination: artt. 13 e 15 GDPR)»: P. Tullini, Dati, in M. Novella -P. Tullini (a cura di), Lavoro Digitale, Giappichelli, 2022, 121*".

[155] Nel già citato decreto Foodinho (provv. 10 giugno 2021, n. 234), il Garante per la protezione dei dati personali ha ritenuto violato: (i) l'art. 13, comma 2, lett. f), GDPR "*considerato che la predetta informativa non fa riferimento alla effettuazione di trattamenti automatizzati compresa l'attività di profilazione … preordinati all'assegnazione di un punteggio al rider al dichiarato fine di determinare la priorità nella prenotazione degli slot (fasce orarie determinate dalla società all'interno delle quali sono inviati gli ordini di consegna); sono state pertanto altresì omesse "informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato*"; (ii) l'art. 22, comma 3, GDPR "*in quanto non risulta … che la società abbia provveduto ad attuare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano […], di esprimere la propria opinione e di contestare la decisione … non vi è evidenza alcuna della adozione di misure relative all'esercizio dei diritti attraverso l'attivazione di canali dedicati (chat accessibile attraverso l'applicazione, sportelli dedicati, email) … Né risulta che gli interessati fossero in alcun modo consapevoli della possibilità di esercitare tali diritti nei confronti delle decisioni adottate mediante l'utilizzo della piattaforma*".

introduttiva alla proposta del Parlamento Europeo e del Consiglio relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali, "*sebbene tali diritti siano particolarmente pertinenti per le persone che lavorano mediante piattaforme digitali soggette a gestione algoritmica, recenti procedimenti giudiziari hanno messo in evidenza le limitazioni e le difficoltà che i lavoratori — e in particolare le persone che svolgono un lavoro mediante piattaforme digitali — devono affrontare quando intendono far valere i loro diritti in materia di protezione dei dati nel contesto della gestione algoritmica. Ciò riguarda in particolare la difficoltà di tracciare la linea di demarcazione tra decisioni algoritmiche che incidono o meno sui lavoratori in modo sufficientemente significativo*"[156].

A questo punto, risulta necessario operare una scelta: confermare la disposizione del Codice ILO che preclude le decisioni automatizzate oppure individuare regole volte a tutelare i lavoratori soggetti a processi decisionali automatizzati basati sul trattamento dei dati personali per le ipotesi in cui questi siano ammessi a norma delle disposizioni nazionali, come avviene nel contesto europeo qualora la decisione automatizzata "*sia necessaria per la conclusione o l'esecuzione di un contratto di lavoro*" (art. 22, comma 3, lett. a), GDPR).

Nel caso in cui si optasse per l'introduzione di regole specifiche, si potrebbe spostare il baricentro regolativo dall'informazione sul trattamento dei dati personali in senso stretto alla spiegazione del funzionamento dei sistemi e delle decisioni assunte utilizzando – in tutto o in parte – i dati personali dei lavoratori, prevedendo appositi diritti di informazione *ex ante* e di motivazione *ex post*.

Per quanto riguarda la previsione di dettagliati obblighi informativi preventivi, questi consentirebbero di ridurre l'asimmetria informativa che connota la gestione algoritmica dove i lavoratori risultano sempre più trasparenti, mentre le decisioni datoriali sempre più

Nell'ordinamento olandese, l'art. 22 GDPR è stato applicato dell'Amsterdam District Court, 11 marzo 2021, C/13/689705/HA RK 20-258, per richiedere di spiegare la logica sottostante a una decisione completamente automatizzata adottata nei confronti di una una piattaforma di trasporto via taxi. Per un commento della sentenza si rinvia a R. GELLERT, M. VAN BEKKUM e F. ZUIDERVEEN BORGESIUS, *The Ola & Uber judgments: for the first time a court recognises a GDPR right to an explanation for algorithmic decision-making*, in *EU Law Analysis*, 28 aprile 2021.

[156] COM/2021/762.

opache[157]. In questo modo, i lavoratori sarebbero informati in maniera puntuale sia sull'esistenza dei sistemi decisionali basati, in tutto o in parte, sul trattamento dei loro dati personali sia sulle specifiche modalità di funzionamento degli stessi[158].

A tal proposito, un utile riferimento può essere rappresentato dalla proposta di direttiva del Parlamento Europeo e del Consiglio relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali[159].

L'art. 6 del Capo III, dedicato alla "*Gestione algoritmica*", richiede di fornire una serie di informazioni sui "*sistemi decisionali automatizzati utilizzati per prendere o sostenere decisioni che incidono significativamente sulle condizioni di lavoro … ad esempio per quanto riguarda il loro accesso agli incarichi di lavoro, i loro guadagni, la loro salute e la loro sicurezza sul lavoro, il loro orario di lavoro, la loro promozione e la loro situazione contrattuale, compresa la limitazione, la sospensione o la chiusura del loro account*". Nello specifico, le informazioni da fornire sono: "(i) *il fatto che tali sistemi siano in uso o siano in fase di introduzione*; (ii) *le categorie di decisioni che sono prese o sostenute da tali sistemi;* (iii) *i principali parametri di cui tali sistemi tengono conto e l'importanza relativa ("relative weight") di tali principali parametri nel processo decisionale automatizzato, compreso il modo in cui i dati personali o comportamento del lavoratore ... incidono sulle decisioni; (iv) i motivi alla base della decisione di sospendere o chiudere l'account ... o di non retribuire il lavoro svolto, delle decisioni in merito alla situazione contrattuale ... o di qualsiasi decisione con effetti analoghi*"[160].

---

[157] È vero che il Codice ILO contiene già diritti di informazione individuale e collettiva (artt. 5, par 8; 8, par. 3; art. 6, par. 2; art. 12, par. 2; 16, par. 14), ma questi non paiono essere dotati di un livello di specificità sufficiente a garantire la trasparenza algoritmica.

[158] Tali diritti, pertanto, presuppongono che il processo decisionale si fondi, almeno in parte, sul trattamento di dati personali, intesi come "*any information related to an identified or identifiable worker*" (art. 3, par. 1, Codice ILO).

[159] In merito alla proposta di direttiva si rinvia ai contributi di C. SPINELLI, *La trasparenza delle decisioni algoritmiche nella proposta di Direttiva UE sul lavoro tramite piattaforma*, in *Lavoro Diritti Europa*, 2/2022; G. GAUDIO, *L'algorithmic management e il problema della opacità algoritmica nel diritto oggi vigente e nella Proposta di Direttiva sul miglioramento delle condizioni dei lavoratori tramite piattaforma*, in *Lavoro Diritti Europa*, 1/2022; V. DI CERBO, *Algorithmic management e piattaforme digitali: verso una normativa EU finalizzata a fissare livelli minimi comuni di tutela dei lavoratori*, in *Lavoro Diritti Europa,* 1/2024.

[160] L'art. 6 prevede anche obblighi informativi in merito ai "*sistemi di monitoraggio automatizzati utilizzati per monitorare, supervisionare o valutare l'esecuzione del lavoro ... con mezzi elettronici*". In tal caso, le informazioni da fornire sono: "*il fatto che tali sistemi siano in uso o siano in fase di introduzione"* e *"le categorie di azioni monitorate, supervisionate da parte di tali sistemi, compresa la valutazione da parte del destinatario del servizio*".

Quanto ai destinatari, tali informazioni sono fornite al lavoratore "*al più tardi il primo giorno lavorativo*" sotto forma di documento che può essere in formato elettronico in forma concisa, trasparente, intelligibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Inoltre, le predette informazioni devono essere messe a disposizione anche dei rappresentanti dei lavoratori e delle autorità nazionali del lavoro su loro richiesta.

Un altro possibile riferimento normativo può essere rappresentato dagli obblighi informativi introdotti dall'ordinamento nazionale al fine di "*disvelare i dati che regolano il funzionamento dei sistemi organizzativo-manageriali*"[161] nel tentativo "*di intaccare l'opacità che caratterizza l'esercizio dei poteri datoriali a mezzo degli algoritmi, ossia il c.d. "algorithmic management*"[162]. Si sta facendo riferimento all'art. 4 del c.d. decreto trasparenza (d.lgs. n. 27 giugno 2022, n. 104)[163] che ha modificato il d.lgs. 26 maggio 1997, n. 152, introducendo l'art. 1-*bis* recante "*Ulteriori obblighi informativi nel caso di utilizzo di sistemi decisionali o di monitoraggio automatizzati*". Trattasi di obblighi i quali, a differenza di quelli della proposta di direttiva UE, hanno il pregio di estendersi anche al *management algoritmico* al di fuori delle piattaforme digitali.

Il citato articolo - prima delle modifiche in senso apparentemente restrittivo introdotte dal c.d. decreto lavoro[164] - imponeva al datore di lavoro o al committente pubblico e privato di fornire informazioni sui "*sistemi decisionali o di monitoraggio automatizzati deputati a fornire indicazioni rilevanti ai fini della assunzione o del conferimento dell'incarico, della gestione o della cessazione del rapporto di lavoro, dell'assegnazione di compiti o*

---

[161] G. PELUSO, *op. cit*, p. 111.

[162] *Ibidem*, p. 107.

[163] Per un commento del c.d. decreto trasparenza si rinvia a D. GAROFALO, M. TIRABOSCHI, V. FILÌ, A. TROJSI (a cura di), *Trasparenza e attività di cura nei contratti di lavoro. Commentario ai decreti legislativi n. 104 e n. 105 del 2022*, Adapt University Press, 2022 nonché al contributo di C. TIMELLINI, *Quale reale trasparenza nel rapporto di lavoro con gli ultimi adempimenti?*, in *Variazioni su temi di Diritto del Lavoro*, 2/2023, pp. 571-605.

[164] Sull'impatto delle modifiche introdotte dall'art. 26, d.l. 4 maggio 2023, n. 48, conv. in l. 3 luglio 2023, n. 85 al citato art. 1-*bis*, d.lgs. 26 maggio 1997, n. 152 – che fa ora riferimento ai sistemi "i*ntegralmente*" automatizzati e esclude dall'obbligo informativo i "*sistemi protetti da segreto industriale e commerciale*" – v. E. DAGNINO, *Modifiche agli obblighi informativi nel caso di utilizzo di sistemi decisionali o di monitoraggio automatizzati (art. 26, comma 2, d.l. n. 48/2023)*, in E. DAGNINO, C. GAROFALO, G. PICCO, P. RAUSEI (a cura di), *Commentario al d.l. 4 maggio 2023, n. 48 c.d. "decreto lavoro"*, Adapt University Press, 2023 nonché G.PELUSO, *op.cit*.

mansioni nonché indicazioni incidenti sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori"[165]. Nello specifico, le informazioni da fornire riguardano: gli aspetti del rapporto di lavoro sui quali incide l'utilizzo dei sistemi; gli scopi e le finalità dei sistemi; la logica ed il funzionamento dei

---

[165] La circolare del Ministero del lavoro e delle politiche sociali 20 settembre 2022, n. 19, emanata prima delle modifiche apportate dal c.d. decreto lavoro, ha fornito chiarimenti sul perimetro degli obblighi informativi introdotti dal c.d. decreto trasparenza. In particolare, la circolare distingue tra "*sistemi decisionali o di monitoraggio automatizzati che siano*: *a) finalizzati a realizzare un procedimento decisionale in grado di incidere sul rapporto di lavoro; b) incidenti sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori*". La Circolare, poi, aggiunge che "*con particolare riferimento alla fattispecie sub a) … ad esempio, l'obbligo dell'informativa sussiste nelle seguenti ipotesi: 1. assunzione o conferimento dell'incarico tramite l'utilizzo di chatbots durante il colloquio, la profilazione automatizzata dei candidati, lo screening dei curricula, l'utilizzo di software per il riconoscimento emotivo e test psicoattitudinali, ecc.; 2. gestione o cessazione del rapporto di lavoro con assegnazione o revoca automatizzata di compiti, mansioni o turni, definizione dell'orario di lavoro, analisi di produttività, determinazione della retribuzione, promozioni, etc., attraverso analisi statistiche, strumenti di data analytics o machine learning, rete neurali, deep-learning, ecc.. … Discorso a parte merita, invece, la previsione sub b), riguardante «le indicazioni incidenti sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori». Anche in questa ipotesi il datore di lavoro ha l'obbligo di informare il lavoratore dell'utilizzo di tali sistemi automatizzati, quali – a puro titolo di esempio: tablet, dispositivi digitali e wearables, gps e geolocalizzatori, sistemi per il riconoscimento facciale, sistemi di rating e ranking, etc. Si deve ritenere che l'obbligo informativo introdotto dal citato articolo 1-bis del d.lgs. n. 152/1997 trovi applicazione anche in relazione all'utilizzo di sistemi decisionali o di monitoraggio automatizzati integrati negli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, allorquando presentino le caratteristiche tecniche e le funzioni descritte in precedenza*".
Successivamente, è intervenuto sul tema anche il Parere del Garante per la protezione dei dati personali del 24 gennaio "*Questioni interpretative e applicative in materia di protezione dei dati connesse all'entrata in vigore del d. lgs. 27 giugno 2022, n. 104 in materia di condizioni di lavoro trasparenti e prevedibili (c.d. "Decreto trasparenza")*". L'intervento del Garante si giustifica in quanto "*considerato che l'impiego dei predetti sistemi dà luogo a "trattamenti" di dati personali, riferiti a "interessati", identificati o identificabili (art. 4, par. 1, nn. 1) e 2), del Regolamento) nel contesto lavorativo, emerge, in via preliminare, la necessità che tale disciplina di settore sia coordinata, in sede applicativa, con la normativa in materia di protezione dei dati personali*". Rispetto all'estensione dell'obbligo di informativa delineato dalla circolare ministeriale, il Garante afferma che "*la menzionata circolare del Ministero, nell'esemplificare i casi in cui possono trovare applicazione gli obblighi informativi oggetto del Decreto, fa riferimento a strumenti e tecnologie, quali, ad esempio, "software per il riconoscimento emotivo", "strumenti di data analytics o machine learning, rete neurali, deep-learning", nonché "sistemi per il riconoscimento facciale, sistemi di rating e ranking", che, specie se impiegati nel contesto lavorativo, determinano un elevato livello di rischio per i diritti e le libertà degli interessati oggetto di specifica tutela nell'ambito del sistema di protezione dei dati personali.*
L'impiego di tali sistemi di monitoraggio particolarmente invasivi, pone, anzitutto, un tema di liceità dei trattamenti di dati personali effettuati mediante gli stessi, tenuto conto della disciplina di settore in materia di impiego di strumenti tecnologici nel contesto lavorativo (v. art. 114 del Codice, che rimanda all'art. 4 della L. 300/1970).
Le specificità delle tecnologie di questi sistemi, nonché la natura dei dati trattati (ad esempio, i dati biometrici e quelli relativi alle emozioni del lavoratore) e le funzionalità che spesso ad essi sono associate, sollevano, altresì, dubbi in ordine alla stessa proporzionalità del loro impiego, nonché di compatibilità con i principi generali in materia di protezione dei dati e con il quadro di garanzie in materia di libertà e dignità del lavoratore, potendosi, peraltro, porsi in contrasto con le disposizioni nazionali che vietano al datore di lavoro di trattare informazioni attinenti alla sfera privata del lavoratore (v. art. 113 del Codice, che rimanda all'art. 8 della L. 300/1970)".

sistemi; le categorie di dati e i parametri principali utilizzati per programmare o addestrare i sistemi, inclusi i meccanismi di valutazione delle prestazioni; le misure di controllo adottate per le decisioni automatizzate, gli eventuali processi di correzione e il responsabile del sistema di gestione della qualità; il livello di accuratezza, robustezza e cybersicurezza dei sistemi e le metriche utilizzate per misurare tali parametri nonché gli impatti potenzialmente discriminatori delle metriche stesse.

Tali informazioni devono essere fornite in modo trasparente in formato strutturato di uso comune e leggibile da dispositivo automatico sia ai lavoratori sia alle RSA ovvero alla RSU o, in assenza delle predette rappresentanze, alle sedi territoriali delle associazioni sindacali comparativamente più rappresentative sul piano nazionale[166]. Invece, il Ministero del lavoro e l'Ispettorato nazionale del lavoro possono richiedere la comunicazione delle medesime informazioni e dati nonché l'accesso agli stessi.

Una questione da porsi riguarda la precisa estensione del diritto di informazione. Sotto tale profilo, pare ragionevole prevedere stringenti obblighi informativi anche nel caso di decisioni "semi automatizzate" nelle quali l'intervento umano rivesta un ruolo meramente eventuale, marginale o accessorio. Si prenda l'esempio di una piattaforma digitale strutturata in modo tale da non procedere alla chiusura automatica dell'*account* dei prestatori, richiedendo che personale aziendale debba prima controllare la correttezza della segnalazione effettuata dall'algoritmo. In questo caso, la decisione non sarebbe completamente automatizzata, ma sembra irragionevole che, per ciò solo, i lavoratori non vengano preventivamente informati dei parametri che conducono alla disattivazione dell'*account*.

Si potrebbe anche valutare se prevedere un diritto di informazione individuale e collettivo formulato in senso ampio anche qualora gli *output* algoritmici costituiscano effettivamente dei meri suggerimenti per i decisori umani. Da un lato, porre tali obblighi informativi potrebbe risultare eccessivo. Dall'altro, qualora, ad esempio, un'azienda ricorresse a un sistema di valutazione del personale per individuare quali siano i lavoratori

[166] Nell'applicazione pratica, la violazione dell'obbligo di informazione collettiva da parte di piattaforme di *food delivery* ha condotto il Tribunale di Palermo all'emanazione dei decreti di condotta antisindacale *ex* art. 28 Stat. Lav. del 4 aprile 2023 e del 20 giugno 2023, quest'ultimo adottato successivamente alle modifiche normative apportate dal c.d. decreto lavoro.
Per un commento dei predetti decreti v. G. A. RECCHIA, *Condizioni di lavoro trasparenti, prevedibili e giustiziabili: quando il diritto di informazione sui sistemi automatizzati diventa uno strumento di tutela collettiva*, in *Labour Law & Issues*, 1, 2023.

migliori ai fini di una promozione, ma la decisione finale fosse effettivamente assunta dal *manager* sulla base anche di aspetti non tenuti in considerazione dal sistema quali la *leadership* o la benevolenza dei colleghi, i lavoratori potrebbero rimanere non adeguatamente informati su quali siano i parametri in base ai quali le loro prestazioni sono valutate (es. il numero di clienti contattati, le vendite concluse, le recensioni dei clienti).

Tuttavia, in dottrina è stato prospettato che la previsione di un diritto di informazione e consultazione sindacale potrebbe non essere sufficiente, essendo, invece, preferibile introdurre un obbligo di "negoziazione collettiva dell'algoritmo"[167]. Ciò consentirebbe al sindacato di codeterminare le modalità con cui vengono trattati i dati personali dei lavoratori, ricercando soluzioni dirette a minimizzare le informazioni raccolte, garantirne la cancellazione dopo un periodo temporale limitato e assicurarsi che non possano essere utilizzate impropriamente.

Ma "la negoziazione dell'algoritmo" avrebbe implicazioni che trascendono l'ambito della *data protection*. Infatti, in questo modo, il sindacato avrebbe la possibilità di "*correggere alcuni profili ("feature") dell'algoritmo con cui l'imprenditore organizza – in tutto od in parte – la propria produzione*"[168]. Così, le parti sociali potrebbero controllare che gli algoritmi che assegnano il lavoro non mettano eccessivamente sotto pressione i prestatori,

---

[167] V. DE STEFANO, "*Negotiating the algorithm": Automation, artificial intelligence and labour protection*, ILO, Employment Policy Department, Working Paper No. 246, 2018. Secondo l'Autore, "*collective bargaining can play a primary role both at the sectoral and at the workplace level. Collective agreements could address the use of digital technology, data collection and algorithms that direct and discipline the workforce, ensuring transparency, social sustainability and compliance with these practices with regulation. Collective negotiation would also prove pivotal in implementing the "human-in-command" approach at the workplace … All this would also be consistent with collective bargaining's fundamental function as an enabling right and as a rationalisation mechanism for the exercise of employers' managerial prerogatives, allowing moving away from a purely unilateral dimension of work governance. "Negotiating the algorithm" could, therefore, become a crucial objective of social dialogue and action for employers' and workers' organization*" (pp. 23 e 24).
Secondo S. BAIOCCO, E. FERNANDEZ-MACÍAS, U. RANI, A. PESOLE, *op. cit.*, p. 26, "*co-determination in the definition of the use of algorithms at work can help rebalancing the negotiating power between workers and employers by preventing abuse of contractual disparities and shield workers from unfair employment terms imposed by a party with a significantly stronger bargaining position*".
Nel contesto nazionale, v., tra gli altri, A. PIZZOFERRATO, *Tecnologie digitali, poteri datoriali e diritti dei lavoratori*, in A. BELLAVISTA e R. SANTUCCI, *op. cit.*, p. 240, il quale afferma che "*al fine di tutelare appieno i diritti e gli interessi dei lavoratori, non sembra sufficiente cercare di mitigare* ex post *gli effetti negativi derivanti dall'impiego di algoritmi e forme di intelligenza artificiale, essendo al contrario indispensabile negoziare* ex ante *l'algoritmo stesso. In altre parole, si rende indispensabile definire in maniera condivisa le finalità, la logica e i parametri di funzionamento dei sistemi".*

[168] F. MARASCO, *Nuove forme di contrattazione sindacale nelle relazioni industriali su piattaforma*, in *Labour & Law Issues*, vol. 5, n. 2, 2019.

accrescendo i rischi per la loro salute e sicurezza, richiedendo, ad esempio, di garantire un "margine di tolleranza" crescente per il completamento delle attività all'aumentare dell'orario di lavoro. Infatti, l'algoritmo dovrebbe tenere conto che, con il trascorrere del tempo, diminuiscono le energie psico-fisiche e la concentrazione dei lavoratori e, di conseguenza, dovrebbe aumentare il tempo stimato per portare a termine le attività. Il sindacato, ancora, potrebbe pretendere che l'algoritmo sia adattato per far fronte alle necessità di lavoratori con esigenze particolari, quali lavoratori parzialmente idonei al lavoro o affetti da disabilità, con un approccio preventivo che tenga in considerazione tali esigenze fin dal momento della progettazione. Infatti, modificare successivamente l'algoritmo potrebbe essere tecnologicamente difficile o eccessivamente oneroso, il che potrebbe determinare l'inutilizzabilità delle prestazioni di quei lavoratori. Tuttavia, per una efficiente negoziazione collettiva dell'algoritmo, occorre che il sindacato accresca le proprie competenze tecnologiche e/o faccia ricorso a "*figure dotate delle competenze indispensabili per negoziare l'algoritmo*"[169].

Passando al secondo profilo, il diritto di spiegazione/motivazione *ex post* della decisione adottata avrebbe la funzione di permettere al lavoratore di conoscere le ragioni poste alla base della decisione. Ciò consentirebbe al prestatore di verificare la legittimità e la correttezza della determinazione datoriale e, nel caso, contestarla in giudizio. Infatti, il rischio è che il procedimento decisionale algoritmico si concluda senza che il lavoratore sia reso edotto delle motivazioni che giustificano la determinazione datoriale. L'assenza di motivazione pregiudica le possibilità di difesa del lavoratore sotto almeno due profili: da una parte, questi non può valutare compiutamente la legittimità o meno della decisione e, quindi, l'opportunità di opporsi alla decisione; dall'altra, qualora decida comunque di contestare la decisione "al buio", avrebbe significative difficoltà nell'articolare la propria linea difensiva.

Ai fini della formulazione di tale diritto, ancora una volta un utile punto di riferimento può essere rappresentato dalla proposta di direttiva europea sul lavoro tramite piattaforma. Questa, infatti, contiene disposizioni volte a garantire che il lavoratore possa ottenere una motivazione scritta e/o una risposta motivata sulla logica sottostante alle

[169] A. PIZZOFERRATO, *Tecnologie digitali, poteri datoriali e diritti dei lavoratori*, *op. cit.*, p. 240.

decisioni che impattano significativamente sulle proprie condizioni lavorative[170].

In particolare, l'art. 8 "*Riesame umano di decisioni significative*" richiede di fornire al lavoratore "*una motivazione scritta per qualsiasi decisione presa o sostenuta da un sistema decisionale automatizzato di limitare, sospendere o chiudere l'account del lavoratore …, qualsiasi decisione di non retribuire il lavoro svolto …, qualsiasi decisione in merito alla situazione contrattuale del lavoratore … o qualsiasi decisione con effetti analoghi*".

Inoltre, al prestatore è riconosciuto "*il diritto di ottenere una spiegazione … per qualsiasi decisione presa o sostenuta da un sistema decisionale automatizzato che incida significativamente sulle condizioni di lavoro*" da parte di "*una persona di contatto designata … per discutere e chiarire i fatti, le circostanze e i motivi di tale decisione*".

Se, poi, i lavoratori "*non sono soddisfatti della spiegazione o della motivazione scritta ottenuta o ritengono che la decisione … violi i loro diritti*, *hanno il diritto di chiedere … di riesaminare tale decisione*" e, in tal caso, deve essere fornita al lavoratore "*una risposta motivata senza indebito ritardo*" entro una settimana dal ricevimento della richiesta, prorogabile a due settimane.

Tali diritti, formulati in favore dei *platform workers*, potrebbero essere agevolmente adattati anche ai lavoratori soggetti a *management* algoritmico nei settori lavorativi tradizionali[171].

Ci si rende conto che è discutibile la collocazione sistematica all'interno del Codice ILO delle disposizioni volte a rafforzare la trasparenza e l'intelligibilità dei sistemi e delle decisioni assunte nel contesto dell'*algorithm management*. Infatti, tali previsioni potrebbero essere introdotte all'interno dello strumento normativo sul lavoro tramite

---

[170] Il che, peraltro, sembra presupporre che il datore di lavoro debba essere sempre in grado di spiegare il funzionamento dei sistemi decisionali utilizzati.

[171] A tal proposito, si segnala la Proposta di Risoluzione legislativa del Parlamento Europeo del 3 maggio 2022 (*Draft European Parliament Legislative Resolution* (PR–PE731.497v01-00), la quale ha proposto di estendere i diritti relativi alla gestione algoritmica a tutti i datori di lavoro, anche al di fuori dell'ambito delle piattaforme digitali, come si evince già dalla prospettazione di modifica dello stesso titolo della proposta di direttiva in "*Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on improving working conditions in platform work and work subject to automated or semi-automated monitoring and decision-making systems*".
Sul punto, v. A. PIZZOFERRATO, *Automated decision-making in HRM*, in *LG*, n. 11/2022 e A. ALAIMO, *Il pacchetto di misure sul lavoro nelle piattaforme: dalla proposta di Direttiva al progetto di Risoluzione del Parlamento europeo. Verso un incremento delle tutele*?, in *Labour & Law Issues*, vol. 8, n. 1, 2022.

piattaforma che sarà oggetto di discussione nell'ambito della Conferenza Internazionale del Lavoro del 2025.

Tuttavia, alcune considerazioni fanno propendere per valutare l'opportunità di collocare disposizioni sulla trasparenza algoritmica all'interno del Codice ILO. Infatti, l'adozione dello strumento normativo sul lavoro tramite piattaforma non è certo come dimostra il sostanziale fallimento del *meeting of experts on decent work in the platform economy* che non è riuscito a esprimere una posizione comune a causa dell'opposizione della componente datoriale.

Inoltre, disposizioni sulla trasparenza algoritmica potrebbero essere introdotte anche all'interno dell'eventuale *standard* sul lavoro tramite piattaforma visto che il Codice ILO "*does not replace national laws, regulations, international labour standards or other accepted standards labour standars*" (sez. 2 del codice). In tal caso, sarebbe evidentemente opportuna un'operazione di coordinamento normativo.

Le disposizioni del Codice ILO, poi, avrebbero una copertura soggettiva più ampia, applicandosi anche ai lavoratori soggetti a *management* algoritmico occupati in settori diversi rispetto al lavoro tramite piattaforma.

Infine, come visto, disposizioni simili - seppur con un minore grado di specificazione - si rinvengono anche in strumenti di *data protection* sia settoriali come la Raccomandazione CM/Rec(2015)5 sul trattamento di dati personali nel contesto occupazionale sia generali come il Regolamento UE 2016/679.

17.2. Code of practice on the protection of workers' personal data: monitoraggio dei lavoratori

Come visto nella sezione n. 1.4, il Codice di condotta consente il monitoraggio dei lavoratori[172]. Il monitoraggio è però soggetto ad alcune restrizioni. In primo luogo, i datori di lavoro non sono liberi di scegliere le modalità di controllo che ritengono più adeguate ai loro obiettivi, ma sono tenuti a minimizzare le conseguenze per la privacy dei lavoratori dando preferenza ai mezzi di sorveglianza meno invasivi (art. 16, par. 14, n. 1). In secondo luogo, il Codice prevede garanzie individuali e collettive. Infatti, i lavoratori devono essere informati in anticipo, prima che il monitoraggio venga attivato, "*of the reasons for*

[172] Lo stesso Commentario al Codice di condotta conferma che "*the code does not exclude the monitoring of worker*".

monitoring, the time schedule, the methods and techniques used and the data to be collected", mentre le rappresentanze sindacali devono essere non solo informate, ma anche consultate "*before the introduction of any electronic monitoring of workers' behaviour in the workplace*".

A differenza del Codice ILO, altri strumenti regolativi adottano soluzioni più tutelanti per il lavoratore che potrebbero essere oggetto di considerazione.

La Raccomandazione CM/Rec(2015)5, al par. 15 "*Sistemi informativi e tecnologie per la sorveglianza dei dipendenti, compresa la videosorveglianza*" vieta il c.d. controllo fine a sé stesso, stabilendo che non dovrebbe essere consentito introdurre e utilizzare sistemi informativi e tecnologie aventi come scopo diretto e primario la sorveglianza dell'attività e del comportamento dei dipendenti. Invece, è ammessa l'introduzione e l'utilizzo di sistemi tecnologici che comportino solo indirettamente la possibilità di sorveglianza qualora ricorrano scopi legittimi - diversi dalla mera finalità di controllo - quali la tutela dell'attività produttiva, della salute e della sicurezza, o l'efficace gestione dell'azienda o dell'ente[173].

Inoltre, la Raccomandazione CM/Rec(2015)5 rafforza la posizione dei rappresentanti dei lavoratori rispetto al Codice ILO, il quale, comunque, valorizza la dimensione collettiva, a differenza di altri strumenti di *data protection* come il GDPR che "*non contempla importanti aspetti collettivi intrinseci al diritto del lavoro, compresi quelli relativi al ruolo dei rappresentanti dei lavoratori"*[174]. Mentre il Codice ILO prevede un diritto collettivo di informazione e consultazione, la Raccomandazione richiede il raggiungimento di un accordo con le rappresentanze dei lavoratori qualora dalla consultazione avviata prima dell'introduzione o della modifica dei sistemi di sorveglianza

[173] Similmente, l'art. 4 St. Lav. – anche a seguito della riscrittura ad opera dall'art. 23, comma 1, d.lgs. 14 settembre 2015, n. 15 – inibisce l'installazione di sistemi finalizzati al controllo a distanza dei lavoratori, prevedendo che "*gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale*".

[174] Questo è quanto affermato nella Relazione preliminare alla proposta di direttiva relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali. In dottrina, A. INGRAO, *La protezione dei dati personali dei lavoratori*, in A. BELLAVISTA e R. SANTUCCI, *op. cit.*, parla della mancata considerazione della dimensione collettiva come "peccato originale" della normativa privacy.

emerga che sussiste il rischio di violare il diritto del dipendente al rispetto della vita privata e della dignità umana[175].

Ancora più incisivamente, nell'ordinamento italiano la trattativa con le parti collettive non è meramente eventuale, ma costituisce "una tappa obbligata". Infatti, come noto, ai sensi dell'art. 4 St. Lav. l'introduzione di impianti audiovisivi e altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori – diversi da quelli utilizzati dal lavoratore per rendere la prestazione lavorativa e dagli strumenti di registrazione degli accessi e delle presenze – richiede il previo accordo sindacale oppure, in mancanza, l'autorizzazione amministrativa dell'Ispettorato del lavoro[176].

Inoltre, potrebbe valutarsi l'introduzione all'interno del Codice ILO di una sezione contenente indicazioni più specifiche sulle modalità di controllo più diffuse nel contesto lavorativo come, a titolo di esempio, l'utilizzo della videosorveglianza, il controllo delle comunicazioni elettroniche e dei *social network*, l'impiego di sistemi di geolocalizzazione.

È vero che l'introduzione di tale sezione non risulta necessaria, essendo comunque possibile ricavare i limiti di tali forme di controllo in via interpretativa dalle regole del Codice ILO. Del resto, sotto l'egida del GDPR, l'*European Data Protection Board* (EDPB)[177] e i Garanti nazionali per la protezione dei dati personali[178] hanno fornito indicazioni operative sui limiti delle pratiche di controllo dei lavoratori, ricavandole dai principi fondamentali del Regolamento, il quale, peraltro, non contiene uno "statuto speciale" dedicato alla tutela della privacy nel contesto lavorativo.

---

[175] Nello specifico, l'art. 21 della Raccomandazione richiede di "*consultare i rappresentanti dei dipendenti conformemente al diritto o alle prassi nazionali prima di introdurre sistemi di sorveglianza ovvero qualora si prevedano modifiche a tali forme di sorveglianza. Se la procedura di consultazione indica che sussiste il rischio di violare il diritto del dipendente al rispetto della vita privata e della dignità umana, si dovrebbe ottenere il concerto dei rappresentanti dei dipendenti*".

[176] Sull'art. 4 St. Lav. v. *ex multis*, P. TULLINI (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli, 2017; R. DEL PUNTA, *La nuova disciplina dei controlli a distanza sul lavoro (art. 23, d.lgs. n. 151/2015)*, in *RIDL*, 1/2016, p. 77 ss. e A. MARESCA, *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 dello Statuto dei lavoratori*, in *RIDL*, 1/2016, I, 513 ss.

[177] Cfr. *Working document on the surveillance of electronic communications in the workplace*, 29 maggio 2002, *opinion n. 8/2001 on the processing of personal data in the employment context*; *opinion n. 2/2017 on data processing at work*, commentati da A. SARTORI, *op. cit.*, pp. 58 ss.

[178] Per l'esame dei principali provvedimenti emessi dal Garante per la protezione dei dati personali in materia di lavoro v. F. BRAVO (a cura di), *DATI PERSONALI. Protezione, libera circolazione e governance* - Vol. 1. *Principi*, Pacini Giuridica, 2023, p. 306 ss.; v. anche Agencia Española de Protección de Datos (AEPD), *Protección de datos y relaciones laborales*, maggio 2021.

Tuttavia, l'introduzione della predetta sezione potrebbe accrescere l'utilità del *Code of practice* come punto di riferimento "*in the develpement of legislation, regulations, collective agreements, work rules, policies and practical measures at enterprise level*".

18. Considerazioni sulle fonti dell'ILO in materia di tutela della riservatezza e possibili sviluppi

All'interno delle fonti dell'ILO non pare ravvisarsi l'esistenza di *international labour standards* di applicazione generale che regolamentino in modo completo la tematica della tutela della riservatezza del lavoratore.

Infatti, il Codice di condotta contiene una disciplina organica della materia, ma, per quanto rilevante, costituisce una fonte di *soft law* priva dello *status* di *international labour standard*.

Come visto *supra*, sono presenti diverse disposizioni sulla privacy in ambito lavorativo anche nelle Convenzioni e Raccomandazione dell'ILO. Tuttavia, si tratta di previsioni settoriali dalle quali è possibile ricavare una regolamentazione sulla tutela della privacy che interessi la generalità dei lavoratori. Infatti, si tratta di disposizioni settoriali che riguardano contesti definiti (agenzie per l'impiego private; segnalazioni agli organi ispettivi; violenze e molestie sul lavoro). Solamente per quanto concerne il trattamento dei dati sanitari – che, comunque, rappresentano solamente una delle tipologie di dati personali – sembra possibile affermarsi l'esistenza di regole, contenute per lo più in Raccomandazioni, aventi un ambito di applicazione soggettivo generalizzato e dalle quali sembra possibile enucleare principi comuni che governano la materia.

Quanto ai possibili sviluppi futuri delle fonti in materia di privacy, l'Organizzazione Internazionale del Lavoro ha individuato come priorità la protezione della riservatezza dei lavoratori tramite piattaforma nel contesto del *management* algoritmico, considerato che tali lavoratori sovente non sono adeguatamente informati su come avviene il trattamento dei propri dati personali e sulle logiche di funzionamento dei sistemi che utilizzano – in tutto o in parte – tali dati per l'adozione di decisioni che impattano sulle opportunità lavorative e sul reddito dei *platform workers*.

Il tentativo dell'ILO di introdurre una regolamentazione a livello internazionale del lavoro tramite piattaforma costituisce una iniziativa di primario interesse in ragione delle

numerose tematiche coinvolte ulteriori rispetto alla tutela della privacy e del carattere transnazionale delle piattaforme[179].

Tuttavia, sotto il profilo delle fonti dell'ILO sulla tutela della riservatezza, si assisterebbe all'introduzione di una ulteriore disciplina della privacy avente carattere settoriale in quanto le regole (eventualmente) approvate riguarderebbero solo i *platform workers*, andando ad escludere tutti gli altri lavoratori, compresi quelli soggetti a gestione algoritmica nei settori tradizionali.

Nemmeno l'eventuale aggiornamento delle regole generali del Codice di condotta – per quanto giudicato opportuno – colmerebbe il *gap* normativo che si ravvisa all'interno delle fonti primarie dell'ILO.

Per porre rimedio a questa situazione di frammentarietà regolativa, si potrebbe valutare di includere nell'oggetto della riunione tripartita degli esperti *on the protection of personal data in the digital era* la richiesta di fornire indicazioni agli organi dell'ILO in merito alla possibile adozione di una convenzione internazionale vincolante in materia di privacy nel contesto occupazionale.

La scelta di intraprendere un *iter* legislativo che miri all'adozione di una Convenzione internazionale richiede quantomeno lo svolgimento di due ordini di valutazioni. La prima concerne la rilevanza globale della materia, mentre la seconda ha per oggetto le *chances* che il procedimento legislativo conduca all'approvazione di un testo contenente un livello di protezione adeguato e suscettibile di essere ratificato da parte degli Stati contraenti.

Tali valutazioni presentano implicazioni di carattere assiologico in quanto, qualora fosse intrapreso il predetto *iter* di *standard setting*, verrebbe occupato "uno spazio" che potrebbe essere dedicato ad affrontare una differente tematica.

Quanto alla prima questione, si ritiene che la protezione della privacy dei lavoratori rappresenti una tematica di rilevanza globale che può accrescere la qualità del lavoro e salvaguardare la dignità delle persone che lavorano. Pertanto, al quesito circa l'opportunità di adottare uno strumento vincolante che ponga *standards* internazionali in materia pare potersi fornire una risposta affermativa.

[179] In prossimità della riunione tripartita degli esperti o*n decent work in the platform economy*, il 7 ottobre 2022 è stato elaborato da studiosi provenienti da differenti nazionalità e istituzioni "*A Global Manifesto for Fairer Platform Work*" per sollecitare "*the ILO to adopt a Convention on platform work*".

Rispondere alla seconda questione non è agevole in quanto la realizzabilità della proposta e la qualità dei suoi contenuti dipende anche dalla "volontà politica" delle diverse componenti dell'ILO.

Tuttavia, ci sono elementi che sembrano deporre in favore in merito alla possibilità di introdurre regole internazionali condivise sulla privacy in ambito lavorativo.

Uno studio del 2020 condotto dalla *Global Privacy Assembly* (GPA) - che riunisce autorità per la protezione dei dati personali e della privacy provenienti da tutto il mondo - ha analizzato in chiave comparatistica alcuni tra i principali strumenti di protezione dei dati personali internazionali e regionali per verificare la presenza di principi condivisi e elementi comuni a livello globale[180]. Il rapporto ha ravvisato l'esistenza di rilevanti convergenze tra le fonti globali per quanto riguarda i principi fondamentali di trattamento dei dati personali (equità/correttezza; legalità/liceità; specificazione delle finalità; proporzionalità; qualità dei dati; trasparenza; sicurezza; limitazione del periodo di conservazione; accountability/responsabilità), i diritti riconosciuti all'interessato (accesso; rettifica; cancellazione e, in misura minore, opposizione), l'esistenza di requisiti specifici per il trattamento dei dati personali sensibili, il ruolo delle autorità di sorveglianza e i trasferimenti transfrontalieri di dati[181]. L'esistenza di una convergenza

[180] Il rapporto della *Global Privacy Assembly* (GPA), *Policy Strategy Working Group 1: Global frameworks and standards*, ottobre 2020, ha confrontato dieci fonti internazionali o proprie di specifiche aree geografiche rappresentative delle diverse "regioni" del mondo: *Madrid Resolution*; *OECD Privacy Guidelines*; *APEC Privacy Framework*; *Convention 108*; *Convention 108+*; *Standards for Personal Data Protection for Ibero-American States*; *African Union Convention on Cyber Security and Personal Data Protection*; *ECOWAS Act on Personal Data Protection*; *EU General Data Protection Regulation*; *UN Guidelines for the Regulation of Computerized Personal Data Files*.

[181] Il rapporto rileva che "*while the nature and scope of the frameworks differed to varying degrees, headline results showed that there were very strong commonalities between the frameworks, particularly around a significant number of core principles and data subject rights, and other requirements such as the role of independent supervisory authorities*" (p. 3).

Più nello specifico, i principi fondamentali che compaiono in tutte o nella maggior parte delle fonti esaminate sono: (i) "*fairness - all frameworks set out that personal data should be processed fairly, although few definitions as to what is meant by 'fairness' are offered. Links are made with nondiscrimination, transparency, as well as the avoidance of deceit or fraud*; (ii) *Lawfulness – nearly all frameworks set out that personal data should be processed lawfully. Only some, however, go on to specify legitimate bases or conditions for processing to be considered lawful or legitimate*; (iii) *Purpose specification – all frameworks include some variation of the requirement that personal data should be processed only for specified, defined, explicit and legitimate purposes*; (iv) *Proportionality – this principle is included in all frameworks, although to varying degrees, from specific data minimisation requirements, some general requirements of proportionality, specific requirements of non-excessive processing of personal data through to broader requirements of relevance to purpose*; (v) *Data quality – requirements to keep personal data accurate, complete and up to date appear consistent across frameworks*; (vi) *Openness/transparency – the inclusion of some degree of openness or transparency can be found in all frameworks. Degrees range from general requirements to have transparent policies, and to ensure*

globale tra i principi e le regole generali in materia di protezione dei dati personali può costituire un rilevante punto di partenza ai fini del loro adattamento rispetto alle specificità proprie del contesto lavorativo[182].

information about personal data processing is made available, to specific lists of information that must be provided directly to data subjects; (vii) *Security – this is another consistently used principle, with all frameworks setting out requirements for appropriate (or sufficient) measures to be in place*; (viii) *Data retention – almost all frameworks require data to be retained only for as long as is necessary for the purposes of processing. Some frameworks make special provision for data processed for archiving or research purposes to be retained for longer periods*; (iv) *Accountability – the inclusion of accountability as a general principle is slightly less generally seen, with six out of the ten frameworks requiring that data controllers (and where applicable, processors) are accountable for the personal data they process and, crucially, in most of them, that they are able to demonstrate or prove compliance*" (pp. 7-8)
Quanto ai diritti dell'interessato, tutti o la maggioranza degli strumenti considerati riconoscono le seguenti prerogative: (i) *Access – the right of access is universally acknowledged across all frameworks, linked in some cases to allowing the data subject to evaluate and contest the processing if necessary*; (ii) *Objection/opposition appears in six out of the ten frameworks*; (iii) *Rectification is a point of similarity across all frameworks, often linked to, and following on from, the right of access, when data is found to be inaccurate*; (iv) *Deletion/erasure is another universally accepted right, albeit with differences in scope. Some frameworks link this right to inaccurate or out of date data; however others allow the data subject to request deletion for a broader set of reasons*" (p. 8).
Inoltre, la ricerca rileva come "*almost all frameworks set out specific requirements for sensitive personal data, bearing in mind the increased risks posed by its processing … require or recommend the establishment of a supervisory or privacy enforcement authority … all frameworks except the African Union Convention include general principles on cross-border transfers. The general approach in these principles is that transfers can take place if appropriate levels of protection are in place*" (pp. 9-10).

[182] F. HENDRICKX, *Protection of workers' personal data: General principles*, ILO Working Paper 62, Ginevra, maggio 2022 ha rielaborato i punti di convergenza globali individuati dalla *Global Privacy Assembly* (GPA), declinandoli nel contesto lavorativo utilizzando come riferimento il Codice ILO, la Raccomandazione del Consiglio d'Europa, il GDPR e alcune normative nazionali. Tuttavia, l'oggetto dello studio non ricomprende *"more specific or complementary principles related to electronic or digital monitoring and surveillance, or specific rules in relation to health data*".

Conclusioni

Nella prima parte dell'elaborato si è proceduto alla ricognizione e all'esame delle fonti dell'Organizzazione Internazionale del Lavoro in materia di tutela della riservatezza dei lavoratori.

Preliminarmente, si è proceduto all'analisi del *Code of practice on the protection of workers' personal data* del 1997, fonte di *soft law* priva dello *status* di *international labour standard* che contiene una regolamentazione organica della materia. In particolare, sono state oggetto di approfondimento la tecnica redazionale utilizzata e i principali contenuti del Codice ILO.

In merito alle scelte tecnico-redazionali, si è dato atto che il Codice ILO recepisce terminologia e principi propri delle normative di *data protection* allora vigenti, adeguandoli alle specificità proprie del contesto lavorativo (rapporto di durata che richiede il trattamento di dati personali per una molteplicità di ragioni fin dalla fase preassuntiva; conflitto tra potere datoriale di controllo e istanze di riservatezza dei lavoratori; situazione di debolezza strutturale del candidato/lavoratore rispetto al soggetto che tratta i suoi dati personali). Inoltre, si è ravvisato come il Codice utilizzi definizioni ampie e clausole generali piuttosto che ricorrere a definizioni puntuali, così da favorirne l'adattamento dei contenuti rispetto all'evoluzione tecnologica.

Quanto ai contenuti, il Codice ILO è stato esaminato anche in chiave attualizzatrice, riscontrando come alcune previsioni potrebbero risultare rilevanti per la regolamentazione di fenomeni di più recente sviluppo e diffusione quali l'*algorithmic management*, le discriminazioni algoritmiche e la *customer satisfaction*.

Di seguito, si è proceduto all'esame delle disposizioni dirette a tutelare la riservatezza del lavoratore rilevate all'interno delle Convenzioni e delle Raccomandazioni adottate dall'ILO anche allo scopo di verificare se sia possibile ricavare dalle previsioni contenute nelle "fonti primarie" una regolamentazione completa e l'esistenza di principi generali inerenti alla tutela della riservatezza del lavoratore.

Si è, quindi, proceduto all'analisi e alla contestualizzazione delle disposizioni rilevanti aventi ad oggetto: (i) i trattamenti di dati personali effettuati nell'ambito delle agenzie per l'impiego privato; (ii) la tutela dei dati sanitari dei lavoratori, con un *focus* sulle

informazioni inerenti allo stato di sieropositività; (iii) la protezione dell'identità personale di coloro che segnalano irregolarità agli organi ispettivi del lavoro; (iv) la protezione della vita privata e della riservatezza dei soggetti coinvolti in situazioni di violenza e molestie nel mondo del lavoro.

All'esito dell'attività di ricognizione e analisi svolta, si è stabilito che le Convenzioni e le Raccomandazioni dell'ILO non sembrano regolamentare in maniera completa la materia, risultando tutelate solamente specifiche categorie di lavoratori o la generalità dei lavoratori, ma esclusivamente rispetto a determinate tipologie di dati personali (dati sanitari). Inoltre, stante il carattere settoriale delle disposizioni rinvenute, non pare nemmeno possibile enucleare principi di carattere generale relativi alla tutela della riservatezza dei prestatori, salvo che nell'ambito del trattamento degli *health data* dei lavoratori (cfr. par. 2.2.3).

Di seguito, si è dato conto delle iniziative attivate dall'Organizzazione Internazionale del Lavoro dirette a rafforzare la protezione della riservatezza dei lavoratori per dare attuazione alle indicazioni programmatiche della *Centenary Declaration for the Future of Work* del 2019, la quale ha sollecitato l'adozione di "*policies and measures that ensure appropriate privacy and personal data protection, and respond to challenges and opportunities in the world of work relating to the digital transformation of work, including platform work*". Nello specifico, l'ILO ha attivato un procedimento legislativo che mira all'approvazione di un *international labour standard on decent work in the platform economy* che dovrebbe contenere anche previsioni dirette a garantire la protezione della privacy dei *platform workers* e la trasparenza dei trattamenti di dati personali effettuati nel contesto della gestione algoritmica del lavoro. Inoltre, a circa trent'anni dall'adozione del *Code of practice on the protection of workers' personal data*, è in fase di organizzazione un *meeting* tripartito di esperti sulla protezione dei dati personali dei lavoratori nell'era digitale. Sebbene l'oggetto della riunione non sia ancora stato fissato definitivamente, è stata paventata la possibilità che l'ordine del giorno possa includere la verifica della perdurante rilevanza del *Code of practice on the protection of workers' personal data* e, ove ritenuto necessario, l'aggiornamento dello stesso.

In considerazione dei possibili sviluppi delle iniziative di cui *supra*, si è fornita una panoramica generale delle sfide poste dall'*algorithm management of work* e dall'evoluzione tecnologica rispetto all'utilizzo dei dati personali dei lavoratori a fini

decisori e/o di monitoraggio della prestazione. Si è rilevato come il rispetto dei diritti alla privacy e alla protezione dei dati personali sia messo sempre più in discussione dall'evoluzione tecnologica e dalla gestione algoritmica del lavoro per il crescente numero di informazioni sulla persona-lavoratore presenti sul *web* e sui *social media*; l'ingresso nelle organizzazioni aziendali di sistemi di raccolta di *feedback* sui lavoratori; la diffusione di strumenti e sistemi - talora di difficile individuazione - capaci di raccogliere in modo continuativo dati personali del lavoratore e del telelavoratore, anche altamente sensibili; la diffusione di nuove modalità di utilizzo dei dati personali come per la "lettura della sfera interiore" del lavoratore allo scopo di misurarne, ad esempio, lo stato emotivo e la resistenza allo *stress*; la velocità di sviluppo e la crescente complessità delle tecnologie utilizzate per il trattamento dei dati personali che pongono sempre maggiori difficoltà di comprensione del loro funzionamento e richiedono il possesso di competenze tecnologiche sempre più sviluppate; l'accresciuta potenzialità di utilizzo, anche non intenzionale, delle informazioni raccolte sul lavoratore - sempre più numerose, dettagliate e sensibili - per finalità discriminatorie o comunque improprie; la mancanza di trasparenza circa le logiche di funzionamento dei sistemi decisionali che si basano, in tutto o in parte, sul trattamento dei dati personali dei lavoratori.

Si è anche evidenziato come un adeguato livello di protezione della vita privata e dei dati personali del lavoratore possa rafforzare l'effettività dei divieti di discriminazione e del diritto alla salute e sicurezza sul lavoro.

Alla luce dello scenario delineato e delle più recenti iniziative dell'ILO, si sono formulate alcune possibili proposte di modifica e/o rafforzamento del *Code of practice on the protection of workers' personal data*. Tali proposte consistono, tra l'altro, nell'estensione dei soggetti considerati anche agli sviluppatori dei sistemi utilizzati dal datore di lavoro per il trattamento dei dati personali dei prestatori; nel rafforzamento della trasparenza e della spiegabilità delle "decisioni algoritmiche" scaturenti dall'analisi e dall'elaborazione dei dati personali dei lavoratori che determinano ricadute rilevanti sulle condizioni di lavoro, potendosi, a tal proposito, utilizzare come riferimenti il GDPR e la proposta di direttiva UE relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali; nel rafforzamento dei diritti collettivi; nella modifica delle previsioni che consentono il c.d. monitoraggio fine a se stesso dei lavoratori e nell'introduzione di una sezione del Codice ILO destinata alla fornire indicazioni pratiche sulle più frequenti

modalità e tipologie di controllo sui lavoratori.

Infine, sono state svolte alcune considerazioni in ordine alla tipologia di fonti dell'ILO da cui promanano le disposizioni dedicate alla tutela della riservatezza del lavoratore, anche alla luce dei possibili futuri sviluppi regolativi di cui si è dato conto. Si valuta positivamente il possibile aggiornamento del Codice di condotta e l'intenzione di introdurre regole sulla privacy e sulla trasparenza dell'utilizzo dei dati personali nel contesto della gestione algoritmica dei *platform workers*. Si evidenzia, però, che, anche qualora queste iniziative andassero a buon fine, permarrebbe un *gap* di tutela per i lavoratori – compresi quelli soggetti a gestione algoritmica nei settori tradizionali – considerata l'assenza di uno strumento normativo vincolante di carattere generale in materia di tutela della riservatezza dei lavoratori. Per tale ragione, sono state oggetto di valutazione l'opportunità di intraprendere un *iter* legislativo diretto all'adozione di una Convenzione internazionale in materia nonché le *chances* che il predetto procedimento conduca all'approvazione di un testo contenente un livello di protezione adeguato e suscettibile di ratifica da parte degli Stati contraenti.

Quanto alla valutazione di opportunità, si ritiene di poter fornire una risposta positiva in quanto la protezione della privacy dei lavoratori rappresenta una tematica di rilevanza globale e la predisposizione di un complesso di regole internazionali vincolanti può accrescere la qualità del lavoro e la salvaguardia della dignità delle persone che lavorano. Invece, fornire una risposta alla seconda questione risulta più complesso in quanto la realizzabilità della proposta e la qualità del suo contenuto dipende anche dalla "volontà politica" delle diverse componenti dell'ILO. Tuttavia, si è segnalato come l'esistenza di studi comparativi che hanno ravvisato l'esistenza di rilevanti convergenze a livello globale in tema di *data protection* sembri deporre in favore della possibilità di introdurre regole internazionali condivise sulla privacy nel contesto occupazionale.

BIBLIOGRAFIA

ADAM R., *Attività normative e di controllo dell'OIL e evoluzione della comunità internazionale*, Giuffrè, Milano, 1993

ALAIMO A., *Il pacchetto di misure sul lavoro nelle piattaforme: dalla proposta di Direttiva al progetto di Risoluzione del Parlamento europeo. Verso un incremento delle tutele*?, in *Labour & Law Issues*, vol. 8, n. 1, 2022

ALCOCK A., *History of the International Labour Organization*, Macmillan, London 1971

ALESSI C., *La Convenzione Ilo sulla violenza e le molestie sul lavoro*, in *Lavoro e diritto*, 3/2023, pp. 577-594

ALESSI C., *Lavoro tramite piattaforma e divieti di discriminazione nell'UE*, in ALESSI C., BARBERA M., GUAGLIANONE L. (a cura di), *Impresa, lavoro e non lavoro nell'impresa digitale*, Cacucci, 2019

BAIOCCO S. (JRC), FERNANDEZ-MACÍAS E. (JRC), RANI U. (ILO), PESOLE A. (JRC), *The Algorithmic Management of work and its implications in different context*s, Background paper Series, 21 giugno 2022

BAIOCCO S., FERNÁNDEZ-MACÍAS E., *Algorithmic management: A basic compass*, JRC Science for Policy Brief on Labour, Education and Employment, 2022.

BALLESTRERO M.V., *Ancora sui rider. La cecità discriminatoria della piattaforma*, in *Labor*, 1/2021

BELLAVISTA A., *Controlli tecnologici e privacy del lavoratore,* in BELLAVISTA A.-SANTUCCI R. (a cura di), *Tecnologie digitali, poteri datoriali e diritti dei lavoratori,* Giappichelli, Torino, 2022

BELLAVISTA A., *Sorveglianza elettronica, protezione dei dati personali e tutela dei lavoratori*, in *LDE*, 21 febbraio 2023

BERG J., FURRER M., HARMON E., RANI U., SIX SILBERMAN M., *Digital labour platforms and the future of work*, International Labour Office, ILO, Ginevra, 2018

BLANPAIN R., COLUCCI M. (a cura di), *L'organizzazione internazionale del lavoro. Diritti fondamentali dei lavoratori e politiche sociali*, Jovene Editore, Napoli, 2007

BRAVO F. (a cura di), *DATI PERSONALI. Protezione, libera circolazione e governance* - Vol. 1. *Principi*, Pacini Giuridica, 2023

CALAFÀ L., *Molestie e violenza sul lavoro: la questione debitoria rinnovata dalla ratifica della Convenzione OIL*, in *ISL - IGIENE & SICUREZZA DEL LAVORO*, 8-9/2023

COLAPIETRO C., GIUBILEI A., *Controlli difensivi e tutela dei dati del lavoratore: il nuovo punto della Cassazione*, in *Labour & Law Issues*, V, 7, 2021, n. 2

DAGNINO E., *Dalla fisica all'algoritmo: una prospettiva di analisi giuslavoristica*, Adapt University Press, 2019

DAGNINO E., *Modifiche agli obblighi informativi nel caso di utilizzo di sistemi decisionali o di monitoraggio automatizzati (art. 26, comma 2, d.l. n. 48/2023)*, in DAGNINO E., GAROFALO C., PICCO G., RAUSEI P. (a cura di), *Commentario al d.l. 4 maggio 2023, n. 48 c.d. "decreto lavoro"*, Adapt University Press, 2023

DE STEFANO V., "*Negotiating the algorithm". Automation, artificial intelligence and labour protection*, ILO, Employment Policy Department, Working Paper No. 246, 2018

DELFANTI A., *Machinic Dispossession and Augmented Despotism: Digital Work in an Amazon Warehouse*", in *New Media & Society*, vol. 23/2019

DI CERBO V., *Algorithmic management e piattaforme digitali: verso una normativa EU finalizzata a fissare livelli minimi comuni di tutela dei lavoratori*, in *LDE,* 1/2024

DI PAOLA L., *Sopravvivenza dei controlli c.d. "difensivi" dopo la modifica dell'art. 4 st. lav.*, in *IUS Lavoro*, 30 settembre 2021

EMILIANI S. P., *Italia, OIL e protezione dei dati personali*, in L. MECHI, A. SITZIA *Cento Anni nell'Organizzazione Internazionale del Lavoro. Prospettive storiche e giuridiche sulla partecipazione italiana*, CEDAM, Milano, 2023

FALLETTI E., *La discriminazione algoritmica: una prospettiva comparata*, Giappichelli, 2023

FALLETTI E., *Algoritmi: la discriminazione non è uguale per tutti*, in *LDE*, 2/2023

FERRANTE V. (a cura di), *A tutela della prosperità di tutti. L'Italia e l'Organizzazione Internazionale del Lavoro a un secolo dalla sua istituzione*, Giuffrè, Milano, 2019

FIORIGLIO G., *Intelligenza artificiale, privacy e rapporto di lavoro: una prospettiva informatico-giuridica*, in *LDE*, 2022

FULLERTON J., *'Mind-reading' tech being used to monitor Chinese workers' emotions*, in *The Telegraph*, 30 aprile 2018

GAUDIO G., *Le discriminazioni algoritmiche*, in *LDE*, 1/2024

GAUDIO G., *L'algorithmic management e il problema della opacità algoritmica nel diritto oggi vigente e nella Proposta di Direttiva sul miglioramento delle condizioni dei lavoratori tramite piattaforma*, in *LDE*, 1/2022

GAUDIO G., *La Cgil fa breccia nel cuore dell'algoritmo di Deliveroo: è discriminatorio*, nota a Tribunale Bologna 31/12/2020, in *RIDL*, 2/2021, pp. 175-195

GELLERT R., VAN BEKKUM M., ZUIDERVEEN BORGESIUS F., *The Ola & Uber judgments: for the first time a court recognises a GDPR right to an explanation for algorithmic decision-making***,** in *EU Law Analysis*, 28 aprile 2021

GLOBAL PRIVACY ASSEMBLY (GPA), *Policy Strategy Working Group 1: Global frameworks and standards*, ottobre 2020

HENDRICKX F., *Privacy and workplace monitoring in a global legal prerspective*, in PISANI C., PROIA G., TOPO A., (a cura di), *Privacy e lavoro: la circolazione dei dati personali e i controlli nel rapporto di lavoro*, Giuffrè, Milano, 2022

HENDRICKX F., *Protection of workers' personal data: General principles*, ILO Working Paper 62, Ginevra, maggio 2022

ILO, *World Employment and Social Outlook 2021: The Role of Digital Labour Platforms in Transforming the World of Work*, Ginevra, 2021

INGRAO A., *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata,* Cacucci Editore, Bari, 2018

INGRAO A., *La protezione dei dati personali dei lavoratori nel diritto vivente al tempo degli algoritmi*, in BELLAVISTA A., SANTUCCI R. (a cura di), *Tecnologie digitali, poteri datoriali e diritti dei lavoratori*, Giappichelli, Torino, 2022

KOJANEC G., *Convenzioni e raccomandazioni della Organizzazione internazionale del lavoro 1919–1968*, Padova, CEDAM, 1969

LACKOVÀ E., *Opacità degli algoritmi e decreto trasparenza: il sindacato fa la sua parte*, in *RIDL*, 2/2023, pp. 367-379

LINFANTE G., *I servizi privati per l'impiego: il caso delle agenzie di collocamento*, in *Monografie sul Mercato del lavoro e le politiche per l'impiego*, n. 4/2002, ISFOL

MAIO V., *I controlli difensivi e la tutela del patrimonio aziendale,* in PISANI C., PROIA G., TOPO A., (a cura di), *Privacy e lavoro: la circolazione dei dati personali e i controlli nel rapporto di lavoro,* Giuffrè, Milano, 2022

MALTSEVA V. K., *Wearables in the workplace: The brave new world of employee engagement*, in *Business Horizons*, Vol. 63, Issue 4, 2020

MARASCO F., *Nuove forme di contrattazione sindacale nelle relazioni industriali su piattaforma*, in *Labour & Law Issues*, vol. 5, n. 2, 2019

MECHI L., SITZIA A., *Cento Anni nell'Organizzazione Internazionale del Lavoro. Prospettive storiche e giuridiche sulla partecipazione italiana*, CEDAM, Milano, 2023

MORRISON S., *Just because you're working from home doesn't mean your boss isn't watching you*, in *Vox*, 2 aprile 2020

NANNIPIERI L., *Eterodirezione "algoritmica" negli appalti della logistica. Verso un quadro giurisprudenziale in mutamento*, in *Rivista Italia di Informatica e Diritto*, 1/2023

NOGUEIRA GUASTAVINO M., *Geolocalización lícita, probablemente desproporcionada. La necesidad de una vigilancia cualitativa, no cuantitativa,* in *Revista de jurisprudencia laboral,* 2023, n. 2

NUZZO V., *Customer satisfaction e contratto di lavoro subordinato*, in *DRI*, 1/2020

NUZZO V., *Il ragionevole sospetto di illecito e la possibilità di controlli difensivi occulti all'esame della Grande Camera della Corte Europea dei diritti dell'uomo,* in *Labor,* n. 2, 2020

NUZZO V., *Sulla sopravvivenza dei controlli c.d. difensivi dopo la riscrittura dell'art. 4 St. Lav.*, in *RIDL*, 2022, n. 1

PELUSO G., *Obbligo informativo e sistemi integralmente automatizzati*, in *Labour & Law Issues*, vol. 9, no. 2, 2023

PENSABENE LIONTI G.*., Lavoro temporaneo: le istanze esogene dell'OIL e il camaleontismo dell'approccio italiano*, in L. MECHI L., A. SITZIA A. (a cura di), *Cento Anni nell'Organizzazione Internazionale del Lavoro. Prospettive storiche e giuridiche sulla partecipazione italiana*, CEDAM, Milano, 2023

PERRONE F., *Corte Europea dei Diritti dell'Uomo, sentenza López Ribalda c. Spagna: la tutela della privacy sul luogo di lavoro dopo Barbulescu 2,* in *Labor,* 22 febbraio 2018

PERULLI A., *La discriminazione algoritmica: brevi note introduttive a margine dell'ordinanza del Tribunale di Bologna*, in *Lavoro Diritti Europa*, 1/2020

PINTO DE ALBUQUERQUE, SITZIA A., *Lavoro e monitoraggio: il "test di proporzionalità" nella giurisprudenza della CEDU* in PISANI C.-PROIA G.-TOPO A. (a cura di), *Privacy e lavoro: la circolazione dei dati personali e i controlli nel rapporto di lavoro*, Giuffrè, Milano, 2022

PIZZOFERRATO A., *Automated decision-making in HRM*, in *LG*, n. 11/2022

PIZZOFERRATO A., *Tecnologie digitali, poteri datoriali e diritti dei lavoratori*, in BELLAVISTA A., SANTUCCI R. (a cura di), *Tecnologie digitali, poteri datoriali e diritti dei lavoratori*, Giappichelli, Torino, 2022

PROIA G., *Controlli a distanza e trattamento di dati personali: due discipline da integrare (ma senza fare confusione),* in PISANI C., PROIA G., TOPO A. (a cura di), *Privacy e lavoro: la circolazione dei dati personali e i controlli nel rapporto di lavoro*, Giuffrè, Milano, 2022

RECCHIA G. A., *Condizioni di lavoro trasparenti, prevedibili e giustiziabili: quando il diritto di informazione sui sistemi automatizzati diventa uno strumento di tutela collettiva*, in *Labour Law & Issues*, 1, 2023

RICCI M., OLIVIERI A. (a cura di), *La tutela dei dati del lavoratore: visibile e invisibile in una prospettiva comparata,* Cacucci Editore, Bari, 2022

ROMEI R., *Il "ragionevole sospetto" in Cassazione,* in *LDE,* 28 febbraio 2023

SAHAN M., *The First International Standard on Violence and Harassment in the World of Work*, Cambridge University Press, 2020

SANFILIPPO G., *La verifica della genuinità dell'appalto nelle organizzazioni d'impresa (ultra)digitalizzate. Nota a Tribunale di Padova, Sez. Lav., sentenza 3 marzo 2023 n. 126*, in *LDE*, 22 giugno 2023

SARTORI A., *Il controllo tecnologico sui lavoratori: la nuova disciplina italiana tra vincoli sovranazionali e modelli comparati*, Giappichelli, Torino, 2020

SATRIANO A., *How my boss monitor me while I work from home*, in *The New York Times*, 6 maggio 2020

SCARPONI S., *La convenzione OIL 190/2019 su violenza e molestie nel lavoro e i riflessi sul diritto interno*, in *Rivista giuridica del lavoro*, 1/2021, pp. 23-39

SITZIA A., *Lavoro, controlli e privacy: un nouveau parcours per il test di bilanciamento nell'elaborazione della sezione lavoro (e del garante privacy),* in *Massimario di giurisprudenza del lavoro*, n. 4/2021

SPINELLI C., *La trasparenza delle decisioni algoritmiche nella proposta di Direttiva UE sul lavoro tramite piattaforma*, in *LDE*, 2/2022

STARK L., *Algorithmic Labor and information asymmetries. A case study of Uber's Drivers*, in *IJC*, n. 10, v. 27, 2016

TARDIVO D., *Controlli tramite l'(ab)uso di dispositivi di geolocalizzazione alla luce dell'art. 8 Cedu,* in *ADL,* 2023, n. 3

TIMELLINI C., *Quale reale trasparenza nel rapporto di lavoro con gli ultimi adempimenti?*, in *Variazioni su temi di Diritto del Lavoro*, 2/2023, pp. 571-605

TOPO A., TARDIVO D., *Hard e soft law nel diritto dell'Unione Europea in materia di trattamento dei dati personali e di tutela della riservatezza del lavoratore,* in PISANI C.-PROIA G.-TOPO A. (a cura di), *Privacy e lavoro: la circolazione dei dati personali e i controlli nel rapporto di lavoro*, Giuffrè, Milano, 2022

TREMELLONI R., *L'Organizzazione internazionale del lavoro*, Aracne, Milano, 1924

TROJSI A. (a cura di), *Trasparenza e attività di cura nei contratti di lavoro Commentario ai decreti legislativi n. 104 e n. 105 del 2022*, Adapt University Press, 2022

TULLINI P., *Dati*, in NOVELLA M. e TULLINI P. (a cura di), *Lavoro Digitale*, Giappichelli, 2022

WOOD A., *Algorithmic Management: Consequences for Work Organisation and Working Conditions*, in *JRC Working Papers Series on Labour, Education and Technology*, European Commission, 2021

WU Q., ZHANG H., LI Z. e LIU K., *Labor Control in the Gig Economy: Evidence from Uber in China*, in *Journal of Industrial Relations*, vol. 61(4), 2019

XENIDIS R., *Tuning EU equality law to algorithmic discrimination: three pathways to resilience*, in *Maastricht Law Journal of European and Comparative Law*, vol. 27, 2020

SUMMARY

In the first part of research work, the sources of the International Labour Organisation (ILO) on the protection of workers' privacy were mapped and examined.

Initially, was undertaken an analysis of the 1997 Code of Practice on the Protection of Workers' Personal Data, a source of soft law without the *status* of an international labor standard but containing a comprehensive regulation of the subject. In particular, the the regulatory technique adopted and the main contents of the ILO Code were examined.

Concerning the technical choices, it was acknowledged that the ILO Code incorporates terminology and principles from the then-current data protection regulations, adapting them to the specificities of the employment context (duration of the employment relationship requiring the processing of personal data for various reasons from the pre-employment phase; conflict between the employer's power of control and workers' privacy demands; structural weakness of the candidate/worker compared to the employer processing his/her personal data). Furthermore, it was observed that the ILO Code uses general clauses instead of specific definitions, so as to facilitate the adaptation of its contents to technological developments.

Regarding the content, the ILO Code was also examined from an actualising perspective, finding that some provisions could be relevant to the regulation of more recently developed phenomena such as algorithmic management, algorithmic discrimination and customer satisfaction.

Subsequently, the provisions aimed at protecting worker privacy within the Conventions and Recommendations adopted by the ILO were examined to determine if it is possible to derive a comprehensive regulation and the existence of general principles related to worker privacy. Therefore, was conducted an analysis of relevant provisions concerning: (i) the processing of personal data within private employment agencies; (ii) the protection of workers' health data, with a focus on information related to HIV status; (iii) the protection of the personal identity of those reporting irregularities to labor inspection bodies; (iv) the protection of the private life and privacy of individuals involved in situations of violence and harassment in the workplace.

As a result of the reconnaissance and analysis carried out, it was established that the ILO Conventions and Recommendations do not seem to comprehensively regulate the matter, protecting only specific categories of workers or workers in general, but exclusively regarding certain types of personal data (health data). Additionally, given the sectoral nature of the identified provisions, it does not seem possible to identify general principles related to the protection of workers' privacy, except in the context of the processing of workers' health data.

The research work then discussed initiatives activated by the ILO aimed at strengthening the protection of workers' privacy in line with the programmatic indications of the 2019 Centenary Declaration for the Future of Work. The ILO has activeted a legislative process aiming to approve an international labor standard on decent work in the platform economy, which should also include provisions to ensure the privacy protection of platform workers and transparency in the processing of personal data in the context of algorithmic management of work.
Furthermore, approximately thirty years after the adoption of the Code of Practice on the Protection of Workers' Personal Data, a tripartite expert meeting on the protection of workers' personal data in the digital era is being organized. Although the subject matter of the meeting has not yet been definitively fixed, it has been suggested that the agenda might include an assessment of the ongoing relevance of the Code of Practice on the Protection of Workers' Personal Data and, if deemed necessary, its updating.

Considering the potential developments of the aforementioned initiatives, a general overview of the challenges posed by algorithmic management of work and technological evolution regarding the use of workers' personal data for decision-making and/or performance monitoring purposes was provided.
It was noted that the respect for privacy rights and the protection of personal data are increasingly being questioned by technological evolution and algorithmic management of work due to the growing amount of worker-personal information avaible on the web and social media; the introduction of feedback collection systems on workers in organizational settings; the proliferation of tools and systems - sometimes difficult to identify - capable of continuously collecting highly sensitive personal data of workers and teleworkers; the spread of new ways of using personal data, such as the "reading of the inner sphere" of the worker to measure, for example, emotional state and stress resistance; the speed of development and increasing complexity of technologies used for personal data processing which pose ever greater difficulties in understanding their functioning, requiring increasingly advanced technological skills; the increased potential for the use of the collected information about workers - becoming more numerous, detailed, and sensitive - for discriminatory or otherwise improper purposes; the lack of transparency regarding the operation of decision-making systems based, in whole or in part, on the processing of workers' personal data.

It was also highlighted that an adequate level of protection of the private life and personal data of workers can strengthen the effectiveness of prohibitions on discrimination and the right to health and safety at work.

In light of the outlined scenario and the most recent ILO initiatives, some proposals for amending and/or strengthening the Code of Practice on the Protection of Workers' Personal Data were formulated. These proposals include, *inter alia*, extending the subjects considered in order to include also developers of systems used by employers for processing the personal data; strengthening the transparency and explainability of "algorithmic decisions" resulting from the analysis and processing of workers' personal data that have significant impacts on working conditions, using the GDPR and the proposal for an EU directive onon improving working conditions in platform-based

digital work as references; strengthening collective rights; modifying provisions that allow the so-called monitoring for its own sake of workers and introducing a section of the ILO Code aimed at providing practical guidance on the most common methods and types of worker monitoring.

Finally, some considerations were made regarding the type of ILO sources from which provisions dedicated to the protection of worker privacy originate, also in light of possible future regulatory developments mentioned above. The possible updating of the Code of Conduct and the intention to introduce rules on privacy and transparency in the use of personal data in the context of algorithmic management of platform workers are viewed positively. However, it is emphasized that, even if these initiatives were to succeed, would persist a protection gap for workers - including those subject to algorithmic management in traditional sectors - given the absence of a binding general normative instrument regarding the protection of workers' privacy. For this reason, the feasibility of initiating a legislative process for the adoption of an international convention on the matter and the likelihood that the aforementioned process leads to the approval of a text containing an adequate and ratifiable level of protection by contracting states were evaluated.

With regard to the assessment of appropriateness, a positive response is believed can be given insofar as the protection of workers' privacy is an issue of global relevance and the drafting of a set of binding international rules can increase the quality of work and the protection of the dignity of persons at work. On the other hand, providing an answer to the second question is more complex as the feasibility of the proposal and the quality of its content also depend on the "political will" of the components of the ILO. However, it has been pointed out that the existence of comparative studies that have identified the existence of significant convergences at global level on the subject of data protection would seem to argue in favour of the possibility of introducing shared international rules on privacy in the employment context.