REGIONE TOSCANA

Consiglio Regionale

Premio tesi di Laurea
“David Sassoli”
edizione 2022

Presentazione

La scelta del Consiglio Regionale della Toscana di dedicare un premio di laurea a David Sassoli è un piccolo modo per tenere viva la memoria di tutto ciò che ha rappresentato nella sua vita.

Il Premio Sassoli non è soltanto un tributo all'eccellenza accademica, ma anche un omaggio all'immenso impegno di un uomo che ha dedicato la sua vita all'ideale dell'integrazione europea.

David è stato un politico appassionato, leader leale, rigoroso, ha saputo nutrire con la sua cultura un'iniziativa politica al servizio delle persone e delle Istituzioni. Un uomo del dialogo, sempre alla ricerca del bene comune, ma fermo nel difendere i valori della solidarietà e della libertà. Sassoli ha saputo avvicinare l'Europa alle cittadine e ai cittadini e questo senza dubbio rappresenta una delle sue più importanti eredità.

Oggi l'Unione Europea, grazie anche al suo contributo, rappresenta una dimensione essenziale, irrinunciabile per la nostra democrazia e per la libertà di ogni cittadino europeo. Senza le istituzioni europee i singoli Stati sarebbero impotenti di fronte alle sfide globali del nostro tempo: dai mutamenti climatici ai fenomeni migratori, dalle dinamiche demografiche a quelle geopolitiche condotte da attori di dimensione continentale fino ai poteri economici e finanziari che travalicano i confini e condizionano i mercati.

La nostra Europa non è perfetta, ma è la migliore garanzia per tutti i nostri cittadini.

Pubblicando le tesi vincitrici del premio, vogliamo tenere insieme il ricordo di David offrendo anche una prospettiva futura che solo i più giovani, coi loro occhi e il loro studio possono offrire per aspirare all'Europa della speranza tanto cara al Presidente Sassoli.

Spero, dunque, che questa collana possa ispirare ulteriori ricerche e riflessioni su questi temi cruciali, contribuendo a costruire un'Europa più inclusiva, solidale e democratica, proprio nel solco tracciato da David Sassoli.

Dobbiamo guardare all'Europa come luogo delle opportunità, come sogno per realizzare il proprio futuro, come orizzonte per le nuove generazioni.

L'Europa unita è l'eredità che Altiero Spinelli ci ha lasciato col suo "Sogno Europeo" nato sull'isola di Ventotene. Un sogno e un patrimonio di libertà di cui oggi noi dobbiamo essere non solo testimoni ma, soprattutto, custodi.

Antonio Mazzeo
Presidente del Consiglio regionale della Toscana

Prefazione

È con grande soddisfazione che salutiamo la pubblicazione di questa tesi che ha conquistato uno dei riconoscimenti assegnati nell'ambito del premio di laurea intitolato a David Sassoli.

Si tratta di un'iniziativa che abbiamo fortemente voluto come Commissione Politiche Europee e Relazioni Internazionali del Consiglio Regionale della Toscana, trovando pieno e fondamentale sostegno da parte dell'Ufficio di Presidenza della nostra Assemblea a partire dal Presidente Antonio Mazzeo.

Valorizzare le idee e le proposte delle giovani generazioni ci è sembrato il modo più bello ed emozionante per ricordare ed onorare David Sassoli.

Un'esperienza che nel giorno della consegna dei riconoscimenti tiene insieme emozioni contrastanti, quali il dolore per una scomparsa tanto rilevante e al tempo stesso la gioia nel vedere evidenziato il lavoro delle ragazze e dei ragazzi, guardando soprattutto alle prospettive di un'Europa che deve essere rafforzata e costruita partendo proprio dalle idee delle giovani generazioni. Ed a questo David Sassoli teneva moltissimo.

E noi teniamo tantissimo anche al supporto che abbiamo ricevuto dal mondo delle Università toscane e vogliamo ringraziare le docenti ed i docenti che hanno accettato di far parte della commissione che ha scelto le tesi da premiare, perché, con la loro competenza e passione, hanno dato un valore aggiunto a questa nostra iniziativa: una commissione presieduta da Jacopo Cellini dell'Istituto Universitario Europeo e composta da Benedetta Baldi dell'Università degli Studi di Firenze, Edoardo Bressanelli della Scuola superiore Sant'Anna di Pisa, Massimiliano Montini dell'Università degli studi di Siena, Manuela Moschella della Scuola Normale Superiore di Pisa, Luca Paladini, dell'Università per Stranieri di Siena, Saulle Panizza, dell'Università di Pisa.

E la pubblicazione che state per sfogliare rappresenta anche un altro obbiettivo che abbiamo fortemente voluto e che porterà alla creazione di un'apposita collana all'interno delle pubblicazioni del Consiglio Regionale della Toscana. Queste tesi resteranno dunque segno tangibile di un impegno che guarda all'Europa ed anche di un'iniziativa che è stata inserita, per volontà unanime, tra le attività istituzionali del Consiglio Regionale della Toscana e che dunque affidiamo anche alle colleghe ed ai colleghi che arriveranno dopo di noi.

Ma tutto questo non si sarebbe potuto realizzare senza lo straordinario impegno e lavoro dei componenti della "Commissione Europa" che ho avuto l'onore di guidare. Una Commissione di cui, in questa XI Legislatura, hanno fatto parte Giovanni Galli (vicepresidente, Lega), Anna Paris (vicepresidente segretaria, PD), Irene Galletti (M5S), Valentina Mercanti (PD), Fausto Merlotti (PD), Massimiliano Pescini (PD), Marco Stella (FI), Andrea Vannucci (PD) e Gabriele Veneri (FdI).

È tutto loro il merito dei risultati raggiunti, di chi c'era all'inizio e soprattutto di chi continua a fare parte di questa Commissione con una passione ed una competenza davvero uniche. È a loro che va tutta la mia riconoscenza che estendo a tutti gli uffici ed al personale che ci hanno accompagnato in questo percorso.

Mi sia concesso di ringraziare il mio gruppo, il PD, per un supporto che è stato totale e costante ed anche il gruppo di Italia Viva che, seppur non rappresentato in Commissione, non ha mai fatto mancare stimoli e sostegno. Ma è a tutti i gruppi, di maggioranza e di opposizione, che va la mia più profonda gratitudine per un lavoro che, grazie alle commissarie ed ai commissari, stiamo portando avanti insieme, costruendo una modalità di dialogo e di confronto che è un elemento di vanto ed orgoglio.

Un lavoro, quello della Commissione, che proseguirà con iniziative e progetti legati alle Giornate dell'Europa a cui si aggiunge una volontà di approfondimento dei vari temi, contando anche sulla disponibilità della Giunta guidata dal Presidente Eugenio Giani con le assessore e gli assessori che ne fanno parte.

In conclusione mi sia permesso di rivolgere un affettuoso pensiero ai familiari di David Sassoli che, in questi anni, hanno sempre dimostrato grandissima attenzione a questa nostra iniziativa: a loro va un abbraccio fortissimo, unito all'impegno che vale per l'oggi e per il domani e che è quello di tenere sempre vivo il ricordo di un uomo come David che ci ha fatto sentire orgogliosi di essere toscani, italiani ed europei.

Francesco Gazzetti
Presidente Commissione Politiche Europee
e Relazioni Internazionali del Consiglio Regionale della Toscana

UNIVERSITÀ DI PISA

Dipartimento di Giurisprudenza

Corso di Laurea in Giurisprudenza

Management attraverso algoritmi e problemi di privacy: un approccio europeo

Candidato
Filippo Bordoni

Relatore
Chiar.mo Prof.
Oronzo Mazzotta

Anno accademico 2020/2021

Alla mia famiglia di lavoratori

Sommario

Introduzione

Spesso accade che il diritto del lavoro si confronti per primo con le innovazioni tecnologiche, economiche e sociali: quando le imprese apportano cambiamenti ai propri processi produttivi, in genere adottando una nuova tecnologia o un nuovo metodo di organizzazione delle risorse, i lavoratori sono quasi sempre coinvolti da tali cambiamenti.

A causa delle caratteristiche del rapporto di lavoro, un rapporto durevole nel tempo, caratterizzato dall'inevitabile disequilibrio tra i poteri del datore e quelli del dipendente e connotato con forza dalla dimensione collettiva dell'azione sindacale, le modificazioni nella realtà aziendale tendono a incidere con sorprendente rapidità sul piano giuridico: come regolare i nuovi rapporti di potere? Come tutelare il lavoratore dalle situazioni pregiudizievoli per la sua salute e la sua dignità? Quali strumenti e quali pratiche permettere, e quali vietare? Il diritto del lavoro ha il compito di trovare risposte a tali domande, dapprima attraverso le giurisprudenza e l'autonomia collettiva, in un secondo momento attraverso l'attività legislativa.

Quando, a cavallo degli anni '10 di questo secolo, strumenti come computer, smartphone e GPS sono diventati relativamente economici e di uso sempre più comune, una nuova forma di organizzazione del lavoro ha presto iniziato a diffondersi negli Stati Uniti e in Europa: la cd. *gig economy*, che nel dibattito quotidiano viene spesso ricondotta ai fattorini che consegnano cibo a domicilio, ma che in realtà rappresenta un fenomeno molto più complesso e sfaccettato, problematico per più aspetti da un punto di vista giuridico[1].

Sono tecnologie digitali basate su algoritmi più o meno complessi a rendere tecnicamente possibile il lavoro su piattaforma. Quando queste tecnologie vengono utilizzate per esercitare una parte o addirittura la totalità dei poteri propri del datore di lavoro si parla, in generale, di *management attraverso algoritmi*.

Ciò su cui questa ricerca intende soffermarsi è che il potenziale per l'impiego di algoritmi sul lavoro è molto ampio e non si limita affatto alla *gig economy*. In

[11] V. *infra*, cap. 1 par. 1.

misura variabile, le tecniche di *management attraverso algoritmi* sono già oggi impiegate anche in posti di lavoro *standard*, o lo potranno essere in futuro.

Il diritto del lavoro italiano si è occupato, a partire dallo Statuto dei Lavoratori del 1970, di limitare il potere datoriale di controllo, in particolare quando esercitato a distanza con l'ausilio di tecnologie, con il fine di tutelare la libertà di pensiero e la dignità del lavoratore. Attraverso questa disciplina, significativamente, lo Statuto ha introdotto per la prima volta un corpo di regole a tutela della privacy del lavoratore, e quindi della sua dignità.

L'esercizio automatizzato del potere di controllo è senza dubbio uno degli aspetti più inquietanti resi possibili dal management attraverso algoritmi, ma non è certo l'unico: come si vedrà nel primo capitolo, il datore può tecnicamente demandare a un algoritmo sia il controllo, sia la direzione, sia la disciplina del rapporto di lavoro e le decisioni prese in autonomia dal sistema informatico possono riguardare tanto la dinamica quotidiana del lavoro quanto decisioni cruciali per la vita del dipendente, come assunzioni, promozioni, trasferimenti o addirittura licenziamenti.

Una caratteristica cruciale delle tecnologie basate su algoritmi è che, per poter funzionare, necessitano di un gran numero di dati. Sul posto di lavoro, questi dati possono essere raccolti con una notevole facilità: dagli strumenti di lavoro, da sensori sparsi nell'ambiente, da dispositivi indossati dai lavoratori stessi come braccialetti o orologi, dall'attività e dalle recensioni dei clienti.

Come si vedrà, i profili problematici che circondano il management attraverso algoritmi sono molteplici. Tra di essi, il tema della privacy e della protezione dei dati dei lavoratori appare tuttavia cruciale, in quanto la raccolta e il trattamento dei dati personali è una fase preliminare e necessaria in ogni applicazione di management attraverso algoritmi. Se quindi è corretta la previsione per cui i dati occuperanno un ruolo sempre più importante nel lavoro, si può facilmente immaginare una stagione di rinnovata centralità per il tema della privacy dei dipendenti.

Questa ricerca tenta di individuare gli strumenti a disposizione dei lavoratori per contrastare le conseguenze negative dell'applicazione di tecniche di management attraverso algoritmi.

Nel primo capitolo verranno individuati i confini del management attraverso algoritmi, le ragioni per cui appare corretto parlare di un fenomeno nuovo e trasversale e le conseguenze potenzialmente dannose che esso può avere sulla

vita dei lavoratori, anche attraverso una breve rassegna di casi giunti all'attenzione delle cronache negli ultimi quindici anni.

Nel secondo capitolo verrà analizzata la normativa italiana applicabile al controllo dei dipendenti in una prospettiva storica: dapprima l'elaborazione dottrinale del potere di controllo precedente all'approvazione dello Statuto dei Lavoratori, in seguito gli artt. 4 e 8 dello Statuto, poi il Codice della privacy del 2003 e infine la riforma dello Statuto operata dal cd. Jobs Act del 2015.

Nel terzo capitolo verrà affrontata la protezione dei dati personali da un punto di vista eurounitario. Nello specifico, verranno trattati quegli articoli del Regolamento 2016/679 (GDPR) applicabili ai dati raccolti per essere utilizzati da algoritmi di management, con particolare attenzione per l'approccio preventivo e basato su condizioni di liceità che caratterizza il trattamento dei dati personali nella normativa dell'Unione europea.

Nel quarto capitolo si esamineranno concretamente gli strumenti già oggi a disposizione del lavoratore per contrastare le invasioni della privacy in contesti di management attraverso algoritmi. Verrà quindi dato conto della giurisprudenza italiana ed europea e dei provvedimenti del Garante della privacy che dimostrano la concreta funzionalità dello Statuto dei lavoratori e del GDPR nell'ambiente di lavoro.

Capitolo 1. Il management attraverso algoritmi: possibili novità nel rapporto di lavoro e profili problematici

1. *L'oggetto di questo studio: management attraverso algoritmi e problemi definitori*

La rivoluzione digitale ha prodotto e sta producendo nelle aziende delle importanti trasformazioni[1]. La disponibilità di strumenti informatici che permettono di raccogliere, conservare ed elaborare immense moli di dati a costi relativamente contenuti ha il potenziale per produrre conseguenze non solo negli ambiti più scontati, in particolare i servizi al consumatore, ma virtualmente in ogni settore dell'economia[2].

Le possibilità offerte dai cd. *big data* e dall'utilizzazione di intelligenze artificiali all'interno dell'azienda non si limitano all'aspetto commerciale o all'organizzazione dei processi produttivi: molto presto, infatti, le tecniche legate alle nuove tecnologie hanno iniziato ad essere applicate anche alla gestione dei lavoratori.

Per poter procedere oltre nello studio delle novità introdotte dagli strumenti digitali nel rapporto di lavoro, occorre preliminarmente definire con precisione l'oggetto della ricerca. La complessità delle trasformazioni imposte all'ambiente di lavoro dalle nuove tecnologie è forse testimoniata dalla quantità di espressioni che vengono utilizzate per riferirsi a fenomeni talvolta contigui, talvolta in parte sovrapponibili, talvolta legati solamente dal comune riferirsi al lavoro umano.

---

[1] S. Lohr, "'The Beginning of a Wave': A.I. Tiptoes Into the Workplace", *The New York Times* 5/8/2018, consultato online il 20/8/2021 all'indirizzo https://www.nytimes.com/2018/08/05/technology/workplace-ai.html?searchResultPosition=4, D. Peck, "We are watching you at work", *The Atlantic*, 12/2013, consultato online il 20/8/2021 all'indirizzo https://www.theatlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681/.

[2] C. DEGRYSE (2016), in "Digitalisation of the economy and its impact on labour markets", ETUI Working Paper 2016.02, a p. 12 e 13 riporta un discorso del Commissario Gunter Oettinger sull'impatto delle intelligenze artificiali sull'industria dell'auto.

Negli anni recenti, l'attenzione degli studiosi del diritto del lavoro è stata attratta in particolare dalla cd. *gig economy*[3]. Questo fenomeno è interessante, dal punto di vista del giurista, per almeno due elementi che ne determinano la novità: da un lato, i lavoratori della *gig economy* non sono, di solito, qualificati dalle piattaforme come dipendenti, bensì come lavoratori autonomi che volontariamente si mettono a disposizione dell'utente finale, nei tempi e con gli orari che preferiscono, per svolgere singole mansioni tendenzialmente elementari come trasportare un passeggero nella propria automobile oppure consegnare a domicilio del cibo ritirato da un ristorante. Le conseguenze di una tale sistemazione giuridica sono notevolissime in termini di tutela dei lavoratori e continuano ad occupare ancora oggi una parte significativa del dibattito lavoristico in ambito accademico e giudiziario[4].

Dall'altro lato, per quello che più interessa ai fini di questo scritto, un elemento comune ai lavoratori su piattaforma sono i metodi di *management* che vengono impiegati per dirigerli, controllarli e disciplinarli. Poiché le mansioni svolte non sono nella sostanza differenti da quelle che, nell'economia tradizionale, sarebbero affidate a un dipendente dell'azienda, le piattaforme digitali hanno adottato degli strumenti innovativi di gestione del personale. Normalmente, infatti, il lavoratore delle piattaforme non è assegnato a un superiore che ne diriga e controlli la prestazione e che applichi il potere disciplinare, bensì è tenuto a rispettare le indicazioni fornite dagli algoritmi di proprietà della

[3] La *gig economy* è a sua volta un fenomeno complesso. Sotto questo nome sono infatti ricondotte due diverse modalità di lavoro: il *crowdwork*, consistente in una serie di attività completate direttamente su una piattaforma online, e il lavoro su richiesta tramite piattaforma, dove attività tradizionali come il trasporto di persone, la consegna di merci o le pulizie vengono svolte attraverso piattaforme digitali che mettono in contatto il lavoratore con il cliente e stabiliscono degli standard di qualità. Per una panoramica sul tema, v. V. DE STEFANO (2016), "The rise of the «just-in-time workforce»: On-demand work, crowdwork and labour protection in the «gig-economy»", Conditions of work and employment series, n.71, ILO.

[4] Tra i moltissimi, v. A. ALOISI (2016 a), "'Dependent contractors' in the gig economy – a comparative approach", *American University Law Review*, vol. 66 n. 3; A. ALOISI (2016 b), "Commoditized workers. Case study research on labor law issues arising from a set of 'on-demand/gig economy' platforms", *Comparative Labor Law and Policy Journal*, vol. 37 n. 3; F. CAPPONI (2015), "La regolazione delle collaborazioni etero-organizzate tra legge e contratto: il caso delle piattaforme di *food delivery*", *Diritto delle relazioni industriali*, vol. 28 n. 4, pp. 1247-1260; P. ICHINO (2018), "Subordinazione, autonomia e protezione del lavoro nella *gig-economy*", *Rivista italiana di diritto del lavoro*, n. 2, pp. 283-303; A. SITZIA, G. CINÀ (2020), "Subordinazione ed etero-organizzazione: rider e "debolezza economica" in una prospettiva comparata", *La nuova giurisprudenza civile commentata*, n. 4; da ultimo, v. S. BATTISTELLI (2021), "Discriminazione per ragioni di affiliazione sindacale: il caso dei rider", *Il lavoro nella giurisprudenza*, n. 8-9, pp. 862-871; L. DE ANGELIS (2021), "Su forma e prova del lavoro dei riders, anche nella pandemia", *Labor*, n. 2, pp. 59-68.

piattaforma[5], la sua attività viene monitorata attraverso lo smartphone o il pc[6] e, in caso di prestazione inferiore alle aspettative della piattaforma registrata attraverso un sistema di rating, il suo account può essere sospeso o disattivato[7].

In ogni caso, gli strumenti attraverso i quali viene diretta, controllata e disciplinata l'attività del singolo lavoratore che si vorrebbe autonomo sono all'evidenza digitali e quindi automatizzati. La controparte del *rider* o dell'autista di Uber non è, se non in casi eccezionali, un manager in carne ed ossa, bensì un algoritmo[8].

Va tuttavia sottolineato come nulla impone che tali tecnologie siano applicate ai soli rapporti atipici che caratterizzano la *gig economy*, e anzi esse stiano trovando applicazione sempre più diffusa con riguardo a lavoratori subordinati, in settori che definiremmo tradizionali[9]. Allo scopo di migliorare la produttività, infatti, il datore di lavoro può raccogliere e conservare grandi quantità di dati prodotti dai dipendenti medesimi così come dai clienti, analizzarli attraverso algoritmi sempre più raffinati e utilizzare i risultati di tale elaborazione al fine di esercitare i propri poteri datoriali.

A questo proposito, è opportuno richiamare alcune locuzioni comunemente utilizzate nel dibattito sul tema, darne una definizione e chiarire con quale fenomeno specifico si vuole confrontare questa ricerca.

Si parla di controllo elettronico della prestazione (*electronic performance monitoring*, o EPM) con riguardo a tecniche elettroniche che permettono il controllo pervasivo dell'attività del lavoratore. Non si tratta necessariamente di un fenomeno recente: gli strumenti più frequentemente ricondotti a questa categoria vanno dall'accesso alla mail alle intercettazioni delle linee telefoniche

[5] A. MCAFEE, E. BRYNJOLFSSON (2017), *Machine, Platform, Crowd: Harnessing our Digital Future*, WW Norton & Co.
[6] *Ivi*.
[7] A. ALOISI (2016), "Commoditized workers: Case study research on labour law issues arising from a set of 'on-demand/gig economy' platforms", *Comparative Labor Law & Policy Journal*, University of Illinois College of Law, vol. 37, n. 3, pp. 653–690.
[8] Nell'uso proprio delle scienze sociali, vengono definiti algoritmi "computer-programmed procedures that transform input data into desired outputs in ways that tend to be more encompassing, instantaneous, interactive, and opaque than previous technological systems" – K. KELLOGG, M. A. VALENTINE, A. CHRISTIN (2020), "Algorithms at work: the new contested terrain of control", *Academy of Management Annals*, vol. 14 n. 1, p. 366, Academy of Management.
[9] V. *infra*, par. 5.

aziendali, dal controllo del contenuto e dei tempi di utilizzo dei computer alla videosorveglianza e al tracciamento GPS dei dipendenti[10].

Queste tecniche, estremamente intrusive della sfera privata del lavoratore e con un potenziale lesivo della sua dignità, non richiedono di per sé alcun livello di automazione o di analisi in tempo reale dei dati[11]. Tuttavia, con il sopravvento dei *big data*, alle più tradizionali pratiche di EPM si sono aggiunte nuove possibilità di controllo della prestazione.

In questo senso, si può parlare di *workforce* o *people analytics* in riferimento a "un processo o un metodo nella gestione delle risorse umane basato sull'uso di "big data" per acquisire conoscenze riguardo alla prestazione di lavoro"[12]. L'obiettivo del *workforce analytics* è di assoggettare i processi decisionali all'elaborazione di dati obiettivi, in modo da limitare il più possibile valutazioni arbitrarie e da condurre a decisioni il più possibile razionali da parte della dirigenza[13]. Va evidenziato che i dati utilizzati per ottenere questi fini non sono raccolti necessariamente attraverso gli intrusivi strumenti di controllo elettronico della performance visti poc'anzi, ma anzi nella maggior parte dei casi derivano dagli strumenti medesimi attraverso cui viene resa la prestazione di lavoro, dai *feedback* dei clienti e da metadati provenienti da altri contesti[14].

Gli strumenti di *workforce analytics* sono effettivamente una novità recente, resa possibile dall'uso all'interno delle aziende dei *big data*, che possono essere intesi come "la pratica di combinare enormi volumi di informazioni provenienti da

---

[10] "Electronic performance monitoring (EPM) includes email monitoring, phone tapping, tracking computer content and usage times, video monitoring and GPS tracking. Data produced can be used as productivity indicators; indication of employees' location; email usage; website browsing; printer use; telephone use; even tone of voice and physical movement during conversation" – P. MOORE, P. AKHTAR, M. UPCHURCH (2018), "Digitalisation of Work and Resistance", in P. MOORE, M. UPCHURCH, X. WHITTAKER, *Humans and Machines at Work*, Palgrave MacMillan, p. 19.

[11] E infatti la loro applicazione è documentata già dall'inizio del XXI secolo in ambiti specifici come i call center: v. P. TAYLOR, G. MULVEY, J. HYMAN, P. BAIN (2002), "Work organisation, control and the experience of work in call centres", *Work, Employment & Society*, vol. 16 n. 1, pp. 133–150, BSA.

[12] "People analytics is a process or method of human resources management based on the use of "big data" to capture insights about job performance" (trad. in italiano mia) – M. BODIE ET AL. (2016), "The Law and Policy of People Analytics", *Legal Studies Research Paper Series*, n. 2016-6, p. 3, St. Louis University School of Law.

[13] E. DAGNINO (2017), "People Analytics: lavoro e tutele al tempo del management tramite big data", *Labour & Law Issues*, vol. 3 n. 1, p. 7.

[14] Il tema sarà affrontato *infra*, ma per un approfondimento v. fin d'ora K. CRAWFORD, J. SCHULTZ (2014), "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms", *Boston College Law Review*, vol. 55 n. 1, pp. 93-128.

diverse fonti e di analizzarle, usando sofisticati algoritmi per informare le decisioni"[15].

Il *workforce analytics*, in sé considerato, non è una modalità di esercizio dei poteri datoriali se non in senso lato. Esso consiste, nella definizione condivisa più sopra, in una tecnica di analisi di dati che non necessariamente derivano dall'attività di controllo dei dipendenti, i cui risultati possono o non possono essere presi in considerazione dalla dirigenza dell'azienda nell'esercizio del potere direttivo, di controllo ed, eventualmente, disciplinare.

È tuttavia possibile che un algoritmo[16] impiegato dal management dell'azienda non si limiti ad elaborare dati, ma eserciti concretamente poteri datoriali in maniera automatizzata[17]. In questo caso, si parla più propriamente di *management attraverso algoritmi*[18] (MAA) o, in inglese, *algorithmic/AI-driven management*. Queste tecniche si basano naturalmente sulla elaborazione automatizzata dei dati propria degli strumenti di *workforce analytics*, ma, attraverso l'impiego di sistemi di intelligenza artificiale, possono incidere direttamente sul rapporto di lavoro in tutte le sue fasi[19].

Ancora una volta, tali impieghi dell'intelligenza artificiale si sono osservati per primi nell'ambito della *gig economy*, ma sono già oggi diffusi, per alcuni specifici aspetti, con riguardo a posti di lavoro standard in certi settori dell'economia[20].

È importante notare come la netta distinzione qui riproposta tra *workforce analytics* e management attraverso algoritmi non è universalmente accettata, anche per il motivo che spesso i confini tra le due pratiche sono piuttosto sfumati e difficili da individuare per un osservatore esterno[21]. In concreto, nei

---

15 European Data Protection Supervisor, Opinion 7/2015. "Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability", 19/11/2015 (nella trad. di E. DAGNINO (2017), cit., p. 5).

16 Inteso, ancora una volta, nel senso specifico di cui alla nota 7.

17 "[…] there is nothing inherent in the capabilities of such software to limit itself to informing traditional managers: in principle, at least, their actual decisions can be fully automated" - 17 J. ADAMS-PRASSL (2019), "What if your boss was an algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work", *Comparative Labor Law & Policy Journal*, vol. 41 n.1, p. 141, University of Illinois College of Law

18 "We call software algorithms that assume managerial functions and surrounding institutional devices that support algorithms in practice algorithmic management" – M. K. LEE ET AL. (2015), "Working with Machines: The Impact of Algorithmic and Data-Driven Management on Human Workers", *CHI '15: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pp. 1603-1612, ACM.

19 J. ADAMS-PRASSL (2019), "What if your boss was an algorithm?", cit., pp. 126 e sgg.

20 Per una rassegna della cronaca statunitense, europea ed infine italiana, v. *infra*, par. 5.

21 Lo stesso Adams-Prassl, uno dei principali studiosi in materia, in "What if your boss was an algorithm", cit., pare usare come sinonimi i due termini in diversi passaggi dell'articolo.

contesti lavorativi dove sono adottati strumenti digitali di analisi dei dati per la gestione delle risorse umane, l'influenza di tali strumenti può variare molto anche in dipendenza degli ambiti specifici di utilizzo e di fattori come la cultura aziendale, l'attività di sindacati e, naturalmente, la legislazione applicabile.

È ben possibile che un algoritmo di *workforce analytics*, che cioè non è teoricamente in grado di produrre immediatamente degli effetti sui lavoratori ma solo di analizzare i dati che li riguardano, sia nella pratica a tal punto centrale nelle decisioni datoriali da dar luogo di fatto a decisioni automatizzate.

Questa ricerca si concentrerà sui problemi che sorgono dall'applicazione sui posti di lavoro non degli algoritmi in generale, ma solo di quelli rivolti alla gestione delle risorse umane, in particolare per quanto riguarda la privacy dei lavoratori e la protezione dei dati personali. Nel corso della trattazione si farà riferimento principalmente al *management attraverso algoritmi*, con la necessaria avvertenza espressa poc'anzi: e cioè che non è necessario che si dia automatismo della decisione basata sugli algoritmi per incorrere in problemi in larga parte simili a quelli riscontrati nei casi di management attraverso algoritmi in senso stretto.

2. *Il management attraverso algoritmi è una novità?*

Le ragioni per cui sempre più datori di lavoro stanno introducendo nella propria organizzazione strumenti di MAA sono molteplici. La giustificazione più frequentemente offerta è che tali tecniche aumentano l'efficienza e la capacità di innovazione dell'azienda[22].

Questa affermazione, in verità estremamente generica, è molto difficile da contestare; studi economici e sociologici non hanno ancora raggiunto risultati definitivi in merito.

Se non è possibile dare una risposta univoca riguardo all'effetto del MAA sull'efficienza dell'azienda nel suo complesso (né è questo compito del giurista), ci si deve tuttavia interrogare sui cambiamenti che l'introduzione di tali strumenti digitali comporta sulle modalità con cui i poteri datoriali vengono esercitati, sulla loro estensione e infine sugli effetti nella sfera del lavoratore.

[22] V. I. AJUNWA, K. CRAWFORD, J. SCHULZ (2017), "Limitless Worker Surveillance", *California Law Review*, vol. 105 n. 6, p. 109, California Law Review

Tradizionalmente, al datore di lavoro vengono riconosciuti dalla dottrina un potere direttivo, un potere di controllo e un potere disciplinare[23].

Attraverso il MAA, è possibile aumentare l'estensione di ciascuno di questi tre poteri, nel senso di incrementarne la pervasività e ridurre i tempi e i costi necessari all'esercizio.

Questo è particolarmente evidente per quanto riguarda il controllo sui dipendenti, che ha sempre incontrato dei limiti di natura tecnologica ed economica prima ancora che legale: sorvegliare ogni dipendente in ogni momento della sua giornata lavorativa avrebbe richiesto delle risorse enormi e sarebbe comunque risultato estremamente difficoltoso e inefficiente[24].

Oggi, il numero di tecniche messe a disposizione dall'analisi automatizzata dei dati raccolti sul posto di lavoro supera in larga parte i tradizionali limiti tecnici ed economici e rende possibili una serie di attività di sorveglianza che, di fatto, si possono in astratto estendere non solo alla produttività del dipendente, ma anche al suo comportamento sul posto di lavoro e, in parte, nella vita privata, e addirittura alle caratteristiche personali[25].

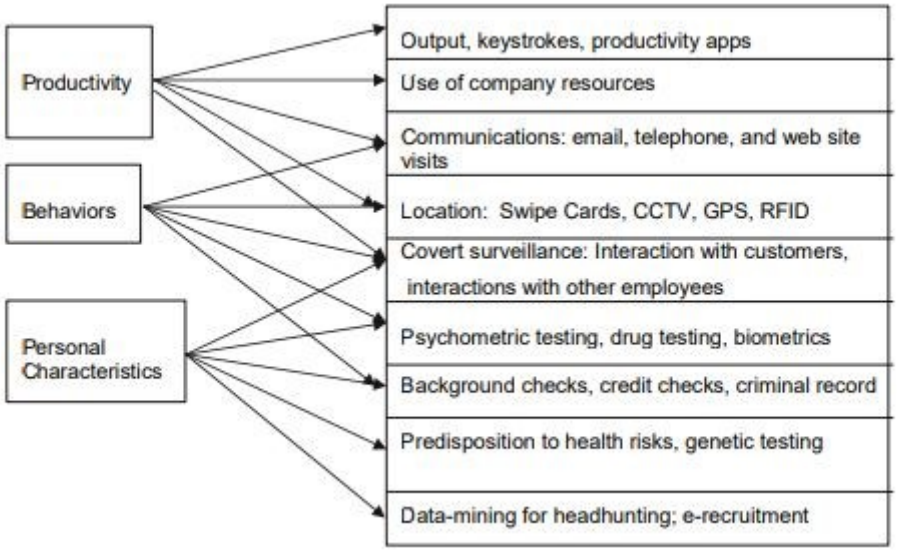

Immagine 1: modalità di controllo del lavoratore in un ambiente di lavoro digitalizzato. Tratta da I. AJUNWA (2017), cit., p. 111.

[23] Tra i molti, v. O. MAZZOTTA (2019), *Diritto del lavoro*, Giuffré.
[24] V. I AJUNWA et al. (2017), cit., pp. 107-108.
[25] V. K. BALL (2010), "Workplace surveillance: an overview", *Labor History*, vol. 51 n. 1, pp. 87-106, Routledge.

Le tecnologie basate su algoritmi, in particolare, possono essere descritte come più esaustive, istantanee, interattive e meno trasparenti delle tecnologie precedenti[26].

Questo significa, innanzi tutto, che le informazioni raccolte nell'attività di controllo sono ricavate da un maggior numero di dati provenienti da un maggior numero di fonti: è tecnicamente possibile rilevare la posizione dei dipendenti nello spazio tramite telecamere e sensori RFID[27], il loro movimento tramite gli accelerometri presenti negli smartphone aziendali, addirittura il loro umore a partire dall'analisi dei testi delle mail o del tono di voce nelle conversazioni.

In secondo luogo, data l'alta velocità di elaborazione dei dati nell'algoritmo, le informazioni sul personale sono disponibili in tempi brevissimi e il meccanismo di feedback rispetto alle direttive datoriali può essere pressoché immediato.

Il management attraverso algoritmi, poi, può aumentare l'interattività, nel senso di permettere al datore di lavoro di intervenire e adattare via via le proprie direttive sulla base delle informazioni rese in tempo reale, come appena visto.

Infine, in virtù delle loro caratteristiche peculiari, gli algoritmi possono diminuire il livello di trasparenza delle decisioni assunte in quanto potrebbe essere più difficoltoso individuare i criteri su cui si basano le procedure. Questo avviene sia poiché nella maggior parte dei casi il codice degli algoritmi usati per il management di lavoratori è protetto dal diritto d'autore, sia poiché, anche una volta reso accessibile, esso richiede un elevato livello di competenze per essere effettivamente compreso[28]. Ulteriori questioni, il cui esame sarebbe impossibile in questa sede, sorgono nei casi di tecnologie di *machine learning*[29].

---

[26] V. K. KELLOGG et al. (2020), cit., p. 371.

[27] Per RFID, o "Radio Frequency Identification", si intende una tecnologia che permette di individuare la posizione nello spazio di un sensore mediante segnali radio. La tecnologia si compone da un lato di almeno un sensore, o *etichetta*, che contiene informazioni sull'oggetto o sulla persona a cui viene applicato, dall'altro di un lettore che permette di captare i segnali radio e interpretarli – voce "RFID", *Enciclopedia on line Treccani*, consultato il 18/9/2021 all'indirizzo https://treccani.it/enciclopedia/rfid/. Sul posto di lavoro, per esempio, è possibile inserire un'*etichetta* RFID nei badge dei dipendenti e ottenere in tempo reale informazioni sulla loro ubicazione.

[28] *Ibid.*, pp. 371-372.

[29] In termini molto generali, si può definire "machine learning" quella branca della scienza informatica che ha lo scopo di "dare ai computer l'abilità di imparare senza essere esplicitamente programmati" – A. SAMUEL (1967), "Some studies in machine learning using the game of checkers", *IBM Journal*, pp. 601-617. Nell'ambito dell'analisi dei dati, il machine learning viene usato per costruire modelli complessi in grado di individuare "pattern" a parire dai dati e predire gli eventi futuri. Sul tema, v. G.

I cambiamenti che il management attraverso algoritmi è potenzialmente in grado di imprimere alle modalità di esercizio dei poteri datoriali, tuttavia, non sono solamente di tipo quantitativo, bensì anche qualitativo: il datore di lavoro, cioè, ha a disposizione sia modalità tradizionali di direzione, controllo e disciplina tradizionali ma potenziate e ampliate dall'uso di algoritmi, sia modalità completamente nuove che non sarebbero state in precedenza possibili.

Gli studi a questo proposito sono ancora piuttosto pionieristici, ma ad oggi un contributo fondamentale deriva dall'opera di Katherine Kellogg[30]. Secondo questo lavoro, che si pone nella prospettiva dello studio dell'organizzazione aziendale, il management attraverso algoritmi contribuisce a ridisegnare ciascuno dei tre ambiti di esercizio del potere datoriale.

Per quanto riguarda il potere direttivo, gli algoritmi permettono innanzi tutto meccanismi di *raccomandazione*, con i quali il lavoratore viene indirizzato verso una determinata modalità di adempimento della prestazione desiderata dal datore attraverso indicazioni fornite in tempo reale, sulla base dei dati raccolti. Il potere direttivo può essere automatizzato nel senso che le direttive fornite al dipendente non provengono più solo dal suo superiore, ma anche da un algoritmo. Nella pratica, spesso le indicazioni assumono la forma del *nudging*[31], risultando così non sempre facilmente individuabili e, soprattutto, non immediatamente discutibili, a differenza di quanto avverrebbe nel caso di un superiore in carne ed ossa.

Una seconda tecnica introdotta dal MAA è la *restrizione*, che consiste, in sintesi, nel ritenere determinate informazioni dal lavoratore per indirizzarne la condotta verso una determinata modalità. Se il principio di fondo non è sostanzialmente diverso da ciò che normalmente può avvenire in qualsiasi organizzazione aziendale "tradizionale", tuttavia l'istantaneità degli algoritmi permette che la scelta su quali elementi restringere e quali no avvenga, ancora una volta, in automatico e in tempo reale.

Per quanto riguarda il potere di controllo, un primo elemento di novità è dato dalla *registrazione*, ovvero dalla possibilità di registrare in ogni momento diversi aspetti relativi all'attività del lavoratore. A differenza di quanto accade con i

---

MALGIERI, G. COMANDÉ (2017), "Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation", *International Data Privacy Law*, vol. 7 n. 4, pp. 243-265, OUP.

30 In particolare, si veda K. KELLOGG et al. (2020), cit.

31 L'elaborazione del concetto si deve a R. H. THALER, C. R. SUNSTEIN (2009), *Nudge: Improving decisions about health, wealth, and happiness*, Penguin.

sistemi di controllo umano, quando questa funzione è affidata a un algoritmo esso è in grado di combinare enormi moli di dati provenienti da fonti differenti e di restituire informazioni in tempo reale al datore di lavoro.

Un altro strumento che sta emergendo sempre più nella pratica del MAA è il cd. *rating*[32]. Si tratta di uno degli elementi caratterizzanti del lavoro tramite piattaforma, che tuttavia, a ben vedere, potrebbe essere estesa anche ad ambienti di lavoro tradizionali: la prestazione del lavoratore viene valutata secondo dei parametri predefiniti, viene attribuito un punteggio e viene stilata una classifica dei lavoratori sulla base di tale punteggio. Il *rating*, quindi, costituisce una valutazione del lavoratore standardizzata[33], che tuttavia permette di aggregare dati oggettivi sulla produttività e giudizi soggettivi da parte dei superiori e soprattutto da parte dei clienti. Esso, nelle intenzioni dei suoi sostenitori, non solo permette di ottenere valutazioni omogenee e quindi confrontabili tra loro, ma è costantemente aggiornato sulla base dei dati analizzati e permette una stima predittiva sul comportamento futuro del dipendente[34].

Per quanto riguarda il potere di disciplina, è stato ampiamente studiato nell'ambito del lavoro tramite piattaforme il fenomeno della *sostituzione*: in un mercato del lavoro estremamente fluido, gli algoritmi permettono in tempi estremamente rapidi di licenziare (o, per quanto riguarda le piattaforme, *disattivare* l'account di) un dipendente la cui prestazione non raggiunge il livello desiderato e subito assumerne (registrare un nuovo utente) un altro al suo posto, sostituendolo[35]. Questo può avvenire alla condizione che le mansioni concretamente svolte dal lavoratore siano piuttosto elementari e non richiedano una particolare formazione – si parla in proposito di *uberizzazione* del lavoro[36] – e che, naturalmente, la legislazione lavoristica lo preveda.

Le piattaforme possono raggiungere questo risultato, esercitando di fatto un potere disciplinare sul lavoratore minacciato di licenziamento, poiché una

---

32 Per i primi studi in materia, v. D. KARREMAN, M. ALVESSON (2004) "Cages in tandem: Management control, social identity, and identification in a knowledge-intensive firm", *Organization*, vol. 11 n. 1, pp. 149–175.

33 K. LEVI, S. BAROCAS (2018), "Refractive Surveillance: Monitoring Customers to Manage Workers", *International Journal of Communication*, vol. 12, pp. 1166–1188.

34 V. K. KELLOGG et al. (2020), cit., p. 378.

35 Sul tema, v., tra gli altri, V. DE STEFANO (2016), cit.

36 V. R. Waters, "Transformation is crucial when digital disruption is the norm", *Financial Times* 30/9/2015; in ambito accademico, v. S. NERINCKX (2016), "The 'Uberization' of the Labour Market: Some Thoughts from an Employment Law Perspective on the Collaborative Economy", *ERA Forum*, vol. 17 n. 2 p. 245.

valutazione della produttività può essere svolta in automatico e in tempo reale, così come la registrazione di nuovi utenti avviene con una velocità che non sarebbe immaginabile in un contesto tradizionale. Se l'estensione ai posti di lavoro *standard* delle tecniche di sostituzione sia legittima sotto l'attuale normativa lavoristica è assai discutibile, ma rimane il fatto che le aziende possono, da un punto di vista meramente tecnico, sfruttare le tecniche di registrazione e rating per valutare il dipendente in tempo reale ed eventualmente giungere alla decisione di licenziarlo, così come possono utilizzare (e utilizzano sempre più spesso) algoritmi nella fase di selezione del nuovo personale, soprattutto per quanto riguarda l'analisi dei curricula.

Infine, una nuova modalità di esercizio del potere disciplinare riguarda la *premiazione*. Attraverso gli algoritmi, la prestazione di un determinato lavoratore, valutata come particolarmente positiva, viene premiata in maniera dinamica e interattiva attraverso aumenti salariali, promozioni, miglioramenti, turnazione più favorevole, etc. Questa modalità di esercizio del potere datoriale è spesso, anche se non necessariamente, legata al fenomeno della cd. *gamification*, ovvero della tendenza a creare un sistema di incentivi sul posto di lavoro improntato alla competizione e con caratteristiche del mondo dei videogiochi[37]. Anche in questo caso, senza un algoritmo che gestisca in automatico il sistema degli incentivi e i "giochi" sarebbe sostanzialmente impossibile ottenere un effetto così pervasivo e a costi così contenuti da giungere a poter modificare il contenuto stesso della prestazione di lavoro[38].

Ciascuna di queste nuove modalità di esercizio dei poteri datoriali è generalmente presente nella *gig economy*, e anzi si può dire che elementi come il *rating* e la sostituzione ne costituiscono un elemento fondamentale. Il lavoro nella *gig economy* ha costituito un importante opportunità di mettere alla prova nella pratica le potenzialità del management attraverso algoritmi, ma va riconosciuto che si tratta in buona parte di lavori che godono di scarsa - o in alcuni casi nulla - protezione da parte del diritto del lavoro, in Europa e forse ancor più negli Stati Uniti.

Ciò che, ancora una volta, preme sottolineare è che le innovazioni portate sul posto di lavoro dagli algoritmi non si limitano a questi lavori ma hanno, per diversi aspetti, il potenziale per essere applicate a molti posti di lavoro

[37] T. W. KIM (2018), "Gamification of Labor and the Charge of Exploitation", *Journal of Business Ethics*, vol. 152, pp. 27-39.
[38] Prime riflessioni in tal senso si possono leggere in D. EDERY, E. MOLLICK (2009), *Changing the game: How video games are transforming the future of business*., FT Press.

tradizionali, con grosse preoccupazioni per la qualità della vita e per i diritti dei lavoratori.

3. Il management attraverso algoritmi come fenomeno trasversale

Come si è in più occasioni accennato, quindi, il management attraverso algoritmi può essere considerato un fenomeno trasversale, secondo due diverse accezioni del termine: da un lato, esso può trovare applicazione non solamente nei nuovi lavori della *gig economy*, ma anche in moltissimi posti di lavoro tradizionali di settori economici diversi, dall'industria alla vendita al dettaglio, dai servizi alle professioni intellettuali, dai lavori a reddito più basso a quelli a più alta specializzazione. Dall'altro lato, si può facilmente intuire come tecniche diverse di MAA possano essere introdotte in ogni fase del rapporto di lavoro: dalla fase formativa, alla fase esecutiva, all'estinzione.

Con riferimento alla trasversalità tra settori economici e tipologie di lavoro, va notato come da subito il management attraverso algoritmi non sia stato prerogativa esclusiva dal lavoro tramite piattaforma. Tracciare una cronologia dell'implementazione di questo tipo di tecnologie negli ambienti di lavoro sarebbe sostanzialmente impossibile, ma vale la pena provare a fornire alcune coordinate orientative.

Innanzi tutto, sistemi di controllo elettronico della prestazione sono largamente utilizzati da diverso tempo nei contesti più disparati almeno dall'inizio del nuovo millennio[39] e, anzi, hanno da subito trovato terreno d'elezione nel contesto di lavori "da colletto bianco" nel settore terziario[40], in particolare nei Paesi anglosassoni. Come detto più sopra, non si trattava necessariamente di processi automatizzati, in particolare nei primi casi di applicazione di queste tecnologie. Tuttavia, il dato è indicativo del favore con cui i datori di lavoro guardano a sistemi che permettano di aumentare il controllo sulla prestazione

[39] Ma il controllo dei lavoratori dei call center con strumenti digitali è stata studiata in profondità dagli psicologi già nella prima metà degli anni '90: v. J. AIELLO (1993), "Computer Monitoring of Work Performance: Extending the Social Facilitation Framework to Electronic Presence", *Journal of Applied Social Psychology*, vol. 23 n. 7, pp. 537-548.

[40] R. BLANPAIN, M. VAN GESTEL (2004), *Use and Monitoring of E-Mail, Intranet and Internet Facilities at Work*, Kluwer Law International.

di lavoro, anche nei settori più avanzati dell'economia e con riguardo ai lavori relativamente meglio pagati[41].

Prima ancora che la *gig economy* prendesse piede, tuttavia, alcune aziende nel settore della logistica avevano avviato dei programmi di controllo a distanza che impiegavano tecniche di management attraverso algoritmi in senso stretto: UPS, che fornisce servizi postali negli Stati Uniti e in molti altri Paesi, già nel 2009 (anno di fondazione di Uber) aveva fornito tutti i propri furgoni di sensori in grado di rilevare le prestazioni alla guida dei propri autisti e l'esatta posizione attraverso GPS: il sistema era stato introdotto per aumentare la sicurezza dei dipendenti, e forniva ai manager locali informazioni sui casi di eccesso di velocità o di guida senza cintura, che erano poi utilizzati come base per esercitare il potere disciplinare[42]. Tuttavia, con i dati ottenuti UPS è stata in grado di ottimizzare i percorsi e i protocolli per la consegna dei pacchi, e nel giro di pochi anni è riuscita ad aumentare il numero di consegne mediamente effettuate in un turno di lavoro, diminuendo allo stesso tempo gli infortuni sul lavoro, il carburante utilizzato e i chilometri percorsi dai suoi mezzi[43].

Sempre nella logistica, è noto da tempo l'uso su vasta scala da parte di Amazon di strumenti digitali che permettono di guidare i lavoratori nei magazzini, assegnare volta per volta la mansione specifica e, soprattutto, registrare i dati sulla prestazione[44].

Il settore del commercio al dettaglio è uno dei più esposti al potenziale espansivo del management attraverso algoritmi, con le grandi aziende in cerca di nuove strategie per massimizzare le vendite: così, le catene di negozi hanno iniziato a utilizzare i dati sulle connessioni alla propria rete wi-fi non solo dei clienti, ma anche dei dipendenti, per monitorarne in ogni momento la posizione nello spazio[45].

Addirittura, strumenti di controllo digitale sono stati documentati anche con riferimento al settore agricolo, con i lavoratori stagionali identificati addirittura

---

41 V. V. DE STEFANO (2018), "Negotiating the Algorithm: Automation, artificial intelligence and labour protection", Employment Working Paper n. 246, p. 8.
42 E. Kaplan, "The Spy who Fired Me: The Human Costs of Workplace Monitoring", *Harper's Magazine* 3/2015, p. 32. Vedi anche *infra*, par. 5.
43 *Ibid.*, p. 33.
44 C. Baraniuk, "How algorithms run Amazon's warehouses", *BBC Future*, 18/8/2015, consultato il 20/8/2021 all'indirizzo https://www.bbc.com/future/article/20150818-how-algorithms-run-amazons-warehouses.
45 K. LEVI, S. BAROCAS (2018), cit.

tramite dati biometrici e sorvegliati e indirizzati con braccialetti digitali, in maniera simile ai dipendenti dei magazzini Amazon[46].

Da questi pochi esempi, appare evidente come al di fuori dell'ambito della *gig economy* siano già moltissimi i settori dove, con modalità naturalmente diverse tra loro, le aziende hanno ritenuto conveniente adottare strumenti di management attraverso algoritmi, e si può immaginare che nei prossimi anni questa tendenza proseguirà[47]. Inoltre, la diffusione di queste tecnologie non riguarda solo le grandi aziende, ma anzi promette proprio alle imprese più piccole di incrementare la loro efficienza raggiungendo con costi relativamente contenuti livelli di precisione del management prima impensabili[48].

Un altro senso in cui il potenziale di diffusione del management attraverso algoritmi è trasversale riguarda i diversi momenti del rapporto di lavoro. Una possibile chiave di lettura di questo fenomeno è la condizione di informazione imperfetta sul mercato del lavoro e di asimmetria informativa nel rapporto di lavoro[49]. I mercati del lavoro, cioè, soffrono un'inevitabile inefficienza dovuta all'imperfetta informazione riguardo a chi sono e dove si trovano i lavoratori idonei alle mansioni richieste e alle opportunità di lavoro offerte: soprattutto per alcuni settori, dove sono richiesti lavoratori più specializzati[50], questo può comportare un costo anche molto rilevante per l'azienda.

Per quanto riguarda la fase formativa, allora, una delle prime applicazioni estensive del MAA ha riguardato l'analisi e il filtro dei curriculum da parte delle grandi aziende: in una prima selezione, sempre più aziende affidano la scrematura dei candidati ad algoritmi di analisi testuale che, attraverso tecnologie predittive, selezionano i curriculum con le maggiori possibilità di risultare adatti per la posizione pubblicizzata e li classificano secondo un ordine di preferenza[51]. In alcuni casi, la stessa tecnologia viene utilizzata nella direzione opposta per personalizzare la comunicazione pubblicitaria nei confronti dei

---

[46] C. Ramsaroop (2019), "Reality Check 101: Rethinking the impact of automation and surveillance on farm workers", sul blog *Data & Society: Points*, https://medium.com/@ramsaroopchris?p=c6e501c3b9a3

[47] Peraltro, la pandemia da Covid-19 ha quasi certamente accelerato questa tendenza con riguardo al controllo sullo smart working: v. B. CARUSO (2020), "Tra lasciti e rovine della pandemia: più o meno smart working?", in *Rivista Italiana di Diritto del Lavoro*, n. 2.

[48] B. WABER (2013), *People Analytics*, Pearson, p. 178.

[49] In questa direzione muove A. ADAMS (2018), "Technology and the labour market: the assessment", *Oxford Review of Economic Policy*, vol. 34, n. 3, pp. 355 e sgg.

[50] B. HERSHBEIN, L. B. KAHN (2018), "Do Recessions Accelerate Routine-Biased Technological Change? Evidence from Vacancy Postings", *American Economic Review*, vol. 108 n. 7, p. 1743.

[51] K. CRAWFORD et al. (2019), *AI Now 2019 Report*, NYU, p. 17.

potenziali candidati, operando di fatto una sorta di selezione all'origine, basata sul risultato atteso dall'algoritmo medesimo[52]. Entrambe queste applicazioni coinvolgono, a ben vedere, un momento immediatamente precedente all'inizio del rapporto di lavoro e sono volte a contenere i costi di informazione che tradizionalmente sostengono le aziende nella fase di assunzione del personale.

È tuttavia sulla fase esecutiva che si concentra la maggior parte dei possibili impieghi di tecniche di management attraverso algoritmi: qui, infatti, è strutturalmente presente un'asimmetria tra le informazioni in possesso del lavoratore e quelle in possesso del datore riguardo alle abilità e alla qualità del lavoro svolto, che è interesse del datore rimuovere o limitare il più possibile. Soprattutto nella fase iniziale del rapporto di lavoro, una valutazione realistica sulle qualità del dipendente, con i mezzi tradizionali, è estremamente difficoltosa; il management attraverso algoritmi, invece, promette di ottenere in tempi brevissimi il maggior numero di informazioni sulla prestazione e prevederne i risultati futuri attraverso l'analisi automatizzata dei dati.

Va detto che non è questo l'unico motivo per cui le aziende sono interessate ad adottare le nuove tecnologie sul posto di lavoro: esse, infatti, come mostrato nel par. 2, rendono possibili nuove forme di direzione, controllo e disciplina dei lavoratori che dovrebbero comportare un efficientamento della produzione e una riduzione dei costi. Anche quando le tecniche di MAA si limitano ad ampliare i poteri nelle forme in cui sono già attualmente esercitati (per esempio automatizzando il controllo sulle mail aziendali attraverso algoritmi di analisi testuale), comunque lo scopo è quello di aumentare l'efficienza del lavoro del manager preposto a tali attività (rimanendo sullo stesso esempio, si evita al manager di leggere tutte le mail alla ricerca di comportamenti illeciti e viene risparmiate ore lavorate).

Per quanto riguarda la fase estintiva, essa è gestita senza intermediazioni dall'algoritmo in molte applicazioni di lavoro tramite piattaforma[53]. Questo è possibile poiché i lavoratori sono qualificati come autonomi e non si tratta di un licenziamento in senso stretto, che in ogni ordinamento richiede presupposti e forme più o meno gravosi: la piattaforma, constatato lo scarso rendimento da

[52] D. GREENE, I. AJUNWA (2017), "Automated Hiring Platforms as Technological Intermediaries and Brokers," in S. VALLAS, A. KOVALAINEN (2019), *Work and Labor in the Digital Age*, Emerald.
[53] A. ROSENBLAT, L. STARK (2016), "Algorithmic labor and information asymmetries: A case study of Uber drivers", *International Journal of Communication*, vol. 10, pp. 3758–3784.

parte del prestatore, si limita a disattivare il suo account e non farlo più accedere ad opportunità di lavoro.

Un utilizzo così estremo degli algoritmi nella fase estintiva del rapporto non è permessa dalla legge nel contesto italiano[54], ma le esigenze di efficienza del datore di lavoro possono comunque essere in parte soddisfatte. È infatti chiaro che un licenziamento per giustificato motivo soggettivo può essere giustificato per lo scarso rendimento del lavoratore, misurato attraverso un'elaborazione algoritmica dei dati rilevati da varie fonti e magari organizzati secondo un sistema di *rating*. Allo stesso modo, una condotta illecita potrebbe essere rilevata in automatico da sistemi di MAA che incidono sul potere di controllo e condurre infine a un licenziamento disciplinare. Va comunque precisato che, nell'ordinamento italiano, il licenziamento disciplinare è sottoposto alle garanzie procedurali dell'art. 7 dello Statuto dei Lavoratori[55]: sarebbe così necessario da parte del datore adempiere preventivamente a specifici obblighi informativi e, in ogni caso, andrebbero osservati termini a vantaggio del dipendente.

In questi casi, non sarebbe il licenziamento in sé ad essere automatizzato ed affidato agli algoritmi, bensì una parte del processo decisionale sottostante. Il datore di lavoro, cioè, baserebbe la propria scelta di procedere all'estinzione del rapporto di lavoro anche sulla base delle risultanze degli algoritmi adottati sul posto di lavoro[56].

Un simile scenario è indubbiamente inquietante e va osservato con giusta preoccupazione, ma i rischi legati all'applicazione di strumenti di management attraverso algoritmi non riguardano solamente il licenziamento automatizzato (c.d. *robo-firing* nel contesto anglosassone).

4. Il possibile impatto sul lavoro

È evidente come a una così varia gamma di possibili impieghi di algoritmi in ambienti lavorativi, in settori così diversi e con riguardo a fasi diverse del rapporto di lavoro, i possibili impatti sui lavoratori delle nuove tecnologie adottate è difficile da sintetizzare. Vale tuttavia la pena di individuare alcune direttrici su cui si è concentrata la ricerca scientifica, non solo nel campo del

[54] V. *infra*, cap. 2.
[55] V. M. TREMOLADA (1993), *Il licenziamento disciplinare*, CEDAM.
[56] J. ADAMS-PRASSL (2019), cit., p. 14.

diritto ma anche per quanto riguarda gli studi sociologici, economici e manageriali.

Va anzitutto evidenziato come le possibili implicazioni degli algoritmi nella gestione delle risorse umane[57] possono essere positive non solo dal punto di vista dell'azienda ma, talvolta e a certe condizioni, anche da quello del lavoratore. Per esempio, un sistema di valutazione della prestazione automatizzata basato su parametri certi e condivisi anche dai dipendenti, magari attraverso la mediazione delle organizzazioni sindacali, potrebbe aiutare a ridurre l'arbitrarietà dei giudizi forniti dai manager, così come un sistema di gestione della turnazione che tenga in considerazione le esigenze di volta in volta espresse dai lavoratori e garantisca sempre l'organizzazione ottimale delle risorse potrebbe migliorare l'equilibrio vita-lavoro.

Gli aspetti problematici, tuttavia, sono molteplici e riguardano diversi aspetti del rapporto di lavoro.

Innanzi tutto, l'uso intensivo di management attraverso algoritmi può produrre un peggioramento dell'esperienza dei dipendenti e un deterioramento dell'ambiente di lavoro. L'esercizio automatizzato di potere direttivo può risultare estremamente frustrante per il lavoratore: le decisioni prese dall'algoritmo si basano, generalmente, su modelli e inferenze tratti dai dati a disposizione e non su un vero e proprio percorso logico argomentabile, come quello che adopererebbe un manager in carne ed ossa[58]. L'impossibilità di comprendere la logica dietro alle direttive, e l'impossibilità di discuterle direttamente con il proprio superiore, comporta da un lato confusione e frustrazione e dall'altro un senso di alienazione dato dalla percezione di fungere come da strumento esecutore di un'intelligenza artificiale spesso imperscrutabile[59]. Questo, insieme alle tecniche di restrizione, rende più difficoltose le occasioni di interazione tra colleghi e con i superiori, diminuendo per i lavoratori le possibilità di esporre il proprio punto di vista e di intrattenere una sana vita sociale anche nell'orario di lavoro[60].

---

[57] Per ragioni di spazio la ricerca è limitata a questo aspetto, ma non si può certo ignorare l'impatto che gli algoritmi in generale, a partire dall'uso di AI nei processi produttivi, hanno e avranno sul mondo del lavoro: v. E. ERNST (2018), "The economics of artificial intelligence: Implications for the future of work", *ILO Future of work research paper series*.

[58] M. VALENTINE, R. HINDS (2021), "'Rolling Up the Leaf Node' To New Levels of Analysis: How Algorithmic Decision-Making Changes Roles, Hierarchies, and Org Charts", *Stanford Engineering WP*.

[59] J. DANAHER (2016), "The threat of algocracy: Reality, resistance and accommodation", *Philosophy & Technology*, vol. 29 n. 3, pp. 245–268.

[60] A. ROSENBLAT, L. STARK (2016), cit.

Anche per quanto riguarda il potere di controllo, la percezione di essere costantemente soggetti a sorveglianza può portare i lavoratori a stravolgere la propria condotta in funzione delle aspettative del soggetto sorvegliante[61]. Allo stesso tempo, se il dipendente dovesse dubitare dell'accuratezza dei dati raccolti, consapevole che verranno usati nella valutazione della sua prestazione, questo potrebbe ancora una volta aumentare il senso di frustrazione e di sfiducia nei confronti dell'ambiente di lavoro.

Per quanto riguarda il potere disciplinare, infine, è del tutto evidente che la possibilità di subire ripercussioni sulla base di una valutazione svolta da un algoritmo, con difficoltà nel contestare la decisione di fronte a un manager vero e proprio, crea un forte senso di precarietà e può sottoporre il lavoratore a un'enorme pressione, in grado di rendere l'ambiente di lavoro inospitale[62]. Dall'altro lato, un sistema premiale che presenta meccanismi di funzionamento sconosciuti ai lavoratori e che restituisce esiti incomprensibili è garanzia di frustrazione e di alienazione rispetto alla qualità del proprio lavoro.

Un secondo fronte su cui possono agire i sistemi di management attraverso algoritmi riguarda l'equilibrio vita-lavoro dei dipendenti. Se già da anni è presente una tendenza all'assottigliamento del confine tra la vita privata e quella professionale, accentuata dal lavoro da casa durante la pandemia di Covid-19[63], tale fenomeno rischia di essere radicalizzato dalle nuove tecnologie.

La possibilità di impartire direttive ai lavoratori e di rendere la prestazione a distanza in molti settori, soprattutto per quanto riguarda i servizi, permette una notevole flessibilità con riguardo al luogo e al tempo di lavoro. Nei casi di smart working, per esempio, il dipendente non solo può essere raggiunto in ogni

---

[61] S. AHMED et al. (2016), "Peer-to-peer in the Workplace: A View from the Road", presentato alla CHI Conference on Human Factors in Computing Systems.

[62] V., per un esame approfondito dei risvolti psicologici dell'automazione del potere disciplinare, lo studio di M. GRAHAM, I. HJORTH, V. LEHDONVIRTA (2017), "Digital labour and development: Impacts of global digital labour platforms and the gig economy on worker livelihoods", *Transfer: European Review of Labour and Research*, vol. 23 n. 2, pp. 135–162. Dalla cronaca, anche in Italia, giungono segnali simili: sulle conseguenze della sorveglianza costante sull'ambiente di lavoro nella logistica, v. tra i molti S. Morosi, "Amazon brevetta il braccialetto elettronico che controlla i lavoratori: scoppia la polemica", *Corriere della Sera*, 1/2/2018, consultato online il 20/8/2021 all'indirizzo https://www.corriere.it/cronache/18_febbraio_01/amazon-brevetta-braccialetto-elettronico-che-controlla-lavoratori-scoppia-polemica-6eacf7d2-0760-11e8-8886-af603f13b52a.shtml.
V., infine, A. ALOISI, V. DE STEFANO (2020), *Il tuo capo è un algoritmo: contro il lavoro disumano*, ed. Laterza, p. 73.

[63] R. PALUMBO (2020), "Let me go to the office! An investigation into the side effects of working from home on work-life balance", *International Journal of Public Sector Management*, vol. 33 n. 6/7, pp. 771-790.

momento e in ogni luogo dalle indicazioni del datore, ma spesso viene anche sorvegliato a distanza da sistemi di intelligenza artificiale. Ne consegue un rischio di intrusione del datore di lavoro anche nella sfera privata e familiare del dipendente, e un'erosione del concetto stesso di lavoro dipendente, con la garanzia di un orario fisso e di limiti temporali imposti dalla normativa: se la prestazione è resa, controllata, misurata e valutata a distanza, senza quindi necessità di una contemporanea presenza in un luogo diverso dall'abitazione del lavoratore, come si può garantire che il carico di lavoro rientri nei limiti legali e non divenga eccessivo[64]? Come si può evitare di comprimere la vita privata dei dipendenti?

L'assottigliamento della linea di demarcazione tra lavoro e vita privata si muove anche nella direzione opposta: i lavoratori potrebbero consultare con strumenti dell'azienda la propria mail personale oppure i profili social. Se l'uso del pc aziendale è costantemente sorvegliato, è immediatamente evidente la portata dell'intrusione che si può verificare nella vita privata del dipendente.

Un terzo possibile impatto degli algoritmi sulla vita dei lavoratori riguarda un possibile cambiamento della struttura stessa del lavoro e della sua organizzazione, in sintesi nota come *uberizzazione*. Un aspetto fondamentale riguarda la scomposizione della prestazione di lavoro in singoli *task*, compiti elementari di volta in volta assegnati dall'algoritmo che non richiedono al lavoratore alcuna sintesi. Si tratta di una sorta di parcellizzazione della mansione, un ritorno a un Taylorismo-Fordismo esasperato[65], in cui i lavoratori meno qualificati divengono meri esecutori materiali di pochi gesti coordinati fra loro. Questo fenomeno, come già accennato, oltre alle ovvie implicazioni sulla qualità del lavoro, solleva parecchi dubbi con riguardo al fortissimo rischio di precarizzazione che consegue alla facilità nel sostituire del lavoratore, ulteriormente aumentata dagli algoritmi di selezione del personale[66].

Il tema del rapporto tra tecnologia e lavoro umano non è certo nuovo ed è oggetto di studi approfonditi di diritto e sociologia del lavoro da diversi decenni[67]; i pericoli per la stabilità del rapporto di lavoro, in particolare, sono stati avvertiti anche prima che tecniche di management attraverso algoritmi venissero concretamente utilizzate. Tuttavia, l'impatto delle tecnologie digitali

---

64 C. DEGRYSE (2016) cit., p. 41.
65 F. W. TAYLOR (1911), *The Principles of Scientific Management*, Harper.
66 Come visto *supra*, par. 3.
67 AA. VV. (1986), *Rivoluzione tecnologica e diritto del lavoro: Atti dell'VIII Congresso di diritto del lavoro, Napoli, 12-14 aprile 1985*, Giuffré.

su questo specifico tema ha il potenziale per rivelarsi notevole, e va studiato con attenzione per evitare le conseguenza meno desiderabili[68].

Si è avuto modo di osservare l'uberizzazione del lavoro nella *gig economy* – così come le stesse tecnologie che permettono di suddividere il lavoro di fattorino o di autista in singoli *task* dalla durata di pochi minuti sono in astratto applicabili anche a molte situazioni di lavoro subordinato, protette dal diritto del lavoro.

Accanto a questo fenomeno si situa una tendenza diversa per quanto riguarda invece i lavoratori più specializzati: le nuove tecnologie, abbattendo i costi di informazione, permettono in certi casi di abbattere le pesanti strutture aziendali gerarchiche e di organizzare il lavoro dei professionisti per progetti, assegnando e gestendo i compiti nella squadra in maniera più fluida e valutando l'operato dei singoli attraverso metriche più raffinate di quelle disponibili in passato[69].

Le conseguenze dell'uberizzazione, se portata alle estreme conseguenze, potrebbero essere enormi: si tratterebbe di un cambiamento del concetto stesso di lavoro, con un impatto sociale difficilmente prevedibile ma difficilmente positivo. La possibilità di abbandonare strutture gerarchiche dell'ambiente di lavoro, invece, è più spesso vista con favore e potrebbe avere effetti benefici sia con riguardo all'efficienza dell'azienda, sia con riguardo alla qualità dei lavori così organizzati.

Per quello che più interessa il giurista, però, due sono le conseguenze più preoccupanti del management attraverso algoritmi: la possibilità di produrre discriminazioni sul posto di lavoro e i problemi di privacy e di protezione dei dati personali dei dipendenti.

Per quanto riguarda il rischio di discriminazione, gli algoritmi in generale e quelli che operano nell'ambito della gestione del personale in particolare presentano dei profili di forte criticità. Da un lato, infatti, gli algoritmi sono comunque sempre programmati da esseri umani, i cui eventuali pregiudizi si trasferiscono nel codice da loro scritto[70]: è possibile che un algoritmo restituisca risultati

---

[68] V., per esempio, D. AUTOR (2013), "The 'task approach' to labor markets: an overview", *NBER Working Paper*, n. 18711; D. AUTOR, D. DORN (2013), "The growth of low-skill service jobs and the polarization of the US labour market", *American Economic Review*, vol. 103 n. 5, pp. 1553-1597; E. ANTHES (2017), "The shape of the work to come: Three ways that the digital revolution is reshaping workforces around the world", *Nature*, vol. 550, pp. 316-319.

[69] A. ADAMS (2018), cit., p. 358.

[70] "Algorithms are […] programmed by human beings, whose values are embedded into their software" - F. PASQUALE (2015), *The Black Box Society: The Secret Algorithms That Control Money and Information*, p. 38, Harvard University Press.

discriminatori poiché i parametri che prende in considerazione sono costruiti in modo da privilegiare una determinata categoria di persone su un'altra, verosimilmente secondo lo schema della discriminazione indiretta. Questo rischio immediatamente percepibile per quanto riguarda i sistemi impiegati nella selezione del personale, sia per l'analisi dei curriculum, sia per la pubblicità mirata ai potenziali candidati.

Dall'altro lato, l'output degli algoritmi dipende strettamente dai dati che vengono inseriti: tali dati potrebbero riflettere il pregiudizio dei soggetti da cui sono stati raccolti, e condurre a loro volta a risultati discriminatori[71]. In questo senso, i sistemi di rating sono particolarmente problematici, soprattutto quando tutta o parte della valutazione proviene dai clienti, quindi da soggetti esterni al rapporto di lavoro.

Quel che è peggio, l'algoritmo risulta nella maggior parte dei casi una sorta di "scatola nera", per cui il codice è protetto da diritto d'autore e non è disponibile per il destinatario delle decisioni[72], e anche quando lo fosse non sarebbe intellegibile se non a esperti del settore[73]. Diventa di conseguenza molto difficile per i lavoratori anche avere l'effettiva certezza di subire una condotta discriminatoria e, soprattutto, di poterla provare in giudizio[74].

Infine, ogni uso di algoritmi sul posto di lavoro solleva problemi di privacy in quanto, come appena detto, ogni algoritmo necessita di molti dati per poter funzionare. Questi dati, quando utilizzati per applicazioni di MAA, provengono spesso dai lavoratori stessi[75] e in molti casi si tratta di dati personali, ovvero "qualsiasi informazione riguardante una persona fisica identificata o identificabile"[76]: la loro raccolta, conservazione e trattamento deve essere sempre bilanciata con il diritto del lavoratore alla riservatezza, come sarà elaborato oltre nel prosieguo di questa ricerca.

È tuttavia allarmante il fatto che sia possibile, grazie a sistemi basati su algoritmi predittivi, profilare i dipendenti senza utilizzare loro dati personali, bensì

---

71 S. BAROCAS, A. SELBST (2014), "Big data's disparate impact", *California Law Review*, vol. 104, pp. 671-732.
72 F. PASQUALE (2015), cit.
73 G. MALGIERI, G. COMANDÉ (2017), cit., pp. 243-265.
74 C. O'NEIL (2016), *Weapons of Math Destruction: how Big Data Increases Inequality and Threatens Democracy*, Crown
75 Ma non solo: v. K. LEVI, S. BAROCAS (2018), cit., nonché E. ALES et al. (2018), *Working in Digital and Smart Organizations*, Palgrave MacMillan, in particolare cap. 2.
76 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27/4/2016 (GDPR), art. 4 par. 1.

elaborando *proxy* e metadati di per sé anonimi[77], con la possibile conseguenza di eludere la disciplina nazionale ed europea sul trattamento dei dati personali.

Nella larghissima maggioranza dei contesti lavorativi, è probabile che i dipendenti non siano affatto consapevoli o non siano sufficientemente informati della natura delle informazioni che vengono raccolte dal datore, né soprattutto dello scopo per cui avviene tale raccolta[78]. A differenza del passato, in cui sistemi di sorveglianza erano nella maggior parte dei casi visibili e facilmente riconoscibili (principalmente impianti di videosorveglianza, che peraltro in Italia sono sottoposti al regime di pubblicità dell'art. 4 dello Statuto dei Lavoratori e in molti altri Paesi dell'Unione europea a previsioni normative simili), oggi una grande varietà di dati può essere raccolta dagli strumenti di lavoro più comuni, come i computer installati negli uffici e gli smartphone aziendali, nonché da sensori distribuiti nell'ambiente di lavoro, in particolare nel contesto delle cd. industrie 4.0[79].

Spesso i dati sono raccolti con lo scopo di aumentare l'efficienza dei processi produttivi, ma in un ambiente di lavoro in cui vengono estesamente adottati sistemi di registrazione[80] possono sorgere seri dubbi sull'effettiva portata dei dati acquisiti e sull'utilizzo che ne viene fatto nella valutazione dei dipendenti: viene valutata solo la produttività o anche caratteristiche personali dei lavoratori, come il loro stato di salute o certi profili psicologico-attitudinali[81]?

L'uso di dispositivi indossabili forniti direttamente dal datore di lavoro, come braccialetti, collanine e smartwatch, potrebbe essere fortemente incentivato o addirittura obbligatorio: in entrambi i casi, si potrebbe trattare di una notevole minaccia al diritto alla privacy dei lavoratori con riguardo a dati particolarmente sensibili come quelli sullo stato di salute e sulla posizione e, in ultima analisi, alla loro stessa autonomia e autodeterminazione[82].

Inoltre, un ulteriore aspetto critico è rappresentato dalle politiche di lavoro da casa e di "bring your own device" (o BYOD). Nel primo caso, infatti, il lavoratore utilizza generalmente uno strumento fornito dall'azienda,

---

77 V. K. CRAWFORD, J. SCHULTZ (2014), cit.
78 Article 29 Data Protection Working Party, "Opinion 2/2017 on data processing at work", p. 4, adottata l'8 giugno 2017, consultata online il 18/9/2021 all'indirizzo https://ec.europa.eu/newsroom/article29/items/610169.
79 V. E. ALES et al. (2018), cit.
80 Nel senso definito *supra*, par. 2.
81 M. ANTEBY, C. CHAN (2018), "A self-fulfilling cycle of coercive surveillance: Workers' invisibility practices and managerial justification", *Organization Science*, vol. 29 n. 2, pp. 247–263.
82 V. I. AJUNWA et al. (2017), cit., p. 132.

solitamente un computer, per rendere la prestazione lavorativa non nell'ordinario luogo di lavoro ma direttamente da casa propria. Se tuttavia la sua prestazione è controllata attraverso algoritmi che raccolgono dati direttamente dal pc, è possibile che tale attività di sorveglianza possa accidentalmente acquisire dati estranei alla prestazione, che riguardano la sfera privata del lavoratore[83].

Nel senso opposto, le politiche di BYOD – un altro elemento strutturale del lavoro tramite piattaforma – prevedono che il lavoratore renda la prestazione utilizzando come strumento di lavoro un proprio dispositivo, generalmente uno smartphone. Ma uno strumento personale, anche laddove utilizzato per adempiere al contratto di lavoro, è per definizione personale: dati come immagini, posizione nello spazio registrata con tecniche di geolocalizzazione e altri ancora, contenuti nel dispositivo, potrebbero entrare nel possesso del datore di lavoro[84] e con ciò ledere gravemente il diritto alla riservatezza del dipendente.

I profili legati alla riservatezza dei dipendenti sul posto di lavoro non sono certo nuovi al dibattito giuslavoristico[85]: basti pensare alla centralità dell'art. 4 dello Statuto dei Lavoratori e alla discussione seguita alla sua riforma nel 2016[86]. Tuttavia, la assoluta centralità che ricopre la raccolta dei dati personali senza i quali nessun sistema di management attraverso algoritmi potrebbe funzionare, porta a pensare che tale tematica acquisterà nei prossimi anni una posizione sempre più centrale nelle questioni di diritto del lavoro.

5. Il management attraverso algoritmi nella pratica

Nei precedenti paragrafi si è provato a definire il fenomeno del management attraverso algoritmi, se ne sono spiegate le ragioni di novità rispetto al rapporto di lavoro tradizionale, si è sostenuta la portata trasversale dell'adozione di tali

---

83 V. DE STEFANO (2020), "'Masters and Servers': Collective Labour Rights and Private Government in the Contemporary World of Work", *International Journal of Comparative Labour Law and Industrial Relations*, vol. 36 n. 4.

84 I. ALVINO (2016), "I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy", *Labour and Law Issues*, vol. 2 n. 1, p. 26 e sgg.; la stessa preoccupazione è mostrata nell'Article 29 DPWP, "Opinion 2/2017", cit., p. 16 e sgg.

85 R. DE LUCA TAMAJO et al. (1988), *Nuove tecnologie e tutela della riservatezza dei lavoratori*, Franco Angeli.

86 Tra i molti, M. T. CARINCI (2016), "Il controllo a distanza dell'attività del lavoratori dopo il "Jobs Act" (art. 23 D. Igs. 151/2015): spunti per un dibattito", *Labour and Law* Issues, vol. 2 n. 1.

tecniche sui posti di lavoro oggi esistenti e si sono accennati i cinque principali ambiti in cui sorgono e sorgeranno i profili più problematici.

Una tale trattazione teorica, tuttavia, non deve far perdere di vista il fatto che il management tramite algoritmi non è una possibilità da cui guardarsi per il futuro, bensì una realtà con cui abbiamo a che fare già oggi; e ancora, che non si tratta di un fenomeno che tocca solo gli Stati Uniti, da sempre più recettivi rispetto alle nuove tecnologie e in genere più restii a regolare nel dettaglio e limitare le prerogative datoriali, ma anche l'Unione europea e l'Italia.

Vale allora la pena provare a dar conto di alcuni casi di cronaca che, negli ultimi anni, hanno mostrato alcuni dei pericoli legati a questa nuova forma di gestione del personale.

Uno dei primi casi di impiego su vasta scala degli algoritmi sul lavoro, come accennato in precedenza[87], è rappresentato da UPS, che a partire dal 2009 ha iniziato a "cablare" i propri furgoni negli Stati Uniti con sensori e GPS e a dotare gli autisti di palmari da utilizzare per le consegne[88]. Queste tecnologie registrano un grande numero di dati legati alla guida del dipendente, al ritmo tenuto nelle consegne, agli eventuali comportamenti pericolosi come frenate improvvise e guida senza cintura.

Lo scopo è da subito stato duplice. Da un lato, un'azienda di consegne di grandissime dimensioni, come UPS, ha a che fare con margini anche molto sottili in termini di efficienza: riuscire a rendere anche solo minimamente più efficienti le operazioni ordinarie può significare un risparmio di decine di milioni di dollari a bilancio, al termine dell'anno fiscale. Per prendere le migliori decisioni al riguardo, tuttavia, sono necessarie statistiche affidabili – e quindi un numero enorme di dati – su ogni aspetto del lavoro degli autisti. Per raggiungere questo scopo sono necessarie tecnologie di *workforce analytics*, senza le quali sarebbe materialmente impossibile non solo analizzare ma anche raccogliere tali dati.

Questo è particolarmente evidente per quanto riguarda il cd. "problema del commesso viaggiatore", un problema di informatica teorica che trova applicazione pratica quando un soggetto deve determinare il percorso ottimale per raggiungere un certo numero di destinazioni a una data distanza tra loro[89] –

[87] V. *supra*, par. 3.
[88] E. Kaplan, "The spy who fired me", cit., p. 32.
[89] "Traveling salesman problem". *Encyclopedia Britannica*, consultato online il 20/8/2021 all'indirizzo https://www.britannica.com/science/traveling-salesman-problem.

come nel caso di un autista UPS. Solo grazie ai dati raccolti dai singoli furgoni è stato possibile per l'azienda elaborare un modello efficiente e in grado di adattarsi in tempo reale alle esigenze di ogni consegna, che suggerisce all'autista il percorso e l'ordine migliore durante il suo turno di lavoro[90].

La "Telematics" (così UPS ha battezzato il proprio sistema di *workforce analytics*) permette anche ai manager di ottenere statistiche sul singolo lavoratore, in tempo reale, e di esercitare direzione e controllo a distanza. Per esempio, attraverso la costante sorveglianza sulle misure di sicurezza, ora quasi il 99% degli autisti UPS indosserebbe la cintura di sicurezza mentre guida, secondo le dichiarazione dell'azienda[91]. Come però già detto in precedenza, il comportamento dei lavoratori tende a cambiare quando hanno la consapevolezza di essere costantemente controllati, e questo potrebbe avere conseguenze negative. In questo caso, poiché il tempo impiegato per le consegne viene registrato e confrontato a fine giornata tra i vari autisti, vengono riportati casi di lavoratori che per guadagnare tempo semplicemente allacciano la cintura dietro la schiena prima di sedersi alla guida, così restituendo un dato falso di adeguamento alle politiche aziendali ma allo stesso tempo mettendo a repentaglio la propria sicurezza[92].

Le statistiche, inoltre, sono valutate alla fine di ogni turno dal manager e hanno un certo peso sulla valutazione della prestazione; in ultima analisi, se il lavoratore non risponde ai parametri di efficienza, talvolta molto specifici[93], imposti dall'azienda, questi può essere licenziato per scarsa produttività.

Il caso di UPS può essere considerato un buon esempio dell'impatto della tecnologia su un ambiente di lavoro tradizionale: UPS ha applicato a un'attività che conduce da decenni, la consegna di pacchi a domicilio, sistemi di management attraverso algoritmi per aumentare l'efficienza del processo. Ci è riuscita: basti pensare che il numero di consegne che un singolo dipendente è in grado di effettuare durante un turno di lavoro è passato da meno di 100 a una media di 130. Le condizioni dei lavoratori, per quanto minacciate dall'innovazione, non sono però peggiorate: hanno ottenuto di non poter essere

[90] J. Goldstein, "The future of work looks like a UPS truck", podcast di National Public Radio, consultato online il 20/8/2021 all'indirizzo https://www.npr.org/ sections/money/2014/05/02/308640135/episode-536- the-future-of-work-looks-like-a-ups-truck.
[91] E. Kaplan, "The spy who fired me", cit., p. 34.
[92] *Ivi.*
[93] L'autista intervistato in J. Goldstein, "The future of work", cit., riferisce per esempio che un alto numero di retromarce innestate è considerato un importante indicatore di inefficienza e che la valutazione a fine giornata può essere molto frustrante.

licenziati esclusivamente sulla base dei dati ricavati dalla Telematics e vengono informati sul tipo di dati raccolti e sulla finalità del trattamento. Soprattutto, a fronte dell'aumento di produttività, hanno visto i propri salari raddoppiare tra il 1995 e il 2015. Tuttavia, va registrato come il caso di studio sia in realtà peculiare, almeno nel panorama americano: i lavoratori UPS sono altamente sindacalizzati e sono riusciti a fare fronte comune per governare il fenomeno del management attraverso algoritmi che li coinvolgeva; inoltre, essi la loro posizione contrattuale ha beneficiato del fatto che l'azienda non avrebbe potuto nemmeno volendo delocalizzare il loro lavoro[94].

La sorveglianza sugli autisti dei furgoni per le consegne, in effetti, può essere ancora più intrusiva: all'inizio del 2021, Amazon ha deciso di introdurre su tutti i suoi veicoli un sistema sviluppato da una terza parte, chiamato Driveri, che utilizza quattro telecamere indirizzate e coordinate dall'intelligenza artificiale per individuare, tramite algoritmi di machine learning, comportamenti rischiosi come distrazioni, eccesso di velocità e frenate troppo brusche e inviare un avvertimento all'autista. Una delle quattro telecamere inquadra costantemente il conducente e verifica, per esempio, che la cintura di sicurezza sia sempre allacciata[95].

Quando viene rilevato un comportamento pericoloso, in automatico il sistema emette un allarme verbale che intima al lavoratore di rallentare o di fare più attenzione. Con questo sistema, si prevede di ridurre il numero di incidenti di 1/3.

Anche a prescindere dall'immagine non lontana dalla distopia che una simile descrizione può prefigurare, non si può ignorare il forte rischio che la privacy dell'autista sia completamente travolta da un sistema così pervasivo di controllo e direzione. Amazon dichiara che il materiale filmato non è conservato se non su richiesta del lavoratore stesso o in specifiche condizioni di "rischio per la sicurezza", ma non è esattamente chiaro cosa si intenda con tale espressione e dubbi sul trattamento dei dati personali degli autisti rimangono irrisolti se non

[94] *Ivi.*

[95] T. Sonnemaker, "Amazon is deploying AI cameras to surveil delivery drivers '100% of the time'", *Business Insider*, 3/2/2021, consultato online il 20/8/2021 all'indirizzo https://www.businessinsider.com/amazon-plans-ai-cameras-surveil-delivery-drivers-netradyne-2021-2?r=US&IR=T.

aggravati dalla richiesta da parte dell'azienda di sottoscrivere una sorta di consenso al trattamento dei dati biometrici[96].

In effetti, la politica aziendale di Amazon è particolarmente incentrata sulla ricerca della massima efficienza e sull'uso dei dati per ottenere questo obiettivo[97]. Anche il lavoro all'interno dei magazzini dell'azienda è coinvolto dalle applicazioni del management attraverso algoritmi: è infatti un sistema automatizzato che attribuisce in tempo reale i compiti ai lavoratori e li guida verso la posizione del prodotto che devono spostare perché possa essere spedito. Tale sistema ha due immediate implicazioni: la prima è che la mansione del magazziniere viene quotidianamente e addirittura ogni ora scomposta in singoli compiti elementari – si tratta, cioè, di una forma piuttosto vistosa di parziale *uberizzazione*. La seconda è che il lavoratore dipende completamente dalla tecnologia per portare a termine il proprio lavoro, in quanto senza gli algoritmi non potrebbe né ricevere le istruzioni a un ritmo adeguato, né orientarsi nella controintuitiva organizzazione degli spazi interni[98].

Un caso tutto sommato simile a quello di UPS è avvenuto in Francia, quindi nell'Unione europea, con i tecnici degli ascensori Kone che sono stati dotati di telefoni aziendali e di un particolare strumento di lavoro, una sorta di cassetta degli attrezzi computerizzata in grado di intervenire sugli impianti e di registrare i dati dell'intervento e la posizione in tempo reale. Soprattutto, attraverso questo strumento il tecnico può scattare fotografie delle parti meccaniche su cui deve lavorare e ottenere direttamente le istruzioni su come svolgere la manutenzione, nonché elaborare un preventivo e farlo firmare al cliente, inserendo l'ordine nel sistema dell'azienda in tempo reale.

Della prestazione di lavoro dei tecnici Kone viene registrata e conservata una grande gamma di dati, a partire dagli orari in cui la "cassetta" è stata accesa: viene così preparata in automatico la busta paga del dipendente, tenendo conto anche di eventuali straordinari.

I tecnici, tuttavia, si lamentano del fatto che la sensazione di essere costantemente sotto controllo aggiunga un notevole carico di stress al loro lavoro, probabilmente aumentato dal fatto che l'azienda non è finora stata in

---

[96] A. Vinci, Amazon, gli autisti Usa sorvegliati da una telecamera: sono obbligati a firmare il «consenso biometrico»", *Corriere della Sera*, 26/3/2021, consultato online il 20/8/2021 all'indirizzo https://www.corriere.it/tecnologia/21_marzo_26/amazon-autisti-usa-sorvegliati-una-telecamera-sono-obbligati-firmare-consenso-biometrico-cb073d88-8d6f-11eb-90de-f8af7075b4bc.shtml.

[97] C. Baraniuk, "How algorithms run Amazon's warehouses", cit.

[98] *Ivi.*

grado di fornire sufficienti rassicurazioni e garanzie sull'effettiva estensione dell'attività di controllo attraverso algoritmi[99].

In Italia, qualche anno fa una grossa polemica ha coinvolto proprio la proposta di Amazon di dotare i propri magazzinieri di speciali braccialetti elettronici che indirizzano i lavoratori verso lo scaffale giusto, ne registrano gli spostamenti e sono in grado di captare i movimenti delle mani, vibrando se non sono corretti[100]. Questo sistema permette di esercitare il potere direttivo sui singoli compiti affidati al dipendente e il potere di controllo sulla produttività in maniera completamente automatizzata, raccogliendo costantemente dati sul lavoratore che possono essere facilmente utilizzati per profilarlo, valutarlo e disciplinarlo.

Le reazioni da parte dei partiti politici e dei sindacati sono state unanimemente contrarie, in particolare per quanto riguarda il diritto alla privacy dei lavoratori[101].

Queste preoccupazioni, condivisibili, riguardano in realtà ogni tipo di dispositivo indossabile. Non si deve pensare che il fenomeno, in Italia, riguardi soltanto grandi multinazionali come Amazon: per esempio, l'azienda di raccolta dei rifiuti di Livorno aveva dotato i suoi dipendenti di braccialetti elettronici dotati di GPS che dovevano servire per segnalare le aree da spazzare e soprattutto per mappare posizione dei cestini in maniera automatizzata e in tempo reale[102].

In questo scenario, la pandemia da Covid-19 non ha fatto che accelerare un processo già in corso. Da un lato, nei contesti in cui è stato possibile *remotizzare* la maggior parte del lavoro, molte aziende si sono trovate a dover riorganizzare i propri processi produttivi per adattarsi alla nuova dislocazione dei lavoratori. L'esigenza avvertita da subito è stata quella di garantire lo stesso livello di controllo datoriale pur non condividendo più lo stesso spazio: di conseguenza, la sorveglianza a distanza attraverso sistemi automatizzati si è diffusa in molte aziende in cui non era precedentemente contemplata.

---

[99] C. DEGRYSE, "Digitalisation of the economy", cit., p.41.
[100] S. Morosi, "Amazon brevetta", cit.
[101] *Ivi.*
[102] "Garante Privacy – Braccialetto elettronico: le condizioni per il trattamento dati", *LavoroSì*, 27/3/2019, consultato online il 20/8/2021 all'indirizzo http://www.lavorosi.it/rapporti-di-lavoro/riservatezza/garante-privacy-braccialetto-elettronico-le-condizioni-per-il-trattamento-dati/.

Dall'altro lato, nei casi in cui i luoghi di lavoro sono rimasti aperti e i dipendenti hanno continuato a recarvisi, molte aziende hanno introdotto sistemi di tracciamento dei contatti (e dei contagi) che si avvalgono di algoritmi per raccogliere i dati ed analizzarli. Tali sistemi possono essere anche molto intrusivi e possono comprendere telecamere di sicurezza dotate di strumenti di intelligenza artificiale e sensori RFID[103].

In tali casi i rischi per la privacy derivano dalla modalità con cui i dati sono conservati (per quanto tempo? Sono possibili usi ulteriori rispetto alla finalità sanitaria?) e alla possibilità che, una volta introdotte, queste tecnologie divengano parte della cultura aziendale e vengano mantenute anche in tempi successivi per ottenere informazioni sui lavoratori[104].

[103] P. Dave, "Companies bet on AI cameras to track social distancing, limit liability", *Reuters* 27/4/2020, consultato online il 20/8/2021 all'indirizzo https://www.reuters.com/article/us-health-coronavirus-surveillance-tech-idUSKCN22914R.

[104] A. PONCE DEL CASTILLO (2020), "COVID-19 contact-tracing apps: how to prevent privacy from becoming the next victim", ETUI Policy Brief n.5/2020.

Capitolo 2. Le fonti lavoristiche italiane: evoluzione storica della normativa applicabile

1. Una premessa: raccolta di dati personali e potere di controllo

Il diritto alla riservatezza e la protezione dei dati personali., come abbiamo visto, non sono certo gli unici aspetti problematici attraverso i quali ci si può accostare al fenomeno del management attraverso algoritmi. Tuttavia, sia per la relativamente lunga tradizione di strumenti di diritto del lavoro italiano applicabili a fenomeni *contigui*, sia per la particolare attenzione posta dall'Unione europea a questi temi anche fuori dal contesto lavoristico, la prospettiva del diritto alla privacy pare tra le più promettenti per fornire al lavoratore protezione contro le minacce che si sono esaminate[1].

Il legislatore nazionale ha in più momenti disciplinato il potere di controllo di cui il datore dispone nei confronti del lavoratore. Tuttavia, una volta di più occorre fare chiarezza riguardo agli esatti confini del fenomeno in esame.

Innanzi tutto, come si è visto, il management attraverso algoritmi non coinvolge l'esercizio del solo potere di controllo, ma anche del potere direttivo e disciplinare. Deve quindi essere chiaro fin da subito che una trattazione nella chiave qui proposta non esaurisce l'intero spettro delle possibili applicazioni del MAA, bensì si concentra su un momento specifico, per quanto necessario, del funzionamento di tale tecnologia.

In secondo luogo, in riferimento ai problemi di *privacy*, l'attenzione dell'osservatore è necessariamente colta dal momento della raccolta dei dati che riguardano i dipendenti. Tuttavia, la disciplina nazionale "autoctona" (non influenzata, cioè, dalle norme sulla privacy di derivazione europea entrate in vigore a partire dagli anni '90) è più propriamente riferita al potere di controllo del datore di lavoro. È allora necessario identificare con esattezza i rapporti tra raccolta dei dati personali sul posto di lavoro e potere di controllo.

[1] V. *supra*, cap. 1 parr. 4 e 5.

È lecito chiedersi, per prima cosa, se il potere di controllo del datore di lavoro si eserciti sempre attraverso la raccolta dei dati personali dei suoi dipendenti. La risposta non può che essere negativa, e secondo due accezioni diverse.

Innanzi tutto, è difficile pensare che il datore, anche negli ambienti di lavoro più digitalizzati, possa delegare interamente agli algoritmi ogni sua funzione: almeno allo stato attuale di avanzamento tecnologico il fenomeno che si osserva normalmente è quello in cui la tecnologia *affianca* il lavoratore e il manager, e non li *sostituisce*[2]. Di conseguenza, seppure in misure diverse, in molti casi in cui la sorveglianza dei lavoratori avviene con metodi tradizionali, come l'osservazione diretta da parte dei superiori, non si potrà individuare alcuna attività di trattamento di dati personali[3].

È poi scorretto sostenere che anche il controllo specificamente esercitato attraverso algoritmi implichi necessariamente il trattamento di dati personali. Se è vero che ogni algoritmo dipende da un certo numero di dati per poter funzionare, non è tuttavia necessario che si tratti di dati personali: attraverso tecniche di analisi di *big data*, infatti, è possibile combinare dati di per sé non personali, come *proxy* e metadati, per ottenere informazioni comunque utilizzabili nella sorveglianza ed eventualmente nella disciplina del personale[4], sino ad arrivare a una vera e propria "de-anonimizzazione", nella quale dati non personali sono utilizzati per ricostruire un profilo del lavoratore[5].

Il potere di controllo del datore di lavoro, quindi, può essere esercitato tanto attraverso la raccolta di dati personali, quanto secondo metodi che non prevedono tale passaggio, sia in un ambiente di lavoro "tradizionale"[6], sia in un ambiente digitalizzato.

---

[2] È questa la tesi di A. ALOISI, V. DE STEFANO (2020), cit., in particolare cap. 2.

[3] Giova qui richiamare la definizione di trattamento di dato personale ("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" – GDPR, art. 4 par. 2).

[4] V. *Supra*, cap. 1 par. 4.

[5] O. TENE, J. POLONETSKY (2012), "Privacy in the Age of Big Data: A Time for Big Decisions", *Stanford Law Review Online*, vol. 64 n. 63, pp. 63-69.

[6] È infatti chiaro che è possibile anche il caso, qui non esaminato, in cui il potere di controllo viene esercitato con strumenti tradizionali che tuttavia implicano la raccolta dei dati personali: si pensi al caso della timbratura del "cartellino" all'ingresso del posto di lavoro, con la possibilità di conservare in un registro gli orari di entrata e di uscita dei lavoratori.

Per seconda cosa, stabilito che il potere di controllo non si esercita sempre tramite raccolta dei dati personali, è giocoforza chiedersi se sia almeno vero il contrario: vi è esercizio del potere di controllo ogni volta che il datore raccoglie dati personali dei dipendenti?

In questo senso, è opportuno definire la categoria di "potere di controllo" con più precisione.

Il Codice del 1942, pur in poche scarne disposizioni, si occupa del potere direttivo e disciplinare del datore[7], tralasciando però completamente di considerare il potere di controllo. È solamente con la promulgazione della Legge 300/1970, e in particolare nel Titolo I, che tale potere viene esplicitamente riconosciuto, pure con il fine di limitarlo[8]; tuttavia, non è data nessuna definizione normativa in senso stretto, sicché l'individuazione dei confini esatti di questa prerogativa datoriale è in sostanza rimessa alla dottrina.

L'esistenza di un potere in capo al datore di controllare la prestazione dei propri dipendenti, tuttavia, non era mai stata in discussione, e in verità non si tratta nemmeno di un carattere specifico del rapporto di lavoro: il Codice civile stesso, in più occasioni, riconosce infatti al creditore di una prestazione di *facere* la possibilità di controllare che l'adempimento sia esatto con un diritto più o meno penetrante di intrusione nella sfera personale del debitore[9].

Per esempio, l'art. 1619, rubricato proprio "Diritto di controllo", riconosce in capo al locatore "in ogni tempo, *anche con accesso in luogo*[10]" il diritto di accertare l'adempimento degli obblighi che incombono sull'affittuario, parte debitrice in un contratto di affitto.

Nell'ambito del contratto di appalto, poi, l'art. 1662 stabilisce che "Il committente ha diritto di *controllare*[11] lo svolgimento dei lavori e di verificarne a proprie spese lo stato". La conseguenza, sul piano giuridico, può essere particolarmente rilevante: se il committente riscontra una difformità rispetto alle condizioni contrattuali, e se l'appaltatore non procede entro un termine congruo, il contratto si risolve.

---

[7] In particolare, per il potere direttivo v. artt. 2103 e per il potere disciplinare v. 2106; più approfonditamente, v. *infra*, par. 2.

[8] M. T. CARINCI (2017), "Il controllo a distanza sull'adempimento della prestazione di lavoro, in P. TULLINI, *Controlli a distanza e tutela dei dati personali del lavoratore*, ed. Giappichelli, p. 45.

[9] A. BELLAVISTA (1995), *Il controllo sui lavoratori*, ed. Giappichelli, pp. 1-2.

[10] Corsivo mio.

[11] *Idem*.

L'art. 2224, infine, prevede un simile meccanismo di risoluzione a fronte dell'inadempimento del debitore in un contratto d'opera: tale strumento previsto dal Codice presuppone, naturalmente, un preventivo controllo dell'esecuzione del contratto da parte del creditore, che avrà quindi un potere di verifica rispetto alla prestazione del prestatore d'opera.

È quindi evidente come, in linea generale, il nostro ordinamento stabilisca un potere di controllo, più o meno esteso, in capo al creditore di prestazioni di *facere* all'interno di rapporti di durata[12]. Nei tre casi qui riportati, tuttavia, si tratta di contratti tra pari, in cui cioè non è riscontrato l'elemento della subordinazione che caratterizza il rapporto di lavoro dipendente. Se si fa invece riferimento allo specifico contesto lavoristico, il potere di controllo assume tratti parzialmente diversi.

Se si assume come caratteristica tipica della subordinazione il fatto che il lavoratore sia inserito nell'organizzazione dell'imprenditore e che debba sottostare alle sue direttive, è giocoforza attribuire all'imprenditore medesimo una facoltà di verifica che la prestazione di lavoro avvenga secondo quanto prescritto, in ogni rapporto[13]. Ma altro è ammettere che una qualche forma di verifica sia elemento necessario della subordinazione, altro è descrivere l'effettivo contenuto del controllo.

A questo proposito la dottrina, prima ancora che confrontarsi con il dettato dello Statuto dei Lavoratori, è stata costretta a una riflessione sul concetto stesso di controllo, sui suoi limiti e sul suo oggetto, e si è aiutata innanzi tutto con l'elaborazione del potere di controllo in ambito pubblicistico.

In questi termini, il potere di controllo può essere visto come "*giudizio* sulla normalità o meno dell'agire o del modo di essere degli operatori controllati"[14], oppure come "verificazione di regolarità di una funzione propria o aliena"[15]: in entrambi i casi, si tratta di un giudizio comparativo tra la realtà fattuale e quanto previsto dal diritto, basato sull'osservazione diretta dell'attività di un soggetto destinatario. Tale attività, nell'ambito del diritto pubblico, si fonda sulla legge ed è tipica della funzione pubblica.

---

12 L'osservazione, di G. GHEZZI, U. ROMAGNOLI (1995), *Il rapporto di lavoro*, ed. Zanichelli, p. 217, prende le mosse da C. SMURAGLIA (1967), *La persona del prestatore nel rapporto di lavoro*, ed. Giuffré, pp. 267 e sgg.

13 A. BELLAVISTA (1995), cit., p. 2.

14 O. SEPE (2010), voce "Controlli", *Enciclopedia Giuridica*, ed. Treccani, vol. 4, p. 2.

15 M. GIANNINI (1974), "Controllo: nozioni e problemi", *Rivista trimestrale di diritto pubblico*, vol. 99 n. 1, p. 1264.

Nell'ambito del diritto del lavoro, tuttavia, non si possono trascurare alcune specificità fondamentali. Se si accetta la tripartizione dei poteri datoriali condivisa nel corso di questa ricerca, il potere di controllo va visto come un elemento necessario del rapporto di lavoro, che si caratterizza, a differenza dei contratti di diritto privato visti poc'anzi, per la presenza di un debitore con limitata autonomia organizzativa e un creditore che programma la prestazione, organizza l'apparato dell'impresa e dirige il lavoratore nelle sue mansioni[16]. La conseguenza, allora, è che il datore-creditore deve poter controllare la rispondenza delle singole operazioni elementari, e del loro insieme coordinato, ai parametri della «diligenza richiesta dalla natura della prestazione» e alle «disposizioni per l'esecuzione e per la disciplina del lavoro»[17]" di cui all'art. 2104 c.c..

Non sempre l'osservazione dei dipendenti conduce a una valutazione in termini comparativi con lo standard previsto dalla legge o dal contratto di lavoro[18]: nella maggioranza dei casi, anzi, il controllo ha natura implicita, dovuta alla struttura sempre in qualche modo gerarchica dell'impresa[19], e nella fisiologia del rapporto di lavoro essa non costituisce il presupposto per il riscontro di un'irregolarità nella prestazione del debitore.

Caratteristica fondamentale del potere di controllo nel contesto del rapporto di lavoro, assente negli altri contratti di diritto privato, è che esso può avere ad oggetto tanto la prestazione dedotta nel contratto quanto la persona stessa del lavoratore – come peraltro confermato dall'impostazione del Titolo I dello Statuto dei Lavoratori. È forse più corretto parlare allora di un controllo integrativo del potere direttivo, con il quale in ogni momento il datore può verificare la rispondenza della prestazione resa alle sue direttive, il quale è implicato nella struttura stessa del contratto di lavoro, e di un controllo "separato dal potere direttivo, appartenente ad una dimensione para- od extracontrattuale, e perciò inessenziale alla realizzazione dell'interesse tipico del creditore di lavoro"[20]. Tali controlli si giustificano per il fatto che il lavoro si

[16] G. GHEZZI, U. ROMAGNOLI (1995), cit., p. 217.
[17] *Ivi.*
[18] A. BELLAVISTA (1995), cit., p. 4.
[19] "[…] talora il controllo appare minimo e semplicemente implicito, in relazione al fatto che il lavoro si svolge nel quadro di un'organizzazione aziendale già predisposta a tal fine; talvolta, invece, esso si rafforza nel ricorso alle forme più svariate, proprio perché l'attività del prestatore si svolge fuori dall'immediata vigilanza del datore" – C. SMURAGLIA (1967) cit., pp. 272-273.
[20] G. GHEZZI, U. ROMAGNOLI (1995), cit., p. 218.

svolge all'interno dei locali del datore, con gli strumenti forniti dal datore, il quale è titolare di un interesse alla sicurezza della propria azienda.

È evidente che adottare la definizione pubblicistica o rifarsi rigidamente ai modelli di controllo tipici del diritto privato sarebbe troppo restrittivo: se vi deve essere sempre un giudizio sulla regolarità della prestazione, così non è nella pratica del controllo nel rapporto di lavoro. A ben vedere, non si può parlare di "giudizio sulla normalità dell'agire" nemmeno per quanto riguarda tecniche di MAA che sono pacificamente ricondotte entro il perimetro del controllo, come per esempio il *rating*: qui, infatti, il confronto non avviene tra l'attività in concreto osservata e il modello legale o contrattuale a cui ci si attende adesione, bensì tra l'attività di uno specifico lavoratore e l'attività degli altri lavoratori[21]. Il dipendente "ultimo classificato" in una graduatoria prodotta con tecniche di *rating* è *comparativamente* meno apprezzato dei suoi colleghi, ma potrebbe tranquillamente adempiere con precisione all'obbligazione contrattuale e quindi non giustificare in nessun caso l'applicazione del potere disciplinare del datore.

Nei termini ora analizzati, possiamo allora individuare come nucleo fondamentale del potere di controllo la sua necessaria presenza nel rapporto di lavoro subordinato, il duplice oggetto, che può riguardare tanto l'attività lavorativa quanto il lavoratore, e la funzione ineliminabile di verificare che la prestazione corrisponda alle direttive e ai parametri di diligenza prescritti per legge.

Entro queste coordinate, è lecito affermare che non ogni raccolta di dati personali dei lavoratori consiste nell'esercizio di potere di controllo da parte del datore. Limitando l'analisi, per quel che qui interessa, al management attraverso algoritmi, un'attività di raccolta automatizzata dei dati sul luogo di lavoro volta a permettere il funzionamento di strumenti tipici del potere direttivo, nella maggior parte dei casi, si situa al di fuori del perimetro del potere di controllo. Questo è parzialmente vero per quanto riguarda la *raccomandazione*[22]: in alcuni casi il lavoratore potrebbe essere indirizzato con questa tecnica in virtù di un precedente controllo – anch'esso automatizzato – sulla sua prestazione lavorativa. Uber, per esempio, utilizza i dati sulla guida registrati dallo smartphone dei propri autisti per determinare se essi stanno compiendo manovre troppo brusche o se stanno seguendo percorsi illogici per suggerire

[21] *Ivi.*
[22] V. *supra*, cap. 1 par. 2.

agli autisti di interrompere la prestazione e riposarsi[23]: evidentemente si tratta di un controllo sulla prestazione dal quale consegue una scelta, tipica del potere direttivo, sul tempo di lavoro.

Non sempre però il processo decisionale è altrettanto lineare: in molti casi, gli algoritmi (specialmente se applicano il *machine learning*) non seguono nessi causali, ma osservano correlazioni tra dati e ne determinano un *output* ritenuto ottimale. Ne consegue che i dati raccolti dai lavoratori, in questi casi, non interessano affatto una valutazione nemmeno implicita sulla loro performance, ma sono solamente la "materia prima"[24] attraverso la quale vengono suggerite determinate modalità di resa della prestazione per il solo fine di incrementare la produttività.

Un discorso simile si può applicare alla *restrizione*: in certi casi è possibile che le informazioni siano ritenute dal lavoratore sulla base di una valutazione sulla sua specifica attività, che chiaramente rientra nell'ambito del controllo. Upwork, una piattaforma che permette a professionisti di proporre i propri progetti online ai clienti, utilizza un algoritmo di analisi testuale per inviare messaggi di allerta che ricordano al lavoratore-utente del patto di non concorrenza stipulato con la società ogni volta che rileva determinate parole chiave, oscurando mail e numeri di telefono[25] che potrebbero portare a contatti e prestazioni di lavoro al di fuori della piattaforma.

In altri casi, tuttavia, non è così: sempre Uber in passato ha utilizzato i dati sulla disponibilità degli autisti per limitare le possibili scelte in merito ai turni o alle singole corse per meglio adattare l'offerta di lavoro a momenti di richiesta particolarmente alta: qui non c'è alcuna valutazione sulla rispondenza della prestazione dell'autista allo standard richiesto, bensì un semplice uso dei dati prodotti ai fini, ancora una volta, di efficientamento dell'attività d'impresa.

Una volta tratteggiati con più precisione i confini di questi due fenomeni – potere di controllo e raccolta dei dati dei lavoratori – è possibile proseguire nella trattazione, con la consapevolezza che la legislazione italiana che si occupa di limitazioni al potere di controllo spesso si interseca ma non coincide con la protezione dei dati dei lavoratori, e non sempre è applicabile al management attraverso algoritmi.

---

[23] A. ROSENBLAT, L. STARK (2016), cit.
[24] Tra i molti v. E. DAGNINO (2017), cit., p. 5.
[25] M. H. JARRAHI et al. (2019), "Platformic management, boundary resources, and worker autonomy in gig work", *Computer Supported Cooperative Work*, n. 1 p. 37.

2. *La disciplina precedente lo Statuto: il Codice civile e il lavoro a cottimo*

Come detto in precedenza[26], l'esistenza di un potere di controllo in capo al datore di lavoro era pacifica ben prima del 1970, quando lo Statuto dei Lavoratori ha esplicitamente normato questo aspetto del rapporto di lavoro.

Il Codice civile, in termini generali, detta una disciplina piuttosto scarna del rapporto di lavoro, ma addirittura rinuncia a pronunciarsi in qualsiasi modo sul potere di controllo e sul diritto alla riservatezza. Come visto, questo significa che, nella pratica, i controlli sul lavoratore e in particolare sulla sua persona erano prima dello Statuto "sottratti all'attenzione dell'ordinamento e, di fatto, se non in principio, erano esenti da limiti alla stregua del diritto comune"[27].

Del diritto comune, tuttavia, il potere di controllo pre-1970 non condivide i limiti: come già evidenziato, infatti, è caratteristica peculiare dei controlli nel rapporto di lavoro di potersi estendere anche sulla persona del lavoratore – a differenza, per esempio, di quanto previsto dagli artt. 1619, 1662 e 2224 c.c..

Il datore, infatti, specialmente in questa fase storica, non è un semplice creditore che si accerti dell'esattezza della prestazione del debitore. Poiché il dipendente è inserito in una struttura organizzata e diretta dall'imprenditore a proprio rischio, e utilizza strumenti e infrastrutture di proprietà dell'imprenditore; quest'ultimo, *padrone a casa propria*, ha diritto di adottare ogni misura necessaria non solo a condurre la propria impresa, ma anche a prevenire danni al patrimonio aziendale[28].

Nel rapporto di lavoro la persona stessa del lavoratore è implicata in misura più o meno estesa, in quanto è elemento fondamentale e necessario della subordinazione stessa che la prestazione abbia carattere *personale*[29]. Di conseguenza, per quanto non si possa parlare di un vero e proprio rapporto fiduciario[30], è chiaro che l'imprenditore ha un interesse a conoscere le qualità personali del lavoratore.

---

[26] *Supra*, par. 1.
[27] T. TREU (1990), voce "Statuto dei lavoratori", in *Enciclopedia del diritto*, ed. Treccani, vol. XLIII p. 1051.
[28] A. BELLAVISTA (1995), cit., p. 8.
[29] O. MAZZOTTA (2016), cit., pp. 314 e sgg.
[30] C. SMURAGLIA (1967), cit., pp. 47 e sgg.

Non è comunque vero che nel contesto giuridico precedente all'entrata in vigore dello Statuto l'interesse del datore a sorvegliare e conoscere ogni aspetto della vita del lavoratore non incontrasse alcun limite. Se è vero che il Codice del 1942 lascia potenzialmente aperto ogni spazio al potere di controllo, è pur vero che il lavoratore, tutelato dalla Costituzione, gode *in quanto cittadino* di diritti della personalità (specificamente, alla riservatezza) che contrastano con l'interesse datoriale.

I diritti alla riservatezza sono, per loro stessa natura, disponibili[31] e, proprio l'implicazione della persona del lavoratore nel rapporto di lavoro di cui si è detto poc'anzi determina una "parziale rinuncia, da parte dello stesso prestatore, alla tutela della propria riservatezza nei confronti del datore di lavoro"[32]. Se tale rinuncia deve essere parziale, tuttavia, è giusto chiedersi entro quali limiti possa considerarsi legittimo il bilanciamento tra gli interessi del lavoratore e quelli della controparte datoriale[33] e quando invece si sconfini nell'invasione arbitraria della sfera personale.

In un tempo in cui la legge ancora nulla disciplinava in proposito, soccorrono a questo fine gli interventi di una parte della dottrina. Il ragionamento generalmente utilizzato per stabilire i limiti all'intrusione dell'imprenditore nella sfera personale dei dipendenti fa perno in questa fase sulla causa tipica del lavoro subordinato, riletta alla luce dei principi costituzionali, con il risultato di individuare i caratteri propri della *subordinazione tecnica*. In sostanza, i poteri di controllo (e quindi il corrispondente sacrificio in termini di riservatezza da parte dei lavoratori) si devono arrestare laddove ha fine la prestazione dedotta nel contratto; i controlli ulteriori, relativi alla persona del lavoratore ma inessenziali rispetto all'adempimento della prestazione, non si possono considerare leciti[34].

In questo senso, è stato possibile individuare già prima della vigenza delle regole statutarie una serie di limiti al potere di controllo.

È stato affermato, innanzi tutto, che il limite estremo del controllo corrisponde a quegli aspetti della vita privata del lavoratore del tutto irrilevanti per l'esatta

---

31 P. ICHINO (1986), *Diritto alla riservatezza e diritto al segreto nel rapporto di lavoro*, ed. Giuffré, p. 50.
32 *Ibid.*, p. 52.
33 V. anche L. MENGONI (1965), "Contratto e rapporto di lavoro nella recente dottrina italiana", *Rivista della Società*, pp. 674 e sgg.
34 P. ICHINO (1986), cit., p. 53. V. Anche C. SMURAGLIA (1967), cit., p. 285, secondo cui "[…] la dipendenza del prestatore non può estendersi al di là della fase di attuazione dell'obbligazione, fino ad investire la vita privata o le attività extralavorative", ma già in precedenza molti autori avevano adottato questa posizione: L. BARASSI (1901), *Il contratto di lavoro nel diritto positivo italiano*, p. 623; L. RIVA SANSEVERINO (1958), *Diritto del lavoro*, ed. CEDAM, p. 46.

esecuzione della prestazione: è vero che alcuni rapporti (ma solo alcuni[35]) sono caratterizzati da "una particolare struttura o da un vincolo fiduciario, nei quali la stessa vita privata del dipendente può avere influenza sulla prestazione"[36]; tuttavia, anche in questi casi, in verità eccezionali, sarà sempre necessario individuare un nesso di causalità diretta tra la condotta extralavorativa e la possibilità di adempiere esattamente all'obbligazione di prestare la propria opera.

La giurisprudenza precedente allo Statuto, in realtà, non è mai stata particolarmente aperta a una simile ricostruzione, per quanto rigorosa: in più occasioni[37] è stata anzi affermata la rilevanza di comportamenti tenuti da un dipendente al di fuori dell'orario lavorativo, in quanto in grado di produrre effetti anche indiretti sulla reputazione dell'azienda. Una simile posizione, a ben vedere, non può essere sostenuta che per un ristretto numero di situazioni[38] in cui esiste effettivamente un rapporto di fiducia, ma non certo nella normalità dei casi[39].

Un altro importante portato dottrinale riguarda il presunto obbligo precontrattuale di informare il datore di lavoro su fatti o circostanze che non rilevassero ai fini della valutazione dell'attitudine professionale, escluso prendendo le mosse da un ragionamento analogo sui confini del contenuto dell'obbligazione contrattuale[40].

Allo stesso modo, è stato possibile ben prima degli artt. 2 e 3 dello Statuto dei Lavoratori verificare l'illegittimità del controllo esercitato pure sul luogo di lavoro ma con metodi e strumenti "spionistici" e senza dubbio vessatori esercitati da personale di vigilanza, in quanto lesivi della dignità e, in ultima

---

35 C. SMURAGLIA (1967), cit., pp. 118-119, fa l'esempio del "giocatore di calcio sorpreso in un night-club alle due del mattino", del "sacrestano che conduce una vita immorale e licenziosa", dell'"indossatrice che si procuri delle vaste bruciature per eccessiva esposizione al sole nel suo giorno di riposo", etc. Si tratta in ogni caso di situazioni le cui conseguenze ricadono direttamente sulla prestazione dedotta in contratto.

36 *Ibid.*, p. 286.

37 V. Cass. 3 settembre 1957, n. 3419, in *Il Foro italiano*, n. 1/1957, p. 1395.

38 V. nota 35.

39 Per una panoramica sulla discussa giurisprudenza dell'epoca, v. nuovamente C. SMURAGLIA (1967), cit., pp. 289-291.

40 U. ROMAGNOLI (1970), "Sulla rilevanza della reticenza del prestatore di lavoro come «culpa in contrahendo», nota a Cass., 30 dicembre 1969 n. 4059, *Giurisprudenza italiana*, n. 1 vol. 1, pp. 1066-1070.

analisi, della libertà morale del dipendente, oltre che in ogni caso esorbitanti rispetto al contenuto della subordinazione tecnica[41].

Già prima dell'entrata in vigore dello Statuto, quindi, una parte della dottrina era stata in grado di sostenere delle teorie che limitavano i poteri intrusivi dell'imprenditore; tuttavia, poiché tali teorie erano fondate sul concetto di subordinazione tecnica e sui limiti della prestazione contrattuale, esse avevano una portata piuttosto limitata. In assenza di una disciplina specifica in grado di limitare e disciplinare i poteri datoriali, la giurisprudenza era poi libera di (e propensa ad) adottare decisioni che riconoscevano al datore poteri quasi illimitati.

3. Lo Statuto dei Lavoratori: gli articoli 4 e 8

Con la Legge 300/1970, nota come Statuto dei Lavoratori, il legislatore si è occupato di realizzare un nuovo bilanciamento di interessi. L'impatto dello Statuto sulla configurazione stessa del rapporto di lavoro è stato dirompente: basandosi sul riconoscimento che nel contesto normativo fino ad allora vigente i poteri del datore di lavoro potevano spingersi sino a "modalità abusive" e "intensità di tipo dominicale e feudale"[42], il legislatore repubblicano si è proposto di *spersonalizzare* il rapporto di lavoro, nel senso di considerare innanzitutto irrilevanti tutte le caratteristiche della persona del lavoratore che non siano in grado di incidere sull'esattezza della prestazione[43].

L'opera di *spersonalizzazione* parte proprio con il limitare la possibilità dell'imprenditore di intromettersi nella vita privata dei dipendenti. In termini generali, il titolo I dello Statuto non ha modificato la struttura del contratto di lavoro, ma ha introdotto nuovi limiti alla disponibilità dei diritti alla riservatezza del lavoratore negli ambiti del controllo sul posto di lavoro, degli accertamenti sanitari e delle perquisizioni personali[44].

---

41 V. CRISAFULLI (1955), "Ancora in tema di libertà costituzionali e rapporti di lavoro subordinato", nota a Pret. Torino 25 luglio 1955, *Rivista giuridica del lavoro*, vol. 2 pp. 524-532, oppure G. GHEZZI (1956), "Polizia privata nelle imprese e tutela dei diritti costituzionali dei lavoratori", *Rivista trimestrale di diritto e procedura civile*, n. 3 pp. 1003-1026.

42 A. BELLAVISTA (1995), cit., p. 9. V. anche L. BARASSI (1901), cit., p. 634, per cui "Un eccesso di subordinazione potrebbe costituire una lesione alla dignità del lavoratore".

43 L. GAETA (1990), "La dignità del lavoratore e i «turbamenti» dell'innovazione", *Lavoro e diritto*, n. 1 pp. 207 e sgg.

44 P. ICHINO (1986), cit., p. 55.

L'insieme di poteri nella disponibilità del datore di lavoro, insomma, viene razionalizzato[45] attraverso la L. 300/1970: concentrandosi sulla sorveglianza dei lavoratori, in certi casi essa è del tutto proibita[46]; in altri e consentita solo a certe condizioni[47]; in altri ancora è subordinata all'accordo con le rappresentanze sindacali o, in assenza, all'autorizzazione da parte di un organo pubblico[48].

Per quanto concerne questa trattazione, gli artt. 4 e 8 sono i più interessanti in quanto ad oggi vigenti e applicabili a molti profili problematici che riguardano il management attraverso algoritmi, naturalmente entro i limiti più sopra individuati[49].

I primi due commi della versione originale dell'art. 4 SL, dedicato agli impianti di registrazione, recitavano:

> *È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori.*
>
> *Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti.*

Il nuovo bilanciamento degli interessi nell'ambito specifico della videosorveglianza era particolarmente rigoroso: il controllo a distanza *sull'attività lavorativa* e sul comportamento generale del lavoratore sul luogo di lavoro era fino ad allora, di fatto, del tutto libero; l'art. 4 riequilibra invece la situazione in maniera fortemente favorevole al lavoratore.

L'articolo si componeva originariamente di quattro commi, ma i primi due, riportati poc'anzi, rivestono un ruolo fondamentale nella nuova configurazione del rapporto tra imprenditore e dipendenti.

---

45 U. ROMAGNOLI (1979 a), *Sub art. 4*, p. 18, in S. GEZZI et al., *Statuto dei diritti dei lavoratori*, ed. Zanichelli, parla di "progetto di razionalizzazione dell'«autocrazia industriale».
46 Art. 4 c. 1, nella formulazione originale.
47 Art. 2, art. 4 c. 2.
48 In particolare, artt. 4 e 6.
49 V. *supra*, par. 1.

Il primo comma dell'art. 4 è dedicato al cd. *controllo intenzionale*, ovvero l'installazione di apparecchiatura di sorveglianza che sin dall'origine è preordinato al controllo a distanza dei lavoratori nell'azienda. Questa attività è vietata in modo assoluto e tale divieto non ammette eccezioni[50].

Il secondo comma è invece dedicato al cd. *controllo preterintenzionale*, che costituisce una "conseguenza meramente accidentale dell'utilizzazione di apparecchiature richieste da esigenze sovraordinate e valutate di primaria importanza per la funzionalità dell'apparato produttivo"[51]. In questi casi, cioè, lo Statuto permette di installare apparecchiature che possano ipoteticamente realizzare un controllo a distanza, ma solo a due condizioni: che esse siano necessarie per esigenze legate al modello produttivo dell'azienda o alla sicurezza dei lavoratori, e che vi sia accordo con le RSA o, in assenza, autorizzazione dell'ispettorato del lavoro.

Si badi che tali condizioni permettono esclusivamente l'installazione di impianti audiovisivi, ma non anche l'utilizzo delle registrazioni per finalità di controllo o disciplinari. Il divieto, in questo senso, rimane assoluto e non rileva che il controllo a distanza sia il fine esclusivo, oppure concorra con fini permessi dalla legge come appunto la tutela della sicurezza o le esigenze produttive dell'impresa: in ogni caso, al lavoratore è riconosciuto un vero e proprio diritto soggettivo a non essere controllato a distanza[52].

Lo scopo della norma, evidentemente, non riguardava tanto la riservatezza della vita privata del lavoratore, rispetto alla quale il controllo a distanza non dovrebbe comunque avere effetto, quanto piuttosto la volontà del legislatore di evitare le modalità più odiose di controllo, alienanti e in grado di rendere l'ambiente di lavoro malsano e difficilmente sopportabile[53].

---

[50] A. BELLAVISTA (1995), cit., p. 76.

[51] *Ivi.*

[52] *Ibid.*, p. 77; v. anche S. DURANTI (1972), "Impiego dei mezzi audiovisivi e Statuto dei lavoratori", *Massimario di giurisprudenza del lavoro*, n. 1 p. 146.

[53] Già dieci anni prima dello Statuto, assistendo alle prime installazioni di tecnologie di videosorveglianza sui luoghi di lavoro, C. SMURAGLIA (1960), "Progresso tecnico e tutela della personalità del lavoratore", *Rivista giuridica del lavoro*, n. 1 p. 312, notava che "un siffatto controllo su ogni momento dello svolgimento dell'attività lavorativa e magari anche sulle pause del lavoro, non può in alcun modo svolgersi senza una palese compressione della libertà dei prestatori di lavoro e senza una clamorosa violazione della dignità umana. Una cosa è il controllo del sorvegliante, che interviene, contesta direttamente un'infrazione, dà modo al lavoratore di difendersi, di prospettare le sue ragioni; altra cosa, e ben diversa, è il controllo anonimo, odioso, scostante, spinto fino all'esasperazione, da parte di un meccanismo controllato soltanto dalla direzione aziendale e dai suoi incaricati".

Al momento dell'emanazione dello Statuto dei Lavoratori gli strumenti di sorveglianza a distanza erano relativamente limitati, ed è abbastanza evidente che, nella formulazione del testo di legge, il legislatore aveva in mente principalmente gli impianti di videosorveglianza (tipicamente, telecamere a circuito chiuso)[54]. L'evoluzione tecnologica dei decenni successivi, tuttavia, ha realizzato la possibilità tecnica di controllare i lavoratori attraverso gli apparecchi più svariati, a partire proprio dagli strumenti di lavoro oggi più comuni come i terminali personali[55] o gli smartphone aziendali[56].

Nel contesto dello Statuto pre-riforma del 2015, si doveva ritenere che tutte le forme di controllo a distanza, realizzate attraverso qualsiasi apparato, dovessero essere coperte dal divieto di cui all'art. 4 comma 1[57]: ne è conferma l'atteggiamento di netta chiusura dimostrato dalla giurisprudenza di legittimità.

L'impatto di una normativa tanto rigorosa e restrittiva con l'evoluzione tecnologica, tuttavia, non era destinato a rimanere senza conseguenze. Alcuni datori di lavoro, nel corso degli anni, hanno dato prova in più casi di preferire eludere la norma, installando i dispositivi di sorveglianza in assenza di alcun accordo o autorizzazione: così facendo, infatti, sarebbero rimasti soggetti al rischio di una pronuncia giudiziale successiva a loro negativa, ma nel frattempo non sarebbero stati sottoposti alle limitazioni e alla procedimentalizzazione tipica dello strumento di cui all'art. 4 comma 2[58].

Un ulteriore elemento di indebolimento del dettato dello Statuto dei Lavoratori, emerso nella giurisprudenza a partire dagli anni '90[59], è dato dai cd. controlli difensivi[60]. Pur nell'impossibilità di dar conto in maniera approfondita del fenomeno, basti notare che una corrente giurisprudenziale non trascurabile ha

---

54 G. GIUGNI (1989), *Lavoro leggi contratti*, ed. Il Mulino, p. 355.

55 R. DE LUCA TAMAJO et al. (1988), *Nuove tecnologie e tutela della riservatezza dei lavoratori*, ed. Franco Angeli, p. 10 e sgg.

56 "È evidente dunque come l'avvento delle nuove tecnologie abbia gravemente "spiazzato" la norma statutaria" – M. T. CARINCI (2016), "Il controllo a distanza dell'attività dei lavoratori dopo il "Jobs Act" (art. 23 D.Lgs. 151/2015): spunti per un dibattito", *Labour and Law Issues*, vol. 2 n. 1 p. VI.

57 M. T. CARINCI (2017), cit., p. 47; in senso contrario – ma tale ricostruzione non è stata accolta dalla giurisprudenza – v. P. ICHINO (2003), *Il contratto di lavoro*, in P. SCHLESINGER, *Trattato di diritto civile e commerciale*, ed. Giuffré, vol. 3 pp. 234 e sgg.

58 V. M. T. CARINCI (2017) cit., p. 48.

59 Ma le prime sentenze di legittimità in questo senso risalgono agli anni 2000: v. Cass. 3 luglio 2001, n. 8998, e successivamente Cass. 3 aprile 2002, n. 4746; Cass. 17 luglio 2007, n. 15892, Cass. 23 febbraio 2010, n. 4375; Cass. 23 febbraio 2012, n. 2722; Cass. 1° ottobre 2012, n. 16622.

60 La massiccia introduzione nei luoghi di lavoro di computer come strumenti di lavoro ha contribuito in maniera sostanziale a diffondere la pratica dei controlli difensivi: v. G. GHEZZI, F. LISO (1986), "Computer e controllo dei lavoratori", *Giornale di diritto del lavoro e relazioni industriali*, n.1 pp. 374 e sgg.

ritenuto giustificato, in quanto estraneo all'oggetto dell'art. 4, l'utilizzo di strumenti di controllo a distanza per accertare in via successiva la condotta illecita del dipendente[61].

Questi due fenomeni, dunque, permettono fin d'ora di osservare che anche prima del 2015 vi erano stati tentativi talvolta fruttuosi, in dottrina e in giurisprudenza così come nella prassi aziendale, di indebolire la portata del divieto di controllo a distanza.

Il secondo punto di interesse, per quanto riguarda questa ricerca, riguarda l'art. 8 dello Statuto, rubricato "divieto di indagini sulle opinioni". Il suo testo, mai modificato, recita:

> *E' fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore.*

Anche in questo caso è possibile vedere il contenuto dell'articolo come essenzialmente bipartito. Da un lato, infatti, le indagini sulle "opinioni politiche, religiose o sindacali del lavoratore sono vietate sempre e comunque"[62]. La finalità di questo primo inciso dell'art. 8, è stato osservato, difficilmente riguarda il diritto alla riservatezza in senso stretto, in quanto proprio le opinioni politiche, religiose e sindacali sono normalmente manifestate "alla luce del sole"[63].

Si deve allora dedurre che il legislatore ha voluto prevenire la possibilità che l'imprenditore basi le decisioni relative all'assunzione di personale e alla gestione dell'azienda su opinioni personali dei lavoratori in ambiti tanto delicati quanto normalmente ininfluenti per l'adempimento della prestazione lavorativa. Si tratta di una sorta di presunzione assoluta di irrilevanza, che non può essere superata se non per le organizzazioni di tendenza, e comunque entro limiti ben ristretti, volta ad anticipare al momento della raccolta delle informazioni la

---

61 M. T. CARINCI (2016), cit., pp. V-VI e in particolare nota 8.
62 Con la sola eccezione delle organizzazioni di tendenza: v. U. ROMAGNOLI (1979 b), *Sub art. 8*, p. 140, in S. GHEZZI et al., *Statuto dei diritti dei lavoratori*, cit..
63 A. BELLAVISTA (1995), cit., p. 80.

tutela contro una potenziale futura discriminazione[64] e, in ultima analisi, a garantire la libertà e l'autodeterminazione del lavoratore[65].

Il secondo inciso dell'art. 8 vieta in ogni caso di effettuare indagini su "fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore". Il principio di cui si fa portatrice questa norma è essenzialmente lo stesso già individuato dalla dottrina precedente allo Statuto dei Lavoratori[66]: il potere di controllo del datore si deve fermare ai confini dell'attività dedotta in contratto e non può investire senza giustificato motivo la vita privata del dipendente.

Il punto più controverso rimane, ancora una volta, quando un fatto possa effettivamente dirsi rilevante per la valutazione dell'attitudine professionale. In questo senso, sarebbe errato ritenere che il diritto del lavoratore alla riservatezza prevalga sempre e comunque sull'interesse del datore a ottenere informazioni[67]: l'imprenditore può legittimamente svolgere indagini anche su fatti appartenenti alla sfera privata del dipendente (o potenziale dipendente, se le indagini avvengono prima dell'assunzione), ma solo se i fatti indagati sono in un rapporto di causalità immediata con le mansioni dedotte nel contratto di lavoro.

Di conseguenza, anche elementi come "lo stile di vita, il carattere, risvolti *lato sensu* morali, e finanche l'ambiente in cui è cresciuto il soggetto"[68] possono rientrare in una legittima attività di indagine: gli esempi più classici riguardano l'abitudine all'ubriachezza per un pilota di aerei o un autista di mezzi pubblici, oppure la dedizione al gioco d'azzardo per un cassiere di banca, ma è ovvio che le possibili implicazioni variano a seconda delle mansioni concretamente espletate.

In entrambi i casi, poi, è necessario che vi sia una vera e propria attività d'indagine, intesa come attività volta alla ricerca di informazioni, sia tramite ricerche all'insaputa (o comunque senza la collaborazione) del lavoratore, sia tramite interrogazioni dello stesso[69]. Perché ci possano essere indagini vietate, quindi, è necessario che vi sia una condotta attiva del datore di lavoro. Se le informazioni giungessero nella sua disponibilità senza che egli realizzasse alcun

---

64 V. L. 300/1970, artt. 15 (Divieto di discriminazione) e 16 (Trattamenti economici collettivi discriminatori).

65 La conferma di tale impostazione si può ritrovare proprio nell'art. 1 dello Statuto, che garantisce la libertà di manifestazione del pensiero "senza distinzione di opinioni politiche, sindacali e di fede religiosa".

66 V. *supra*, par. 2.

67 *Ibid.*

68 A. BELLAVISTA (1995), cit., p. 86.

69 A. FRENI, G. GIUGNI (1971), *Lo Statuto dei lavoratori*, Giuffré p. 41.

comportamento positivo, oppure se le informazioni fossero di pubblico dominio, non si configurerebbe nessuna violazione dell'art. 8[70].

Dall'analisi e dal confronto tra l'art. 4 e l'art. 8 dello Statuto dei Lavoratori si possono trarre almeno due utili osservazioni.

In primo luogo, entrambe le norme hanno, a ben vedere, un contenuto molteplice, poiché molteplici sono i beni che intendono tutelare. L'art. 4, infatti, non si limita a garantire la riservatezza del dipendente vietando i controlli sulla sua persona, ma anche la sua autodeterminazione, vietando pure i controlli sull'attività solutoria, che di per sé non rientrerebbe nella sfera personale del lavoratore. Qualcosa di simile si può dire per l'art. 8 che, come appena visto, tutela tanto la vita privata del lavoratore in riferimento agli elementi "non necessari", quanto la sua autodeterminazione in riferimento alla libertà di opinione[71].

In secondo luogo, e come corollario di quanto appena constatato, si può individuare una coordinata comune ai due articoli dello Statuto: in entrambi i casi l'intento più profondo è quello di limitare i poteri datoriali al fine di realizzare il più pienamente possibile la "spersonalizzazione" del rapporto di lavoro e far sì che il controllo si limiti al contenuto della prestazione di lavoro[72].

4. Il Codice della privacy del 2003 e il diritto europeo

Dall'esposizione del contenuto degli artt. 4 e 8 dovrebbe apparire chiaramente che essi regolano alcuni degli aspetti più pericolosi del potere di controllo, ma sotto la loro vigenza rimangono possibili da parte del datore di lavoro una serie di condotte potenzialmente lesive del diritto alla riservatezza del lavoratore, specialmente in un contesto, come quello degli anni '90, di rapida trasformazione tecnologica dell'ambiente di lavoro. Rimane fuori dall'area di operatività dello Statuto dei Lavoratori ogni raccolta di dati personali non riferibile al potere di controllo, così come la conservazione e la catalogazione in

[70] A. BELLAVISTA (1995), cit., pp. 92-93.
[71] P. ICHINO (1986), cit., p. 121.
[72] V. di nuovo A. FRENI, G. GIUGNI (1971), cit., p. 39.

banche dati di informazioni già note sul lavoratore[73] e le già richiamate indagini difensive[74].

L'impatto delle "nuove" tecnologie sui meccanismi dello Statuto è testimoniato dalla giurisprudenza rilevante: se nei primi dieci anni le decisioni che avevano riguardato l'art. 4 erano state relativamente poche, a partire dagli anni '80 e più ancora nei decenni successivi si è sviluppato un prolifico dibattito in sede giurisprudenziale, che tuttavia ha portato a risultati contraddittori[75].

Dubbi interpretativi hanno riguardato, in particolare, i dati registrati da strumenti di lavoro sostanzialmente assenti nel 1970, ma già ampiamente diffusi vent'anni dopo: in particolar modo, i terminali collegati ad elaboratori centrali e i telefoni collegati a un centralino elettronico[76].

Una parte della dottrina ha proposto una lettura teleologicamente orientata della norma, che nell'analisi degli autori sarebbe volta al solo fine di impedire intrusioni indebite nella sfera personale del lavoratore: di conseguenza, i dati raccolti dagli strumenti di lavoro che riguardino solamente la prestazione lavorativa potrebbero essere utilizzati per finalità di controllo (della rispondenza della prestazione alle direttive impartite, rimanendo sempre escluso il controllo della persona in quanto tale)[77]. Se tale lettura non è stata condivisa dalla giurisprudenza maggioritaria, è pur vero che essa evidenzia una possibilità inedita, ovvero che il controllo si operi non tramite meccanismi che da un punto di vista esterno "osservino" e registrino la prestazione, bensì attraverso lo stesso strumento con cui quella prestazione è resa.

Inoltre, per la prima volta con l'introduzione dei computer sul posto di lavoro si poneva il problema della produzione, processazione e conservazione di moli di dati dei lavoratori senza precedenti. Solo in questa occasione, infatti, diventava tecnicamente possibile tenere costantemente traccia dell'attività dei dipendenti e conservare tali informazioni a costi ragionevoli, grazie al passaggio dagli archivi cartacei alle banche dati[78].

---

[73] A. BELLAVISTA (1995), cit., p. 83; ma in senso contrario v. L. LEO (1981), "Le disposizioni penali dello Statuto dei lavoratori", *Rivista giuridica del lavoro*, n. 4 p. 730.
[74] V. *supra*, nota 59.
[75] R. ROMEI, S. SCIARRA (1995), "The Protection of Employees' Privacy: A Survey of Italian Legislation and Case Law", *Comparative Labour Law Journal*, vol. 17 n. 1, p. 94.
[76] *Ibid.*, pp. 94-95.
[77] R. DE LUCA TAMAJO et al. (1988), cit.
[78] A. BELLAVISTA (1995), cit., pp. 128 e sgg.

In seguito a una prima informatizzazione degli ambienti di lavoro, ad ogni modo, si sono stabilizzati determinati approdi giurisprudenziali riguardo ad alcuni nuovi strumenti in grado di interferire con la sfera personale del lavoratore.

È stato chiarito, per esempio, che è possibile installare sistemi di registrazione automatica delle statistiche delle chiamate di un centralino telefonico, a patto che i superiori non possano in ogni caso ascoltare le conversazioni[79]; che i *badge* magnetici possono essere impiegati per registrare gli orari di ingresso ed uscita dal lavoro, ma non per sorvegliare la posizione del lavoratore sul posto di lavoro, salvo che sussistano specifiche ragioni di sicurezza[80]; che non è lecito installare software in grado di registrare automaticamente i tempi delle singole operazioni, errori, pause, etc.[81].

In un simile contesto si innesta il primo grande intervento comunitario sulla disciplina della privacy, la Direttiva 95/46 sul trattamento dei dati personali.

La Direttiva, la cui base legale è, significativamente l'instaurazione e il funzionamento del mercato interno ex art. 26 TUE (all'epoca in cui la Direttiva è stata redatta, art. 8), non era riferita specificamente all'ambito del lavoro, e anzi adottava un "approccio omnibus"[82], che vede il dato come meritevole di tutela in ogni contesto in quanto "frammento minimo dell'identità umana"[83]. Di conseguenza, essa permetteva l'elaborazione, accanto al diritto alla riservatezza già riconosciuto dallo Statuto dei Lavoratori[84], di un diritto alla protezione dei dati personali[85], forse più adeguato a garantire una tutela effettiva nei contesti lavorativi degli anni '90.

La Direttiva 95/46 è stata adottata in Italia dapprima con la Legge 675/1996 e, successivamente, con il D. Lgs. 196/2003, il cd. Codice della privacy. L'origine comunitaria della disciplina sul trattamento dei dati personali ha fatto sì che essa fosse imperniata su un approccio in verità inedito per il diritto italiano,

---

79 Trib. Milano, 29 settembre 1990, in *Il Foro italiano*.
80 Pret. Milano, 6 luglio 1981, in *Il Foro italiano*.
81 Pret.. Milano, 5 dicembre 1984, in *Il Foro italiano*.
82 P. CHIECO (2000), *Privacy e lavoro. La disciplina del trattamento dei dati personali del lavoratore*, ed. Cacucci, p. 23.
83 A. INGRAO (2018), *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, ed. Cacucci, p. 54.
84 V. *supra*, parr. 2 e 3.
85 Sulla differenza tra riservatezza, tutelata all'art. 7 della Carta di Nizza, e protezione dei dati personali, autonomamente garantita all'art. 8 dello stesso trattato, si rinvia a P. ICHINO (1986) cit.

fortemente legato ad una logica di *prevenzione* del rischio di trattamento illecito[86], piuttosto che di divieto e intervento giudiziale successivo.

La legge, innanzi tutto, individuava un "titolare" del trattamento, responsabile della correttezza di tutto il procedimento di raccolta, conservazione ed elaborazione, ma anche altri soggetti come il "responsabile" e l'"incaricato", i quali intervenivano con gradi più o meno estesi di responsabilità[87]. Erano poi fissati, all'art. 11, dei principi riguardanti le modalità di trattamento dei dati, che dovevano essere necessariamente rispettati al costo di rendere inutilizzabile il dato: si tratta dei principi di *trasparenza*, *finalità* e *necessità*. Il principio di finalità, in particolare, richiedeva che fosse presente una determinata base legale ai fini della liceità del trattamento: il consenso dell'interessato, l'esecuzione di un contratto, un obbligo di legge, la salvaguardia dell'interesse vitale dell'interessato, un compito di interesse pubblico o un legittimo interesse del titolare, purché prevalente sull'opposto interesse alla riservatezza[88].

Al singolo interessato, inoltre, venivano attribuiti una serie di diritti che avrebbero dovuto garantirgli il controllo sul dato personale: innanzitutto un diritto all'informazione, contraltare dell'obbligo di trasparenza stabilito dall'art. 11 e presupposto di ogni azione successiva; inoltre, una volta raccolti i dati, l'interessato aveva diritto di accesso, aggiornamento, rettifica, integrazione e cancellazione, nonché di opposizione alla profilazione[89].

A vigilare sulla corretta applicazione della normativa in tema di privacy, la Legge 675/1996 ha poi istituito il Garante per la protezione dei dati personali, un'autorità indipendente composta da quattro membri con poteri prescrittivi, paragiurisdizionali e autorizzatori[90], nel cui seno la disciplina dei dati personali si è specificata ed evoluta[91].

È evidente che una tale disciplina rivestiva un ruolo di sicuro interesse per i problemi derivanti dalle nuove tecnologie sul posto di lavoro e ci si deve domandare quali siano stati i rapporti con lo Statuto dei Lavoratori. In questo senso, è certamente vero che le due discipline perseguivano fini e logiche diversi (l'una vietava l'utilizzo di strumenti di telesorveglianza, l'altra disciplinava le modalità con cui i dati possono essere trattati, senza tuttavia vietare a priori

---

86 A. INGRAO (2018), cit., p. 61.
87 V. Codice privacy, art. 4 c. 1 lett. f), g) e h).
88 Direttiva 95/46/CE, art. 7.
89 Codice privacy, art. 7.
90 L. 675/1996, artt. 30 e 31.
91 M. G. LOSANO (2001), *La legge italiana sulla privacy. Un bilancio dei primi cinque anni*, ed. Laterza.

modalità specifiche di trattamento[92]), ma è innegabile che esse fossero applicabili agli stessi soggetti (il lavoratore, protagonista dello Statuto, si può vedere come *species* del cittadino interessato dal trattamento, protagonista del Codice della privacy) e che, sul piano assiologico, entrambe tutelassero gli stessi beni giuridici di dignità, autodeterminazione e identità della persona[93]. Dal raffronto tra le due discipline, insomma, si sarebbe dovuto ricavare che all'interno dei limiti stringenti posti dallo Statuto per il controllo a distanza, una volta installati i sistemi di sorveglianza, comunque ci si sarebbe dovuti attenere alla disciplina comunitaria di protezione dei dati personali affinché i dati raccolti fossero legittimamente trattabili e utilizzabili ai fini del rapporto di lavoro.

La realtà, tuttavia, ha dimostrato una notevole ritrosia della giurisprudenza nei confronti di una lettura integrata dei due strumenti normativi, della cui validità pure nessuno dubitava in dottrina: la ragione va con ogni probabilità rinvenuta nell'art. 114 del Codice della privacy, rubricato "Controllo a distanza", che dispone che:

Resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970, n. 300.

Tra il 1996 e il 2015, quando è entrata in vigore la riforma dell'art. 4 dello Statuto, non sono pertanto rinvenibili "significative pronunce giurisprudenziali che abbiano utilizzato le regole del Codice della Privacy per decretare l'inutilizzabilità dei dati raccolti, come peraltro da esso esplicitamente previsto all'art. 11"[94] e si può affermare che l'integrazione tra disciplina sui controlli a distanza e sul trattamento dei dati personali si è arrestata al piano dei provvedimenti dell'autorità garante, in quanto mancano sia leggi di rango primario dedicate alla privacy sul lavoro, sia una solida elaborazione da parte della giurisprudenza[95].

5. Il Jobs Act e le modifiche allo Statuto

Il 14 settembre 2015 è stato promulgato il D. Lgs. 151/2015, il penultimo dei decreti del cd. *Jobs Act* elaborato dal Governo Renzi. Tra le altre disposizioni contenute nel decreto, l'art. 23 ha disposto una modifica radicale dell'art. 4 dello Statuto dei Lavoratori. Il nuovo testo risulta così formulato:

---

92 M. T. CARINCI (2016), cit., p. VI.
93 A. INGRAO (2018), cit., p, 55.
94 M. T. CARINCI (2016), cit., p. VI.
95 A. INGRAO (2018), cit., pp. 66-67. Risultano solamente due sentenze isolate e piuttosto recenti che abbiano fornito una lettura integrata delle due normative: Cass. 1° agosto 2013, n. 18443 e Trib. Milano 23 giugno 2015 e App. Milano 4 agosto 2015, in *Il giuslavorista*.

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 e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione delle sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi.

La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.

Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.

Si possono condurre preliminarmente alcune osservazioni.

Innanzitutto, il divieto generale stabilito dal comma 1 della versione originale della L. 300/1970 non è più esplicitamente contemplato. Tale espunzione, tuttavia, secondo il parere della larghissima maggioranza dei commentatori, non dovrebbe condurre a ritenere che l'attività lavorativa possa essere oggetto legittimo di controlli a distanza[96] e pertanto dovrebbe persistere il limite esterno dato dall'impossibilità di installare sistemi con il fine diretto di sorvegliare i dipendenti. Rimane tuttavia un'area di incertezza, che deve essere colmata facendo riferimento al contenuto del nuovo art. 4.

[96] Tra i moltissimi, v. R. DEL PUNTA (2016), "La nuova disciplina dei controlli a distanza sul lavoro (art. 23, D. Lgs. n. 151/2015)", *Rivista italiana di diritto del lavoro*, n. 1 pp. 77-109; I. ALVINO (2016), "I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy", *Labour and Law Issues*, vo. 2 n. 1, pp. 2-45; P. LAMBERTUCCI (2016), "La disciplina dei controlli a distanza", *Giurisprudenza italiana*, n. 3, pp. 769-776.

Anche la struttura del nuovo art. 4 è bipartita: i primi due commi si occupano infatti di stabilire i casi in cui gli impianti di controllo a distanza possono essere installati e utilizzati, mentre il terzo comma disciplina le modalità con cui i dati raccolti possono essere trattati e opera – finalmente – un raccordo con il Codice della privacy.

Per prima cosa, il legislatore ribadisce la possibilità di installare impianti audiovisivi da cui potrebbe derivare controllo preterintenzionale, ma solo se si verificano determinate condizioni: devono essere impiegati (e non più devono essere "richiesti") per esigenze organizzative e produttive, di sicurezza del lavoro *o di tutela del patrimonio aziendale* – causale assente nella vecchia formulazione. Inoltre, come in precedenza, l'imprenditore che si voglia dotare di tali impianti deve seguire un procedimento specifico che passa per l'accordo con le rappresentanze sindacali oppure per l'autorizzazione da parte dell'ispettorato del lavoro competente.

Sin qui, insomma, l'impianto della norma non pare modificato nella sua sostanza: l'unica aggiunta riguarda la possibilità di controlli difensivi, peraltro già ammessa dalla giurisprudenza. È con il secondo comma, tuttavia, che il legislatore del 2015 opera lo stravolgimento più deciso dell'apparato protettivo del 1970.

I limiti finalistici e procedurali che si applicano agli strumenti di controllo "esterno", infatti, cessano di valere quando l'apparecchio che registra i dati del lavoratore è uno strumento di lavoro o uno strumento di registrazione degli accessi. Non è tuttavia pacifico cosa si intenda per "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa": se il comma 2 costituisce un'eccezione al comma 1, si devono probabilmente ritenere tali quei mezzi di cui il lavoratore si serve attivamente per eseguire la prestazione lavorativa, in una relazione di "stretta correlazione fra strumento di cui il lavoratore viene dotato e mansioni assegnate"[97].

Di conseguenza, è condivisibile l'interpretazione per cui gli strumenti che non vengono utilizzati dal lavoratore per rendere la prestazione, ma solamente dall'imprenditore per organizzarla – per esempio, i GPS che tracciano gli

[97] M. T. CARINCI (2017), cit., p. 52.

spostamenti degli autisti o dei fattorini – non ricadono nell'eccezione del comma 2 e sono sottoposti ai limiti di cui al comma 1[98].

Dal raccordo e dal confronto tra i primi due commi del nuovo art. 4, si può dunque rispondere all'interrogativo sui confini effettivi del divieto dei controlli a distanza: posto che permane un divieto di installazione ai fini di sorveglianza, e posto che è possibile installare nuovi apparecchi solamente alle condizioni indicate dal comma 1, è tuttavia possibile effettuare un controllo a distanza sull'*attività complessiva* del lavoratore o quando il controllo avviene (anche) per i motivi indicati dal comma 1, o quando avviene attraverso uno strumento di lavoro, e in questo caso si può trattare anche di controllo diretto[99].

La seconda parte dell'art. 4, costituita dal comma 3, introduce una disciplina sull'utilizzo dei dati registrati che fa proprio, finalmente, l'approccio eurounitario al diritto alla privacy, e che scioglie un nodo che il legislatore del 1970 non aveva potuto prevedere.

I dati raccolti con gli strumenti disciplinati dai primi due commi, infatti, sono utilizzabili "a tutti i fini connessi al rapporto di lavoro" (quindi anche disciplinari e, per quel che più interessa in questa ricerca, per il funzionamento degli algoritmi di management) a due condizioni: che sia data adeguata informazione ai dipendenti delle modalità con cui i dati sono raccolti e trattati, e che sia rispettata la disciplina del Codice della privacy, con esplicito rinvio.

È lecito chiedersi, per prima cosa, cosa si intenda per "informazione adeguata". Sul punto, bisogna ritenere che i regolamenti aziendali debbano fornire un'informativa esaustiva e debbano essere accessibili e comprensibili ai dipendenti[100].

In secondo luogo, pur apprezzando l'opera di riconoscimento e di raccordo con la disciplina della protezione dei dati personali, va riconosciuto che non era necessario alcun intervento normativo sul punto, poiché anche il Codice della privacy è legge vigente e sicuramente applicabile in tutti i casi di sorveglianza a distanza sul posto di lavoro. Il valore del rinvio dell'ultimo comma dell'art. 4 dello Statuto, allora, deve essere più che altro programmatico: richiama

---

[98] È, d'altronde, la posizione dello stesso Ministero del Lavoro: v. Comunicato stampa del Ministero del Lavoro del 18 giugno 2015, consultato online il 9/4/2021 all'indirizzo https://www.lavoro.gov.it/stampa-e-media/Comunicati/Pagine/20150618-Controlli-a-distanza.aspx

[99] M. T. CARINCI (2017), cit., pp. 54-55.

[100] M. T. CARINCI (2016), cit., p. XI.

all'attenzione dell'interprete la normativa sulla protezione dei dati personali e in qualche modo impone al giudice di considerarla nella soluzione dei casi a cui si ritiene applicabile[101]. Da questo punto di vista, l'ingresso sulla scena del diritto del lavoro di considerazioni legate specificamente alla materia del diritto alla privacy di matrice eurounitaria potrebbe senza dubbio arricchire la ricostruzione degli strumenti a disposizione del lavoratore per difendere la propria sfera personale dai pericoli delle nuove tecnologie[102].

La riforma dell'art. 4 ha acceso un grande dibattito tra gli studiosi, la politica e i protagonisti del mondo sindacale. Essa, per alcuni aspetti, ha preso atto degli approdi dei decenni precedenti (in particolare, per quanto riguarda i controlli difensivi), per altri ha operato una precisa scelta di politica del diritto volta a fornire una risposta a quelle voci che chiedevano un adeguamento dello Statuto dei Lavoratori alla realtà aziendale del XXI secolo[103].

Non si è trattato, tuttavia, di una semplice "manutenzione" della L. 300/1970, bensì di un'opera di profonda riforma che ha reso possibili forme di controllo prima vietate, alcune delle quali tipiche proprio del management attraverso algoritmi. Allo stesso tempo, l'attenzione prestata alla disciplina sulla privacy conferma un parziale cambio di prospettiva, che passa dal divieto di determinate forme di raccolta dei dati dei lavoratori alla loro *regolazione*[104].

6. Il GDPR e la prospettiva della protezione dei dati personali

Tale assetto dei rapporti tra imprenditore e dipendenti, nella tematica del potere di controllo, non era tuttavia destinata a rimanere stabile.

Il 27 aprile 2016, a poco più di sei mesi dalla riforma dello Statuto dei Lavoratori, il Consiglio e il Parlamento dell'Unione europea hanno promulgato il Regolamento generale sulla protezione dei dati 2016/679, detto anche GDPR. Direttamente applicabile a partire dal maggio 2018, il GDPR ha sostituito la precedente Direttiva 95/46 e ha provocato delle importantissime conseguenze sulla protezione della sfera personale del lavoratore, contribuendo a creare il

101 M. T. CARINCI (2017), cit. p. 57.
102 A. INGRAO (2018), cit., p. 56.
103 R. DE LUCA TAMAJO (1988), cit..
104 A. TROJSI (2016), "Controllo a distanza (su impianti e strumenti di lavoro) e protezione dei dati del lavoratore, *Variazioni su temi di diritto del lavoro*, n. 4 pp. 667 e sgg.

quadro attuale delle norme che possono essere applicate nel contrasto alle conseguenze negative del management attraverso algoritmi[105].

[105] V. *infra*, cap. 3.

Capitolo 3. La prospettiva eurounitaria: il GDPR può essere una risposta efficace alle esigenze del lavoro?

1. Il fondamento del diritto alla protezione dei dati personali

Si è appena visto che la Legge 300/1970 mette a disposizione dei lavoratori alcuni strumenti di fondamentale importanza che possono essere utilizzati per contrastare alcune storture legate allo scorretto esercizio del potere di controllo. È certamente possibile ipotizzare un possibile ricorso a tali strumenti nell'ambito del management attraverso algoritmi: così, per esempio, ancora oggi un datore di lavoro che voglia installare dei sistemi di sorveglianza dei dipendenti dovrà raggiungere un accordo con le rappresentanze sindacali o ottenere un'autorizzazione dall'ispettorato del lavoro; e allo stesso tempo sarà possibile ricorrere contro un imprenditore che utilizzi strumenti tecnologici per indagare su aspetti della vita personale dei dipendenti slegati dalla prestazione di lavoro, come il loro stato di famiglia o le attività svolte al di fuori dell'orario di lavoro[1].

Occorre però, a questo punto, osservare più da vicino la disciplina relativa alla protezione dei dati personali, rappresentata in questo momento dal Regolamento 2016/679 e, nel caso italiano, dal Codice della privacy: solo da una lettura integrata dei limiti al potere di controllo e della disciplina della privacy è infatti possibile ricavare il quadro complessivo della normativa applicabile al management attraverso algoritmi.

Il GDPR è il principale strumento di diritto europeo rivolto alla protezione dei dati personali, che può essere definito in sintesi come "diritto del soggetto a cui i dati si riferiscono di esercitare un controllo, anche attivo, su detti dati, che si estende dall'accesso alla rettifica"[2]. Per quanto strettamente collegato al diritto alla privacy, si tratta di un diritto dai tratti parzialmente diversi ed autonomi: vale dunque la pena precisarne meglio il contenuto.

---

[1] V. *supra*, cap. 2.

[2] G. FINOCCHIARO (2012), *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, ed. Zanichelli, p. 1.

Il diritto alla privacy, o riservatezza, è un diritto della personalità che ha avuto origine nella dottrina americana della fine del XIX secolo[3]. Il suo contenuto è essenzialmente negativo e consiste nel "diritto ad essere lasciati in pace" ("*right to be let alone*"[4]), ovvero, in termini più contemporanei, a non subire interferenze nella propria vita privata.

Si tratta di un diritto umano riconosciuto e protetto da diverse fonti sovranazionali. La Dichiarazione Universale dei Diritti Umani del 1948 – ratificata dall'Italia con la L. 848/1955 – è stata il primo documento adottato dalla comunità internazionale a riconoscere il diritto alla privacy: essa stabilisce all'art. 12 che "Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione".

Sul piano europeo, la Convenzione Europea sui Diritti dell'Uomo del 1950 stabilisce parimenti all'art. 8 che "Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza". Il contenuto esatto di tale diritto, che in Italia ha avuto una creazione essenzialmente giurisprudenziale[5], consiste nella possibilità del singolo di "escludere altri dalla conoscenza di vicende strettamente personali e familiari"[6] ed è un diritto della personalità ricondotto in ultima analisi protezione offerta dall'art. 2 della Costituzione[7].

Sia la Dichiarazione Universale dei Diritti Umani, sia la Convenzione Europea dei Diritti dell'Uomo, sia la Costituzione italiana risalgono a un epoca precedente all'adozione su larga scala di computer e allo sviluppo della società dell'informazione. A partire dagli anni '60, prendendo spunto da un processo di informatizzazione sempre più marcato in vari settori della società, il diritto alla privacy tradizionalmente inteso ha iniziato ad essere messo alla prova da nuove sfide e ad essere reinterpretato in una chiave diversa, ossia come "diritto

[3] In particolare viene considerate come pietra miliare il lavoro di S. WARREN, L. BRANDEIS (1890), "The right to privacy", *Harvard Law Review*, vol. 4 n. 5, pp. 193-220. Va comunque ricordato che alcuni importanti precedenti vanno rintracciati in realtà nella dottrina tedesca: v. F. BUSNELLI (1999), "Nota introduttiva al commento della l. 31 dicembre 1996, n. 675", *Nuove leggi civili commentate*, p. 228.
[44] *Ibid.*, p. 193.
[5] La Corte di Cassazione, dopo aver negato l'esistenza del diritto alla riservatezza in Cass. 22 dicembre 1956, n. 4487, lo riconobbe esplicitamente con Cass. 27 maggio 1975, n. 2129.
[6] G. FINOCCHIARO (2012), cit., p. 8.
[7] V. in particolare Cass. 22 giugno 1985, n. 3769.

all'autodeterminazione informativa" ("*informational privacy*")[8]: in questo senso, il contenuto di un tale diritto non è limitato alla tutela dalle altrui condotte intrusive nello spazio privato e familiare, ma si estende alla possibilità *positiva* del soggetto di diritto di controllare le informazioni che lo riguardano e che ne plasmano l'identità nello spazio pubblico[9].

Primi tentativi di disciplinare la materia dei dati personali risalgono all'inizio degli anni '70[10], ma è solo nel 1996 che l'Unione europea decide di dotarsi di un quadro giuridico unitario e coerente con la Direttiva 46 sul trattamento dei dati personali[11].

Ad oggi, il diritto dell'Unione europea guarda alla privacy e alla protezione dei dati personali come due fenomeni distinti: la Carta di Nizza del 2000, infatti, prevede all'art. 7 che "Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni", mentre all'art. 8, accogliendo il progressivo isolamento della *data protection* come valore autonomo, stabilisce che:

> *Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.*
>
> *Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.*
>
> *Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.*

Al caso del management attraverso algoritmi si applicano sicuramente entrambe le concezioni di riservatezza qui analizzate. Poiché tuttavia il GDPR si occupa specificamente di protezione dei dati personali, occorrerà sin d'ora considerare la specifica rilevanza di tale concetto.

---

[8] A. KISS, G. SZOKE (2015), *Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation*, in S. GUTWIRTH, R. LEENES, P. DE HERT, *Reforming European Data Protection Law*, ed. Springer, pp. 313 e sgg.

[9] R. ACCIAI (2004), *Il diritto alla protezione dei dati personali*, ed. Maggioli, pp. 38 e sgg.

[10] AA. VV. (2018), *Handbook on European Data Protection Law*, ed. European Union Agency for Fundamental Rights and Council of Europe, p. 18. Lo Stato Tedesco dell'Hesse fu il primo ad approvare una legge sulla protezione dei dati personali, proprio nel 1970 – v. nota 2.

[11] V. *supra*, cap. 2 par. 4.

2. *Il contesto storico e giuridico attorno al GDPR*

Come già ricordato più sopra, il primo atto dell'Unione europea – o meglio, di quella che in quel momento era la Comunità europea – che ha disciplinato i dati personali è stato la Direttiva 95/46. La Direttiva mirava a regolare la circolazione delle informazioni, scomponendo il trattamento dei dati in fasi e procedimentalizzandolo, cosicché fosse possibile un "controllo di conformità" alla normativa per ciascuna di esse[12]. L'approccio utilizzato era trasversale, nel senso che non distingueva tra le diverse possibili applicazioni pratiche, ma anzi attribuiva una serie di diritti all'interessato inteso come persona fisica[13].

Questo non significa che il legislatore europeo non ha tenuto in considerazione le particolari problematiche legate all'ambito lavorativo: esso anzi sembra accogliere, implicitamente, l'approccio suggerito dalla Raccomandazione del Consiglio d'Europa R (89) 2 del 1989, la quale riconosceva con notevole lucidità i rischi del trattamento informatico dei dati personali e proponeva di adottare una disciplina fondata sui principi di informazione e consultazione sui luoghi di lavoro[14].

In ogni caso, la Direttiva 95/46 si fonda su alcuni principi fondamentali, i cd. "principi sulla qualità dei dati", che sono descritti dal Titolo I. In base all'art. 6, i dati personali devono essere trattati "lealmente e lecitamente", per soddisfare "finalità determinate, esplicite e legittime"; essi devono essere adeguati e pertinenti, non devono eccedere la finalità per cui sono stati raccolti, devono essere "esatti e, se necessario, aggiornati"; infine, la loro conservazione non deve superare il tempo considerato necessario.

L'art. 7 stabilisce poi i presupposti di liceità del trattamento, almeno uno dei quali deve verificarsi appunto per consentire di qualificare un trattamento come lecito[15].

La Direttiva 95/46 realizzava un importantissimo punto d'arrivo di un lungo dibattito dottrinale, sviluppatosi nel ventennio precedente. Essa era basata su un approccio "statico", che teneva conto dell'evoluzione tecnologica dell'epoca e disciplinava esclusivamente lo scambio di dati tra interessato e titolare del

[12] A. INGRAO (2018), cit., p. 54.
[13] P. CHIECO (2020), cit., p. 21.
[14] Raccomandazione R (89) 2, par. 3.
[15] V. più diffusamente *supra*, cap. 2 par. 4.

trattamento[16]. Gli avvenimenti dei due decenni successivi hanno cambiato profondamente l'orizzonte applicativo della normativa elaborata negli anni '90: la diffusione sempre crescente di internet, le nuove funzionalità collegate agli smartphone e i social network sono solo alcuni degli elementi che permettono di parlare di un "modello di condivisione e cogestione di dati e informazioni, destinati fin dall'origine ad una circolazione globale"[17].

Un'altra caratteristica fondamentale della Direttiva 95/46 era la scelta stessa dello strumento di diritto europeo: lo scopo di una direttiva è quello di armonizzare le disposizioni dei singoli ordinamenti nazionali, e non è un caso che nel 1995 molti Stati membri – ma non l'Italia – avessero già approvato leggi a tutela dei dati personali dei cittadini[18].

Le direttive, tuttavia, non sono direttamente applicabili e necessitano di disposizioni di diritto interno che ne diano attuazione. In questo passaggio gli Stati membri sono obbligati a raggiungere certi risultati fissati dal legislatore europeo, ma sono tendenzialmente liberi con riferimento ai mezzi da utilizzare e, di conseguenza, hanno una notevole discrezionalità in merito alle scelte relative alla disciplina di dettaglio.

Il risultato della scelta dello strumento della direttiva non è stato del tutto quello sperato: invece di garantire una reale armonizzazione, la diversa ricezione da parte dei singoli legislatori nazionali ha prodotto nei fatti regole diverse all'interno dell'Unione europea per quanto riguarda la protezione dei dati personali[19]. A fronte di Stati membri che hanno dato un'interpretazione piuttosto rigorosa della Direttiva 95/46, tra i quali rientra sicuramente l'Italia, altri Paesi più attenti alle esigenze degli operatori economici hanno individuato parametri meno stringenti a cui assoggettare la circolazione dei dati personali.

Insomma, utilizzando le parole del legislatore europeo, "Sebbene i suoi obiettivi e principi rimangano tuttora validi, la direttiva 95/46/CE non ha impedito la

---

16 G. FINOCCHIARO (2017 A), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, ed. Zanichelli, p. 4.

17 *Ivi*; v. anche GDPR, considerando n. 6 – "La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che le riguardano […]".

18 Oltre al già ricordato Stato dell'Hesse, la Germania federale ha disciplinato la protezione dei dati personali nel 1976, la Svezia nel 1973, la Francia nel 1977, il Regno Unito nel 1984 e i Paesi bassi nel 1989 – v. AA. VV. (2018), *Handbook* cit., p. 29, nota 30.

19 G. FINOCCHIARO (2017 a), cit., p. 8.

frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche"[20].

Di conseguenza, quando si è trattato di provvedere a una revisione della disciplina, la Commissione ha optato per un regolamento, strumento che a differenza della direttiva non richiede alcun intervento da parte degli Stati membri e, avendo portata generale, produce i suoi effetti nei confronti di tutti i cittadini europei[21]. Il fine del GDPR, che sostituisce la disciplina precedente[22], non è più l'armonizzazione delle normative degli stati membri (per quanto continui ad esistere uno spazio per discipline di settore di produzione nazionale[23]), bensì l'uniformazione del diritto alla protezione dei dati personali, in vista della creazione di un "mercato unico digitale"[24].

Le esigenze alla base dell'elaborazione del Regolamento 2016/679 sono dunque la volontà di adeguare ai nuovi mezzi tecnologici la precedente disciplina e il superamento delle difformità normative nei singoli Stati membri. Il legislatore europeo, tuttavia, non si è limitato a un'opera di *manutenzione*, ma, facendo tesoro dell'esperienza di vent'anni di applicazione della Direttiva 95/46, ha riformato alcuni aspetti dell'impianto della disciplina della protezione dei dati personali, a partire dal principio di *accountability*.

In base alla precedente direttiva, infatti, il trattamento di dati "sensibili"[25] – le categorie di informazioni legate alla sfera più intima dell'individuo e potenzialmente in grado di dare origine a situazioni discriminatorie – era possibile solo a determinate condizioni. In particolare, in Italia esso era

[20] V. GDPR, considerando n. 9.
[21] R. ADAM, A. TIZZANO (2020), *Manuale di diritto dell'Unione europea*, ed. Giappichelli, p. 180. Per quanto di interesse di questa trattazione, va poi sottolineato che nell'ambito del lavoro una armonizzazione delle discipline degli Stati membri sarebbe stata in ogni caso molto difficile da raggiungere, date le profonde differenze di approccio delle norme lavoristiche nazionali.
[22] GDPR, art. 94 par. 1.
[23] GDPR., considerando n. 10.
[24] V. Parere del Comitato Economico e Sociale Europeo INT/823, "Il mercato unico digitale - Tendenze e prospettive per le PMI".
[25] Così definiti dal Codice della privacy italiano, ma si tratta dell'elenco individuato dall'art. 8 par. 1 della Direttiva 95/46: "dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché il trattamento di dati relativi alla salute e alla vita sessuale".

sottoposto a un regime di autorizzazione preventiva da parte del Garante della Privacy, che definiva a priori le modalità e i limiti dell'utilizzo di tali dati[26].

Tale approccio autorizzatorio, tuttavia, non era risultato risolutivo e l'impianto della Direttiva nel suo complesso non era stato in grado di "garantire che gli obblighi in materia di protezione dei dati si traducano in meccanismi efficaci atti a fornire una protezione reale"[27]. Di conseguenza, il GDPR ha introdotto un nuovo regime basato sulla responsabilizzazione del titolare del trattamento, il quale deve in prima persona valutare quali misure tecniche adottare per ogni specifico contesto e garantire l'effettiva protezione dei dati personali in ogni momento, sorvegliare l'applicazione di tali misure e valutare il rischio avvalendosi anche di esperti nel settore[28]. Sul piano processuale, l'onere della prova del fatto di aver adottato di un modello organizzativo efficace riposa ora sul titolare del trattamento e il suo mancato raggiungimento comporta l'attribuzione di responsabilità civile e amministrativa[29].

Il GDPR, come detto, adotta un approccio "omnibus" e si applica ad ogni persona fisica; tuttavia, esso tiene conto delle specifiche esigenze del rapporto di lavoro, individuate ed evidenziate da documenti di fondamentale importanza come la Raccomandazione (2015) 5 del Consiglio d'Europa sul trattamento di dati personali nel contesto occupazionale. Il legislatore europeo era consapevole che le differenze di implementazione della Direttiva 95/46 negli ordinamenti nazionali avevano causato problemi la cui soluzione era ancora più urgente proprio nell'ambito del lavoro[30].

Già nel 2002 la Commissione aveva lanciato una consultazione con le parti sociali, al termine della quale aveva elaborato una serie di proposte rivolte specificamente al trattamento di dati sul posto di lavoro tra le quali, in particolare, l'obbligo di consultazione delle associazioni sindacali prima di installare nuovi strumenti informatici, l'obbligo di autorizzazione delle autorità nazionali di protezione dei dati personali per poter esercitare il controllo a

---

26 V. D. Lgs. 196/2003, art. 40, poi abrogato dal D. Lgs. 101/2018. A tale regime, peraltro, erano sottoposti i trattamenti di dati sul luogo di lavoro: v. F. IAQUINTA, A. INGRAO (2014), "La *privacy* e i dati sensibili del lavoratore legati all'utilizzo di *social networks*. Quando prevenire è meglio che curare", *Diritto delle relazioni industriali*, n. 4 pp. 1027 e sgg.

27 WP 29, Parere n. 3/2010 sul principio di responsabilità, par. 3.

28 G. FINOCCHIARO (2017 a), cit., pp. 13-14.

29 V. F. DI RESTA (2018), *La nuova* privacy *europea. I principali adempimenti del regolamento UE 2016/679 e profili risarcitori*, ed. Giappichelli.

30 V., per esempio, Article 29 – Data Protection Working Party, rapporto 5401/01/EN/Final, "Working document on the surveillance of electronic communications in the workplace".

distanza sui dipendenti e il divieto di sorveglianza all'insaputa dei lavoratori, salvo casi eccezionali[31]. Queste proposte, tuttavia, non hanno avuto un reale seguito e l'argomento della protezione dei dati personali dei lavoratori è rimasto in secondo piano fino alla fine del decennio, nel sostanziale disinteresse delle parti sociali[32]. Ancora nel 2010, a fronte di una nuova consultazione aperta al pubblico, il tema non pareva prioritario nell'agenda dei sindacati, almeno a livello nazionale, mentre alcune grandi società dell'informazione colsero l'occasione per esprimere i propri dubbi riguardo alla prospettiva di una revisione della Direttiva 95/46[33].

Il GDPR ha un sicuro impatto sul luogo di lavoro. Nei prossimi paragrafi si indagheranno alcuni degli elementi salienti che, ragionevolmente, lo rendono uno strumento adatto a rispondere alle esigenze di riservatezza dei lavoratori che entrano in contatto con tecnologie di management attraverso algoritmi.

3. *L'ambito soggettivo di applicazione: le figure individuate dal regolamento e il Data Protection Officer*

Il Regolamento 2016/679[34], così come la precedente Direttiva[35], individua alcuni soggetti che sono coinvolti nel trattamento dei dati personali e assegna loro determinati diritti ed obblighi. Poiché il Regolamento si applica anche al rapporto di lavoro, ma non è pensato specificamente per esso, in alcuni casi i ruoli individuati dal GDPR si sovrappongono a quelli di soggetti già incaricati di specifiche funzioni nell'ambito del rapporto di lavoro, mentre in altri casi il Regolamento crea delle figure precedentemente sconosciute alla disciplina lavoristica.

I soggetti necessari nel trattamento sono due: il titolare e l'interessato.

Il titolare è definito dalla disciplina vigente come:

---

31 I risultati della consultazione del 2002 si possono rinvenire nel documento della Commissione europea, Report COM(2003) 265 final, "First report on the implementation of the Data Protection Directive (95/46/EC)".

32 C. FRITSCH (2015), cit., p. 155.

33 *Ivi.*

3434 Regolamento 2016/679/UE, art. 4 ("Definizioni").

35 Direttiva 95/46/CE, art. 2 ("Definizioni").

> *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali […]*[36]

Si tratta di un soggetto attivo del trattamento, nello specifico il "centro di imputazione delle decisioni in ordine al trattamento dei dati da esso effettuato"[37]. Esso non viene individuato a priori, ma la sua qualificazione discende da un'osservazione della realtà di fatto: il soggetto che detiene l'effettivo potere decisionale sulle varie fasi del trattamento viene ricondotto a questa figura.

La nuova disciplina assegna al titolare un ruolo ancora più centrale all'interno dell'impalcatura del sistema della protezione dei dati personali: se già prima il titolare era il responsabile ultimo della riservatezza e dell'integrità dei dati, con la comparsa del principio di responsabilizzazione tale responsabilità si estende alla fase preventiva e richiede quindi un ruolo decisamente attivo al soggetto che ricopre questo ruolo[38].

Il titolare, in quanto direttamente responsabile della sicurezza del trattamento dei dati personali raccolti, deve istituire un'organizzazione a ciò idonea, nominando altri soggetti a loro volta previsti dal GDPR, come il "responsabile" e le "persone fisiche autorizzate".

Il responsabile, definito dal Regolamento come il soggetto che "tratta dati personali per conto del titolare"[39], è designato dal titolare tra le figure che "presentino garanzie sufficienti"[40] e svolge per suo conto operazioni strumentali rispetto alle finalità del trattamento, a loro volta predeterminate dal titolare. Finalità e modalità del trattamento sono stabilite da un atto di designazione, ossia un contratto il cui contenuto è disciplinato minuziosamente dall'art. 28 par. 3 del GDPR.

Tra i compiti del responsabile rientra l'adempimento di obblighi preventivi, come l'istituzione del registro di cui all'art. 30 par. 2, l'eventuale nomina del *Data Protection Officer* e la comunicazione al titolare di tutte le violazioni

---

36 GDPR, art. 4 n. 7.
37 L. GRECO (2017), *I ruoli: titolare e responsabile*, in G. FINOCCHIARO (2017 a), cit., p. 252.
38 *Ibid.*, p. 254.
39 GDPR, art. 7 n. 8.
40 GDPR, art. 28, par. 1.

riscontrate[41]. Con riguardo a tali obblighi, egli è personalmente responsabile in sede amministrativa.

Dall'altro lato del rapporto di trattamento dei dati personali sta l'interessato, cioè la persona fisica a cui appartengono i dati. L'interessato non è un semplice soggetto passivo del trattamento, e anzi è l'obiettivo stesso della protezione dei dati personali garantire che i soggetti a cui tali dati si riferiscono possano esercitare su di essi e sulla loro circolazione un controllo sufficiente[42].

Nella prospettiva lavoristica è relativamente semplice individuare l'interessato del trattamento: questi coincide con il lavoratore i cui dati sono raccolti sul posto di lavoro[43]. Su questo punto, tuttavia, una semplice considerazione risulta di fondamentale importanza nel raffronto della normativa europea sulla privacy con la normativa italiana sui controlli: lo Statuto dei Lavoratori, elaborato alla fine degli anni '60, ha come punto di riferimento il rapporto di lavoro subordinato *standard* e non si applica ad alcune situazioni particolarmente segnate dal fenomeno del management attraverso algoritmi, in particolare il lavoro tramite piattaforma[44]. La conseguenza è che l'art. 4 e l'art. 8 non trovano applicazione proprio nei casi in cui i lavoratori sono più deboli e il controllo nei loro confronti è più intrusivo.

Quando invece la normativa del GDPR considera il lavoratore, subordinato o autonomo, solo formalmente o anche nella pratica, nella veste di interessato del trattamento, essa si disinteressa della natura del rapporto di lavoro: l'annoso problema della qualificazione dei *riders*, per esempio, non è in alcun modo risolto dalla disciplina europea, ma la protezione dei dati personali dei lavoratori tramite piattaforma non è per questo indebolita. Poiché il punto di riferimento del GDPR non è legato ad alcuno specifico settore, ma anzi consiste nel concetto più ampio possibile di cittadino, quello di *persona fisica*, l'estensione della protezione dei dati personali è trasversale e interessa tutti i rapporti di lavoro[45].

Più complessa è l'individuazione del titolare: se si fa riferimento al principio di effettività esaminato poc'anzi, bisogna riconoscere che il titolare del trattamento non sempre coinciderà con il datore di lavoro formale – la controparte datoriale

---

41 GDPR, art. 33 par. 2.
42 S. RODOTÀ (1997), "Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali", *Rivista critica di diritto privato*, n. 1 pp. 583 e sgg.
43 A. INGRAO (2018), cit., p. 96.
44 Sul punto, v. Trib. Torino, sentenza del 7 maggio 2018 n. 788, in *Il Giuslavorista.*
45 V. ancora A. INGRAO (2018), cit., p. 73.

nel contratto di lavoro – ma talvolta occorrerà indagare al di fuori del perimetro contrattuale per qualificare come "centro di imputazione" del trattamento il soggetto che ne ha un reale interesse[46]. In questo senso, questa dissociazione tra datore formale e titolare del trattamento potrebbe proporsi in contesti particolarmente rilevanti e discussi in dottrina come i gruppi di imprese, gli appalti, le reti e in generale i fenomeni di *outsourcing*[47].

Il lavoratore, tuttavia, potrebbe non rivestire solamente il ruolo di interessato. Il Codice della privacy italiano, così come riformato dalla L. 163/2017, prevede infatti ora all'art. 2-quaterdecies la figura del soggetto *autorizzato*, una qualifica erede dell'*incaricato* presente nella precedente versione del Codice ma è contemplata implicitamente dal GDPR all'art. 29[48]. Si tratta di una persona fisica sotto l'autorità del responsabile o del titolare, a cui vengono attribuiti "specifici compiti e funzioni connessi al trattamento di dati personali": è evidente che tale descrizione si adatta particolarmente bene a quei dipendenti preposti dall'imprenditore-titolare al trattamento di determinate categorie di dati per finalità connesse alle loro mansioni.

I dipendenti autorizzati possono procedere con il trattamento solo se "istruiti"[49] dal datore e, di conseguenza, hanno una competenza limitata dalle direttive ricevute. Concretamente, in virtù del principio di minimizzazione, i soggetti autorizzati devono poter accedere solamente alle informazioni connesse alle loro mansioni[50]. In caso di trasgressione delle direttive, se il dipendente effettua il trattamento di dati a cui non era autorizzato, è fuor di dubbio che sia sottoposto a responsabilità disciplinare[51].

Un'ultima figura di notevole interesse per quanto riguarda il rapporto di lavoro è quella del *Data Protection Officer* (o DPO)[52]. Tale figura, tratta dall'esperienza di Germania e Austria[53], costituisce un'importante novità per la disciplina europea

---

46 V. Garante della privacy, provvedimento 23/11/2006 "Linee-guida per il trattamento dei dati dei dipendenti privati". Sul versante europeo, cfr. WP29, parere 00264/10/IT del 16/2/2010 "sui concetti di «responsabile del trattamento» e «incaricato del trattamento»".

47 A. INGRAO (2018), cit., p. 97.

48 L. GRECO (2017), cit., p. 272.

49 GDPR, art. 29.

50 GDPR, art. 32 par. 4.

51 A. INGRAO (2018), cit., p. 102.

52 Nella versione italiana del Regolamento tale soggetto è denominato "responsabile per la protezione dei dati personali"; tuttavia, per evitare possibili confusioni con la figura del responsabile del trattamento, si preferisce qui mantenere la denominazione in lingua inglese – peraltro di uso corrente anche nella dottrina italiana.

53 Non è infatti un caso che i sindacati di questi Paesi abbiano avanzato come principale richiesta in sede di consultazione con la Commissione che il DPO fosse obbligatorio in ogni luogo di lavoro e

della protezione dei dati personali. Essa è prevista dagli artt. 37, 38 e 39 del GDPR e può essere visto come "una figura manageriale, con funzioni di consulenza e controllo, assimilabile, per taluni aspetti […] alle funzioni svolte da un organismo di vigilanza"[54].

La nomina di un DPO è obbligatoria solo in certi casi: sempre nel contesto di autorità e organismi pubblici, oppure, se si tratta di privati, solo se le loro attività principali "consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala"[55] oppure in trattamenti, su larga scala, di "categorie particolari di dati personali"[56]. I criteri individuati, che hanno sostituito una precedente proposta che invece legava l'obbligo del Data Protection Officer a un numero minimo di dipendenti dell'azienda, lasciano probabilmente spazio a controversie interpretative riguardo al significato di "monitoraggio regolare e sistematico", "attività principali" e, soprattutto, di "larga scala". In ogni caso, è ipotizzabile che almeno quelle applicazioni di management che richiedono una raccolta costante di dati riferibili ai lavoratori (per esempio, il sistema di registrazione delle performance degli autisti UPS esaminato in precedenza[57]) richiedano necessariamente la presenza di un DPO, in quanto tra le "attività principali" rientrano anche le "operazioni essenziali che sono necessarie per il raggiungimento degli obiettivi perseguiti dal titolare"[58].

Per la natura del ruolo, è necessario che la persona nominata come Data Protection Officer sia dotata di una particolare professionalità ed esperienza nel campo giuridico e della protezione dei dati personali[59]. La designazione avviene da parte del titolare del trattamento[60] e il DPO potrebbe anche essere un dipendente dell'azienda[61], ma è di fondamentale importanza che egli mantenga

---

che fosse indipendente dal datore – v. C. FRITSCH (2015), cit., p. 162, ma anche P. SCHAAR (2013), "Die geplante EU-Datenschutz-Grundverordnung, Auch beim Beschäftigtendatenschutz ist ein Nachbessern erforderlich", *Computer und Arbeit* n. 3. In ogni caso, l'estensione dell'esperienza del DPO a tutti gli stati membri è stata fortemente voluta dalle confederazioni sindacali sovranazionali: v. ETUC, "ETUC position in the General Data Protection Regulation. Improving the protection of workers' data", p. 207.

54 A. AVITABILE (2017), *Il data protection officer*, in G. FINOCCHIARO (2017 a), cit., p. 334.

55 GDPR, art. 37 par. 1 lett. b).

56 GDPR, art. 37 par. 1 lett. c).

57 V. *supra*, cap. 1 par. 5.

58 Article 29 – Data Protection Working Party, WP 243 rev. 01, "Linee guida sui responsabili della protezione dei dati", p. 27.

59 GDPR, considerando n. 97.

60 GDPR, art. 37 par. 1.

61 GDPR, art. 37 par. 6.

la propria indipendenza e autonomia rispetto all'interno dell'organizzazione aziendale: non gli deve essere impartita alcuna istruzione e non può essere rimosso o penalizzato per aver adempiuto ai propri compiti[62].

Le funzioni del Data Protection Officer sono molteplici. In primo luogo, egli partecipa assieme al titolare del trattamento alla determinazione dei fini e delle modalità del trattamento, mettendo a disposizione le proprie competenze tecniche per garantirne la legalità. Nell'ambiente di lavoro, il DPO può essere in questa fase un importante *contrappeso* nei confronti di un imprenditore che voglia installare sistemi illeciti di controllo a distanza o, in generale, richieda di raccogliere i dati dei dipendenti secondo modalità non conformi alla legge[63].

In secondo luogo, il DPO si interfaccia con i lavoratori in più occasioni: in base all'art. 34 del GDPR, egli deve comunicare senza ritardo al lavoratore interessato ogni eventuale violazione dei dati personali, utilizzando un linguaggio semplice e chiaro. Inoltre, in linea generale, i lavoratori possono rivolgersi a lui "per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti"[64]: tale formula, dall'alto contenuto di indeterminatezza, lascia aperta la possibilità di un coinvolgimento del DPO da parte dei singoli interessati così come delle rappresentanze sindacali in un grandissimo numero di situazioni riguardanti la privacy dei dipendenti[65].

Infine, il DPO ha rapporti costanti con il Garante nazionale, con il quale deve cooperare soprattutto nel caso in cui dalla valutazione dei rischi emergano particolari criticità[66].

Tuttavia, il momento in cui forse è maggiormente percepita l'importanza della figura del DPO è la valutazione d'impatto sulla protezione dei dati di cui all'art. 35 del Regolamento. Qui la sua presenza è infatti obbligatoria e anzi è richiesto un suo parere preventivo sulla necessità della valutazione stessa e sull'opportunità di affidarla a un organismo esterno[67].

Il Data Protection Officer è insomma una figura di garanzia che permette un migliore collegamento tra i soggetti a vario titolo coinvolti nel trattamento (datore, lavoratori e Autorità Garante) e che porta nel contesto dell'azienda una

---

62 GDPR, art. 48 par. 3.
63 A. INGRAO (2018), cit., p. 108.
64 GDPR, art. 38 par. 4.
65 A. AVITABILE (2017), cit., p. 359.
66 GDPR, art. 39 par. 1 lett. d) ed e).
67 Per maggiori dettagli, v. *infra*, par. 5.

particolare competenza, con ciò migliorando la qualità delle decisioni relative ai dati personali. Va comunque sottolineato che il DPO è stato introdotto nel nostro e in altri ordinamenti nazionali solo di recente – il GDPR è infatti entrato in vigore solo nel 2018: gli sviluppi successivi del potenziale di questa figura sono rimessi alla prassi e andranno indagati nel corso dei prossimi anni.

4. Liceità del trattamento e consenso del lavoratore

Il principio di liceità, sancito dall'art. 5 par. 1 lett. a) del Regolamento, prevede che i dati debbano essere "trattati in modo lecito, corretto e trasparente". Affinché il trattamento possa essere lecito, il successivo art. 6 individua alcuni presupposti, o "condizioni" di liceità, attraverso le quali il legislatore europeo ha selezionato a monte alcuni meccanismi che consentono di "approdare alla giusta composizione degli interessi contrapposti dell'interessato e del titolare del trattamento"[68].

Tra le condizioni di liceità non esiste alcuna gerarchia ed è sufficiente che se ne realizzi una affinché il trattamento possa essere legittimamente svolto; tuttavia, è innegabile che tanto nell'impianto normativo quanto nella prassi il consenso dell'interessato ha sempre ricoperto un ruolo fondamentale[69].

Il GDPR, che non reca novità sostanziali rispetto alla precedente Direttiva quanto al novero delle condizioni di liceità del trattamento, specifica però in maniera più approfondita le caratteristiche che il consenso deve avere per poter essere considerato valido: in particolare, come prescritto dal considerando n. 32, il consenso è definito dall'art. 4 n. 11 come:

> *qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.*

A tal proposito, il considerando n. 42 prescrive che la dichiarazione di prestazione del consenso, quando predisposta dal titolare, "usi un linguaggio semplice e chiaro e non contenga clausole abusive" e che l'interessato sia messo a conoscenza dell'identità del titolare e delle finalità del trattamento.

---

[68] R. MAZZAMUTO (2006), *Il principio del consenso e il problema della revoca*, in R. PANETTA (2006), *Libera circolazione e protezione dei dati personali*, ed. Giuffré, vol. 1 p. 993.
[69] V. F. BRAVO (2017), *Il consenso e le altre condizioni di liceità*, in G. FINOCCHIARO (2017 a), cit., p. 138.

Affinché però sia soddisfatto il requisito della libertà, la scelta deve essere autenticamente libera ed esente da condizionamenti e l'interessato non deve rischiare di subire alcuna conseguenza per il diniego o la revoca del proprio consenso[70].

Di conseguenza, in tutti quei casi in cui è presente un "evidente squilibrio" tra le parti, il consenso non può costituire un valido fondamento giuridico[71]: indici tipici di un tale squilibrio, che permettono di presumere l'invalidità del consenso, sono l'impossibilità di prestare un consenso separato per parti o la subordinazione al consenso dell'esecuzione di un contratto di cui è parte l'interessato[72].

La dottrina ha discusso per lungo tempo la possibilità di considerare valido un consenso prestato all'interno del rapporto di lavoro[73]; oggi la soluzione negativa pare accettata dalla dottrina prevalente e addirittura accolta da organi dell'Unione europea stessa, con funzione consultiva, come l'Article 29 Data Protection Working Party, un gruppo di lavoro indipendente composto da esperti nazionali della materia incaricati di analizzare i principali problemi legati alla protezione dei dati personali prima dell'entrata in vigore del GDPR.

Nel Parere 2/2017 "sul trattamento dei dati sul posto di lavoro", viene riconosciuto che, a causa della subordinazione implicita nel rapporto di lavoro dipendente, "i dipendenti non sono quasi mai nella posizione di poter concedere, rifiutare o revocare liberamente il consenso al trattamento dei dati"[74]. Di conseguenza, il consenso può essere considerato valido solo in circostanze eccezionali, e marginali nella pratica, in cui nessuna conseguenza può derivare al prestatore di lavoro in caso di diniego[75]: per esempio, il caso in cui al lavoratore venga richiesto, a sua discrezione, di completare un profilo personale disponibile nell'intranet aziendale con dettagli come una propria fotografia affinché sia subito riconoscibile alle riunioni[76].

---

70 GDPR, considerando n. 42. Nella stessa direzione va anche il Consiglio d'Europa, "Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data", n. 108/2018.

71 GDPR, considerando n. 43, che rinvia, ma solo a titolo esemplificativo, al caso in cui il titolare del trattamento è un'autorità pubblica.

72 *Ivi.*

73 V. A. SITZIA (2016), "Il controllo (del datore di lavoro) sull'attività dei lavoratori: il nuovo articolo 4 st. Lav. e il consenso (del lavoratore)", *Labour and Law Issues*, vol. 2 n. 1 pp. 83 e sgg.

74 Article 29 Data Protection Working Group, Opinione 2/2017 "sul trattamento dei dati sul posto di lavoro", versione italiana, p. 26.

75 *Ivi.*

76 AA. VV. (2018), *Handbook*, cit., p. 145.

La pratica di consensi prestati all'atto dell'assunzione, oppure attraverso modelli prestampati, o addirittura ricavati da comportamenti concludenti, per quanto non scorretta in sé, non è tuttavia in grado di legittimare il trattamento secondo la normativa europea vigente[77].

È evidente che in molti casi di impiego di management attraverso algoritmi (per praticità, ci si può rifare nuovamente al caso dei furgoni UPS) lo spazio di autodeterminazione del lavoratore interessato nella prestazione del consenso è estremamente ridotto. Ai sensi del GDPR, insomma, la raccolta dei dati dei dipendenti su larga scala, in una prospettiva sistematica e coessenziale al modello di business scelto dall'imprenditore – come è quella svolta nella quasi totalità delle applicazioni di MAA – non potrà fondarsi sul consenso dei lavoratori.

Tuttavia, come accennato in precedenza, il consenso dell'interessato non è l'unico presupposto legittimante del trattamento dei dati personali previsto dall'art. 6 e già prima dell'approvazione del Regolamento 2016/679 era stato individuata come alternativa quella dell'interesse legittimo, che l'ordinamento italiano considerava nel contesto del Codice della privacy previgente un'ipotesi eccezionale e derogatoria rispetto al *principio generale* del consenso[78].

Innanzitutto, l'esistenza di un interesse legittimo deve essere valutata caso per caso, senza che sia possibile a priori fornire una definizione che racchiuda tutti i casi. Si ritiene comunque che un interesse legittimo sia riscontato nella maggioranza dei casi in cui sussiste una relazione qualificata tra l'interessato e il titolare, "ad esempio quando l'interessato è un cliente o è alle dipendenze del titolare del trattamento"[79].

In secondo luogo, l'interesse del titolare deve essere bilanciato con gli interessi e con i diritti del soggetto interessato: solo se tale bilanciamento è favorevole al titolare il trattamento si può considerare lecito. In questa operazione valutativa rientrano vari criteri, tra i quali, segnatamente, le ragionevoli aspettative dell'interessato anche in virtù del rapporto che lo lega al titolare[80].

Inoltre, nel caso in cui un trattamento si basi sull'interesse legittimo del titolare è previsto dall'art. 21 il diritto dell'interessato di opporsi: a quel punto, il titolare

---

77 A. INGRAO (2018), cit., p. 112.

78 G. PROIA (2016), "Trattamento dei dati personali, rapporto di lavoro e l'«impatto» della nuova disciplina dei controlli a distanza", *Rivista italiana di diritto del lavoro*, vol. 1 n. 4 pp. 547 e sgg.

79 GDPR, considerando n. 47.

80 *Ivi.*

deve specificamente dimostrare "l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato" o interrompere il trattamento[81].

All'interno del rapporto di lavoro, in molte occasioni è possibile riscontrare l'esistenza di un legittimo interesse del datore. In questi casi, soccorre l'interprete nel giudizio di bilanciamento degli interessi il cd. *disciplinare interno*, un regolamento aziendale reso noto ai dipendenti cui il datore-titolare è obbligato in base all'art. 24 par. 2 del GDPR. La dottrina prevalente ritiene che tale adempimento corrisponda al requisito di "adeguata informazione" di cui all'art. 4 comma 3 dello Statuto dei Lavoratori: attraverso il disciplinare, cioè, il lavoratore riceverebbe le regole d'uso degli strumenti di lavoro e con ciò le informazioni necessarie in merito alla raccolta dei suoi dati.

Il disciplinare, tuttavia, ha anche un altro effetto: informando il lavoratore in merito ai controlli che possono essere eseguiti attraverso gli strumenti di lavoro, questo documento ha anche la funzione di "circoscrivere l'*aspettativa di privacy*"[82] e con ciò fornire un metro di comparazione nell'operazione di bilanciamento del legittimo interesse.

Per quanto riguarda gli esempi esaminati in riferimento al management attraverso algoritmi, la volontà di raccogliere dati sul posto di lavoro per aumentare l'efficienza dell'organizzazione, la sicurezza, o anche prevenire danni al patrimonio aziendale, costituisce senza molti dubbi un interesse legittimo. Tuttavia, nella successiva fase del giudizio prognostico – il bilanciamento tra gli interessi del datore e i diritti del lavoratore – occorre particolare attenzione. Il trattamento dei dati, infatti, sarà lecito solo se strettamente necessario rispetto alle finalità individuate dall'imprenditore; inoltre, le modalità con cui in concreto verrà effettuato il trattamento dovranno rispondere a un generale principio di proporzionalità, e si dovrà accertare "se tutti i dati sono necessari, se il trattamento viola i diritti generali alla vita privata di cui godono i dipendenti anche sul posto di lavoro, e le misure da adottare per garantire che le violazioni dei diritti alla vita privata e alla segretezza delle comunicazioni siano limitate al minimo necessario"[83].

---

[81] GDPR, art. 21 par. 1.
[82] A. INGRAO (2018), cit., p. 128.
[83] Article 29 Data Protection Working Group, Opinione 2/2017 "sul trattamento dei dati sul posto di lavoro", versione italiana, p. 26.

Negare la possibilità di raccogliere i dati necessari agli algoritmi di management del personale basandosi sul consenso dei lavoratori comporta quindi un'importante conseguenza: se si inquadra il trattamento nella categoria dell'interesse legittimo, ai lavoratori non potrà essere richiesto qualsiasi sacrificio della propria riservatezza a fronte del semplice consenso, ma sarà necessario che il trattamento rimanga entro i limiti di proporzionalità, di necessità e di sussidiarietà stabiliti dal GDPR. In altri termini, cioè, il Regolamento pone dei limiti alla disponibilità del diritto soggettivo del lavoratore alla privacy sul posto di lavoro e, riconosciuto lo squilibrio tra datore e dipendente, realizza a priori un bilanciamento degli interessi non basato sulla volontà delle parti ma su una gerarchia di valori individuata dal legislatore, in maniera non dissimile dallo Statuto dei Lavoratori al Titolo I[84].

5. L'approccio preventivo: un confronto con lo Statuto dei Lavoratori

Una delle caratteristiche principali della disciplina europea della protezione dei dati personali, per la quale essa di differenzia in maniera sostanziale dallo Statuto dei Lavoratori, è l'approccio di fondo basato sulla prevenzione del rischio.

Lo Statuto dei Lavoratori, nel suo Titolo I, impone dei precisi limiti negativi al potere di controllo del datore, vietando determinate attività di sorveglianza agli artt. 4, 6 e 8 e assistendo tali divieti con sanzioni di natura penale[85]. Gli obblighi imposti al datore di lavoro, insomma, sono obblighi di *non facere*, e gli strumenti a tutela dei diritti dei dipendenti hanno natura successiva.

Il GDPR, al contrario, adotta un approccio innovativo, mutuato dalla prevenzione nell'ambito della sicurezza dei lavoratori[86]. Partendo dalla constatazione che l'elemento del rischio è connaturato all'attività di trattamento dei dati personali, e anzi costituisce da sempre una delle principali ragioni per cui si è resa necessaria l'elaborazione di una disciplina[87], il legislatore europeo

---

[84] Cfr. P. ICHINO (1986), cit., pp. 54-55.

[85] L'art. 38 colpiva con un'ammenda le violazioni di tutti e tre gli articoli; a seguito della riforma del 2015, la lettera della legge continua a punire solamente le i trasgressori dell'art. 6 (visite personali), ma si ritiene che le sanzioni continuino ad operare per il tramite di rinvii anche con riguardo alle altre due fattispecie – cfr. M. T. CARINCI (2015), cit., p. XII.

[86] L. D'ARCANGELO (2020), "L'obbligo di protezione dei dati del lavoratore: adempimento e sanzioni", *Diritti lavori mercati*, vol. 1, p. 79.

[87] P. MAYER-SCHONBERGER (1997), *Generational developement of data protection in Europe?*, in P. AGRE, M. ROTENBERG (1997), *Technology and Privacy*, ed. MIT Press, p. 221.

ha impostato tutto l'impianto del GDPR[88] sui concetti di *accountability* del titolare e, quindi, di gestione del rischio da parte sua[89]. Il titolare del trattamento – nel nostro caso, il datore di lavoro – non solo è tenuto a comunicare tempestivamente ogni eventuale violazione dei dati personali (cd. *data breach*) all'autorità di controllo[90] e all'interessato i cui dati sono stati violati[91], ma in virtù del principio di responsabilizzazione è tenuto ad adottare misure idonee ad evitare tali violazioni.

La gestione del rischio è sottoposta a una regolamentazione rigorosa, ma non chiusa: il titolare non deve rispettare degli standard prefissati per legge, ma deve di volta in volta scegliere ed attuare il modello più efficace e garantire che funzioni nella pratica[92]. Tale modello è strettamente correlato ai concetti di *privacy by design* e *privacy by default*[93], prescritti dall'art. 25 del Regolamento: il titolare del trattamento deve "disegnare" un sistema connotato da misure tecnico-organizzative in grado di attuare al massimo grado possibile i principi del Regolamento, tra cui quello di minimizzazione, e integrare in questo sistema le garanzie necessarie[94]. Inoltre, egli dovrà "garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento".

Per poter progettare un tale sistema di garanzia della privacy dei dipendenti, il datore di lavoro deve innanzi tutto procedere alla valutazione del rischio, che può essere svolta secondo due diversi modelli: o un'analisi generica "della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche", prescritta agli artt. 24 e 25 del GDPR, o una vera e propria

---

88 In verità, l'approccio del GDPR non rivoluziona ma rafforza una posizione già adottata dalla precedente Direttiva 95/46: "The so-called 'risk-based approach' is not a new concept, since it is already well known under the current Directive 95/46/EC especially in the security and the DPA prior check obligations" – Article 29 Data Protection Working Party, "Statement on the role of a risk-based approach in data protection legal frameworks", 30/5/2014, p. 2.

89 G. FINOCCHIARO (2017 b), "Introduzione al Regolamento europeo sulla protezione dei dati", *Nuove leggi civili commentate*, vol. 1 pp. 1 e sgg.

90 GDPR, art. 33.

91 GDPR, art. 34.

92 La scelta del modello "aperto" pare in realtà vincente: v. A. MANTELERO (2017), *Il nuovo approccio alla valutazione del rischio nella sicurezza dei dati*, in G. FINOCCHIARO (2017 a), cit., p. 307.

93 Sull'argomento, v. lo studio capofila di S. RUBINSTEIN (2011), "Regulating Privacy by Design", *Berkeley Technology Law Journal*, vol. 26 n. 3, pp. 1409 e sgg.; per l'impatto di tale modello sul GDPR v. invece R. D'ORAZIO (2016), *Protezione dei dati* by default *e* by desgin, in S. SICA, V. D'ANTONIO, G. RICCIO (2016), *La nuova disciplina europea della* privacy, ed. Wolters Kluwer, pp. 79 e sgg.

94 GDPR, art. 25, par. 1.

"valutazione d'impatto sulla protezione dei dati", prevista invece dall'art. 35 nei casi di "rischio elevato per i diritti e le libertà delle persone fisiche".

Il concetto di "alto rischio", in presenza del quale si attiva la più gravosa procedura dell'art. 35, non è definito dal Regolamento e il suo effettivo significato rimane piuttosto incerto. Tuttavia, è possibile ipotizzare che molti trattamenti di dati personali dei lavoratori per finalità di management attraverso algoritmi ricadrebbero nel campo di applicazione dell'art. 35: tali applicazioni rientrano indubbiamente nell'ambito dell'"uso di nuove tecnologie"[95] e possono consistere in "una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato", sulla base della quale sono assunte "decisioni che hanno effetti giuridici o incidono" sui lavoratori[96].

La valutazione dell'impatto, alla quale può partecipare anche il DPO se è stato nominato[97], consiste in realtà di un processo continuo di analisi del rischio e si compone nella pratica di una "valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità"[98] e di una "valutazione dei rischi per i diritti e le libertà degli interessati"[99].

Va sottolineato che è previsto uno spazio per la partecipazione degli interessati stessi o dei loro rappresentanti alla valutazione d'impatto sulla protezione dei dati[100]: nel rapporto di lavoro, quindi, esiste la possibilità per singoli lavoratori e organizzazioni sindacali di esprimere i propri rilievi riguardo al trattamento dei dati da parte dell'imprenditore in una fase preventiva. Se sfruttata adeguatamente, questa opportunità potrebbe garantire una qualche forma di voce in capitolo ai dipendenti per quanto riguarda il disegno del sistema di garanzie di cui si è detto poc'anzi[101]. È importante evidenziare che il datore non ha nessun obbligo in questo senso e potrebbe legittimamente escludere i lavoratori dalla valutazione d'impatto; tuttavia, anche in questo caso, residuerebbe loro la possibilità di avvalersi del Data Protection Officer come anello di collegamento e come mediatore tra le esigenze dell'azienda e quelle dei suoi dipendenti.

---

95 GDPR, art. 35, par. 1.
96 GDPR, art. 35, par. 2 lett. a).
97 V. *supra*, par. 3.
98 GDPR, art. 35, par. 7 lett. b).
99 GDPR, art. 35, par. 7 lett. c).
100 GDPR, art. 35, par. 9.
101 V. più approfonditamente *infra*, par. 7.

Infine, dal confronto tra l'impianto generale del GDPR e la normativa italiana è possibile ricavare alcune osservazioni utili.

Se si guarda al trattamento dei dati personali sul posto di lavoro nella prospettiva dei controlli a distanza sui lavoratori, la disciplina degli artt. 4 e 8 Statuto dei Lavoratori[102], basata su un sistema di divieti e di rimedi giudiziali successivi costituisce probabilmente una risposta valida alle esigenze dei dipendenti: i dispositivi per il controllo possono essere installati solamente a determinate condizioni, che precludono situazioni considerate dal legislatore troppo squilibrate, e quindi lesive della riservatezza dei lavoratori.

Se però si allarga la prospettiva all'intera gamma di utilizzi dei dati dei lavoratori che possono essere fatti in un contesto di impiego sistematico del management attraverso algoritmi, appare evidente che un tale approccio rischia di non tutelare adeguatamente la posizione degli interessati. L'impianto serio e rigoroso di prevenzione del rischio messo a punto dal GDPR, infatti, consente di superare le rigidità dello Statuto dei Lavoratori e, poiché si tratta di un modello aperto di tutela, si adatta alle caratteristiche specifiche dei trattamenti dei dati di volta in volta effettuati.

Inoltre, come visto, il datore non è messo davanti a un'alternativa binaria tra impieghi leciti e impieghi illeciti della tecnologia, ma, anche quando il trattamento dei dati debba considerarsi legittimo ai sensi dell'art. 6 del Regolamento, sarà necessario che il titolare si adoperi attivamente per contenere al minimo i rischi per i diritti dei lavoratori interessati[103].

Partendo proprio da questa considerazione ci si può forse spingere oltre, paragonando la disciplina di prevenzione del GDPR con l'obbligo del datore di tutelare l'integrità fisica e la personalità morale dei lavoratori previsto all'art. 2087 del Codice civile. Entrambe le disposizioni, infatti, si muovono secondo una logica prevenzionistica e impongono all'imprenditore degli obblighi di garanzia della sicurezza dei dipendenti: la prima nell'ambito della protezione dei dati personali, e quindi a tutela del bene della riservatezza e della libertà di autodeterminazione; la seconda nell'ambito della salute fisica e psicologica sul posto di lavoro[104]. Se si accetta questa ricostruzione, i lavoratori sono titolari nei

---

[102] V. *supra*, cap. 2.

[103] E in effetti il titolare, insieme con il responsabile del trattamento, è tenuto in base all'art. 32 GDPR a mettere in atto "misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio", che possono per esempio garantire la pseudonimizzazione dei dati, la riservatezza e l'integrità dei sistemi informatici, nonché la capacità di ripristinarli prontamente.

[104] L. D'ARCANGELO (2020), cit., p. 80

confronti dell'imprenditore di corrispettivi diritti alla sicurezza dell'ambiente di lavoro, nelle due accezioni appena esaminate.

6. I diritti individuali del lavoratore

In verità, il GDPR attribuisce esplicitamente un ampio novero di diritti al lavoratore-interessato che, nelle intenzioni del Regolamento, gli dovrebbero garantire di mantenere il controllo sui dati raccolti che lo riguardano.

Innanzitutto, il lavoratore gode di diritti informativi, strumentali all'attivazione degli altri diritti. In virtù del principio di trasparenza, infatti, l'art. 13 del Regolamento prevede che il titolare del trattamento fornisca all'interessato, nel momento in cui ottiene i dati personali, un'informativa contenente una lunga lista di informazioni. Si tratta, nel dettaglio dell'identità e dei dati di contatto di titolare e responsabile, delle finalità (principio di limitazione) e della base giuridica (principio di liceità) del trattamento; se quest'ultima consiste in un interesse legittimo, tale interesse deve essere esplicitato. Se i dati sono raccolti per essere ceduti a un soggetto terzo, devono essere individuati i destinatari e il paese in cui i dati vengono trasferiti, se diverso da quello in cui sono raccolti.

Il titolare, poi, deve informare l'interessato del periodo per cui i dati saranno conservati e dei diritti che egli può esercitare, per esempio in materia di accesso o di revoca del consenso: è quindi evidente che l'informativa richiesta dall'art. 13 ha la funzione di garantire la trasparenza sui dati raccolti affinché gli interessati possano attivare gli strumenti di autotutela a loro disposizione[105].

Affinché il principio di trasparenza sia pienamente realizzato, poi, è necessario che la forma delle informative sia "concisa, trasparente, intelligibile e facilmente accessibile" e che venga impiegato un "linguaggio semplice e chiaro"[106].

All'interessato è attribuito un diritto di accesso ai dati personali[107], che consiste innanzitutto nel diritto di ottenere dal titolare la conferma che sia in corso un trattamento dei suoi dati. Se un trattamento è effettivamente in corso, il titolare dovrà fornire all'interessato anche informazioni riguardo alla finalità del trattamento, alle categorie di dati in questione, agli eventuali destinatari, al

[105] A. INGRAO (2018), cit., p. 118.
[106] GDPR, art. 12 par. 1.
[107] GDPR, art. 15 par. 1.

periodo di conservazione, al diritto di chiedere una rettifica o di ricorrere presso l'autorità nazionale e all'esistenza di un processo decisionale automatizzato[108].

Anche il diritto d'accesso è visto come prodromico rispetto all'esercizio di diritti ulteriori, come quello di correzione o di opposizione: è anche per questa ragione che non è necessario nemmeno il *fumus* di una lesione della protezione dei dati dell'interessato[109].

All'interessato che eserciti il diritto di accesso devono inoltre essere fornite copie dei dati personali oggetto di trattamento[110]: nel contesto lavorativo, questo dato risulta particolarmente interessante per due differenti ragioni. In primis, se i dati sono il risultato di un'attività di controllo e in seguito a tale attività il lavoratore viene sottoposto al potere disciplinare, gli sarà sempre possibile ottenere il materiale probatorio sulla base del quale gli viene contestato un illecito e ogni altro dato che possa risultare utile ai fini dell'elaborazione di una difesa[111], con il solo limite di non ledere "i diritti e le libertà altrui"[112].

In secondo luogo, nei contesti in cui vengono impiegate tecniche di *rating* – ad oggi, i casi più frequenti sono nella *gig economy* – è possibile che il lavoratore tragga un grave danno se, passando da una piattaforma all'altra, perde il punteggio guadagnato con il tempo, un vero e proprio patrimonio in termini di *reputazione*. Per far fronte a questo problema, è stato proposto in alcuni casi un approccio basato sulla portabilità dei dati del lavoratore: presupposto necessario è che sia possibile ottenere questi dati in un formato intellegibile e compatibile con il nuovo sistema in cui verranno immessi[113].

L'art. 20 del GDPR, infatti, stabilisce un "diritto alla portabilità" in capo all'interessato, per cui egli può ricevere i dati che lo riguardano in un formato "strutturato, di uso comune e leggibile da dispositivo automatico" e poi trasmetterli a un nuovo titolare[114]. Affinché sia possibile attivare il diritto alla portabilità dei dati personali, tuttavia, è necessario che si verifichino

---

[108] GDPR, art. 15 par. 1.
[109] A. RICCI (2017), *I diritti dell'interessato*, in G. FINOCCHIARO (2017 a), cit., p. 184.
[110] GDPR, art. 15 par. 3.
[111] Sul tema v. A. SITZIA (2009), *Potere disciplinare e diritti dei lavoratori*, in P. CENDON (2009), *Il risarcimento del danno non patrimoniale. Parte speciale*, ed. UTET, pp. 2329 e sgg., nonché S. P. EMILIANI (2007), "Potere disciplinare e protezione dei dati personali", *Argomenti di diritto del lavoro*, n. 3 pp. 630 e sgg.
[112] GDPR, art. 15 par. 4.
[113] C. Robinson, "Exploring portable ratings for gig workers", 2/2/2018, consultato online il 10/9/2021 all'indirizzo https://medium.com/doteveryone/exploring-portable-ratings-for-gig-workers-5632fd9b262e.
[114] GDPR, art. 20 par. 1.

contemporaneamente due condizioni[115]: il trattamento deve fondarsi sulla base legale del consenso o dell'esecuzione di un contratto e deve essere effettuato tramite mezzi automatizzati[116].

Nella ricostruzione qui proposta, solo in rari casi è possibile configurare il consenso del lavoratore come effettivamente libero, e quindi valido ai fini di realizzare la condizione di liceità prevista dall'art. 6. Nel contesto della *gig economy*, però, il lavoratore è qualificato come autonomo: in assenza di un formale rapporto di subordinazione, in certi casi l'interprete potrebbe ritenere valido il suo consenso e, poiché il trattamento dei dati è quasi necessariamente autorizzato, attribuirgli il diritto alla portabilità dei dati raccolti dalla piattaforma.

Va comunque sottolineato che i dati portabili sono solo quelli che "riguardano" l'interessato: dunque, secondo l'interpretazione prevalente, le informazioni prodotte direttamente da questi o dalla sua attività e le informazioni generate dall'uso di dispositivi, ma non le informazioni generate dal titolare attraverso l'analisi dei dati, come per esempio i profili[117]. In altri termini, il diritto alla portabilità riguarda i dati grezzi raccolti a partire dall'attività o dal comportamento dell'interessato, ma non anche la loro elaborazione e analisi. Nell'ambito del *rating*, i dati portabili dovrebbero includere le statistiche alla base dei punteggi e le eventuali recensioni da parte dei clienti, ma non il calcolo dei punteggi e la classificazione delle performance.

L'art. 16 del Regolamento stabilisce poi un "diritto di rettifica" dei dati inesatti, cui si accompagna un diritto di integrazione dei dati incompleti. Si tratta di uno degli strumenti attraverso i quali l'interessato può esercitare il controllo sui dati che lo riguardano, tutelando pienamente la propria identità personale da rappresentazioni inesatte nella sfera *sociale*[118]: ne consegue che possono essere oggetto di rettifica solamente i dati oggettivi, sui quali si fondano la valutazione e il giudizio altrui, ma non la valutazione e il giudizio medesimi[119]. Nel contesto del rapporto di lavoro, la distinzione è particolarmente rilevante poiché deve

---

115 Article 29 Data Protection Working Party, WP 242 rev.01, "Guidelines on the right to data portability", 5/4/2017, p. 9.
116 GDPR, art. 20 par. 1 lett. a) e b).
117 Article 29 Data Protection Working Party, WP 242 rev.01, "Guidelines on the right to data portability", 5/4/2017, p. 9.

118 P. ZATTI (2009), *Maschere del diritto. Volti della vita*, ed. Giuffré, p. 79.
119 G. FINOCCHIARO (2012), cit., p. 119.

essere garantito al datore di lavoro un margine di discrezionalità e di libero apprezzamento riguardo alle valutazioni soggettive sui suoi dipendenti[120].

In particolare, nei processi di selezione del personale tramite candidatura – specialmente per quanto riguarda le istituzioni pubbliche – si ritiene che sia possibile, dopo la scadenza del termine per presentare le domande, rettificare solamente le informazioni relative ai criteri di ammissibilità, poiché in caso contrario non sarebbe garantita la correttezza e la trasparenza della selezione; è comunque importante che i partecipanti alla selezione vengano informati preventivamente di questa possibilità[121].

Allo stesso tempo, all'interno delle procedure di valutazione della prestazione del dipendente possono essere rettificate "laddove il nome, la qualifica o ogni altro dato oggettivo possono esserlo"[122]. Al contrario, una valutazione del superiore riguardo alla prestazione del lavoratore non può essere rettificata, nemmeno se si basa su dati oggettivi falsi: anche in questo caso, l'oggetto della rettifica dovranno essere i dati alla base della valutazione, non rientrando in alcun modo nell'oggetto dell'art. 16 i giudizi soggettivi[123], i quali non possono per definizione essere errati ma solamente inaccurati, poiché fondati su informazioni incomplete[124].

Per quanto riguarda il caso del management attraverso algoritmi, è possibile che in certi casi la distinzione tra dati oggettivi e valutazioni soggettive sia piuttosto sfumata: sono sicuramente passibili di rettifica quelle statistiche basate sull'osservazione diretta di elementi oggettivi, come il numero di pratiche evase da un certo lavoratore, i giorni di assenza, le ore di straordinario registrate, etc. Allo stesso modo, ogni volta che un superiore esprime un giudizio personale sulle qualità o le attitudini di un lavoratore non si potrà negare la natura soggettiva di tale informazione, pure espressa in un rapporto[125]. Più sfumata potrebbe essere la qualificazione di situazioni in cui, a partire da metriche di

---

120 A. BELLAVISTA (2007), *La disciplina della protezione dei dati personali e i rapporti di lavoro*, in C. CESTER (2007), *Il rapporto di lavoro subordinato: costituzione e svolgimento*, ed. UTET, p. 479.

121 European Data Protection Supervisor, "Guidelines on the Rights of Individuals with regard to the Processing of Personal Data", 25/2/2014, p. 19, consultato online il 10/9/2021 all'indirizzo https://edps.europa.eu/sites/default/files/publication/14-02-25_gl_ds_rights_en.pdf. Va notato che tali linee guida si applicano ai trattamenti effettuati dalle istituzioni dell'Unione europea; ciononostante, essendo elaborate dall'autorità garante europea, esse vengono considerate un valido strumento di soft law.

122 *Ibid.*, p. 30, traduzione dall'inglese mia.

123 *Ivi*, in particolare nota 45.

124 A. RICCI (2017), cit., p. 191.

125 Garante della privacy, provv. 17 giugno 1999.

base, un algoritmo elabori dei giudizi (per esempio, una graduatoria) basati su parametri che, in ultima analisi, esprimono assunzioni di valore espresse a monte nel momento in cui l'algoritmo è stato programmato. In questo caso, cioè, siamo sì in presenza di un processo automatizzato che non incorpora valutazioni soggettive sul singolo dipendente, ma in questo processo rientrano valutazioni soggettive che orientano i criteri con cui opera l'algoritmo stesso: è allora convincente l'opinione per cui anche in questo contesto sia possibile richiedere solamente la rettifica dei dati oggettivi alla base della valutazione di produttività, mentre non possano essere messi in discussione valutazioni valoriali attinenti, in ultima analisi, alla libertà d'impresa del datore di lavoro.

Assieme al diritto di rettifica, il GDPR rende disponibile al lavoratore un altro importante strumento per contrastare l'esercizio scorretto, poiché basato su assunzioni errate sulla sua persona, dei poteri datoriali: l'art. 17, infatti, stabilisce un "diritto alla cancellazione" in qualche modo complementare alla rettifica[126].

A differenza del diritto di rettifica, tuttavia, il diritto di cancellazione non è attivabile *ad nutum*, ma è necessario che ricorra uno dei presupposti previsti dall'art. 17 del Regolamento: i dati non sono più necessari rispetto alle finalità del trattamento; il trattamento era basato sul consenso e questo viene revocato dall'interessato; l'interessato si oppone al trattamento ex art. 21; il trattamento era illegittimo; la cancellazione serve ad adempiere ad un obbligo di legge[127].

Esercitando tale diritto, i lavoratori fatti oggetto di trattamenti illeciti o sproporzionati potrebbero ottenere la distruzione o l'anonimizzazione irreversibile dei dati raccolti: tale previsione, quindi, non sarebbe in grado di contrastare le conseguenze immediate di usi scorretti del management attraverso algoritmi, ma potrebbe almeno rimuovere la traccia di tali usi e impedire che si verifichi un danno permanente alla sfera personale del dipendente[128].

L'art. 18 del GDPR prevede un "diritto di limitazione del trattamento". La limitazione consiste nel "contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro"[129] e costituisce, nella sostanza,

[126] European Data Protection Supervisor, "Guidelines on the Rights of Individuals with regard to the Processing of Personal Data", 25/2/2014, par. 4.
[127] GDPR, art. 21 par. 1 lett. da a) a e).
[128] A. INGRAO (2018), cit., pp. 143-144.
[129] GDPR, art. 4 par. 1 n. 3.

un'alternativa alla cancellazione: i dati continuano ad essere conservati, ma divengono indisponibili per il titolare del trattamento.

I casi in cui la limitazione può essere richiesta sono tassativamente indicati dalla legge, e sono le ipotesi in cui l'interessato contesta l'esattezza dei dati personali, finché tale contestazione non è verificata; il trattamento è illecito ma l'interessato preferisce conservare i dati e non cancellarli; i dati non sono più necessari ai fini del trattamento, ma l'interessato desidera conservarli per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; l'interessato si è opposto al trattamento, in attesa della verifica in merito all'eventuale esistenza di un motivo legittimo del titolare[130].

La rilevanza che il diritto di limitazione riveste per il rapporto di lavoro in generale e per i casi di management attraverso algoritmi in particolare è ancora una volta legata alla fase successiva, in cui il lavoratore ha subito conseguenze ingiuste dal trattamento dei suoi dati e intende far valere in sede giudiziale i propri diritti. In questo senso, quindi, la funzione della limitazione è essenzialmente cautelare, in quanto "congela" la situazione in vista dell'utilizzo in processo dei dati come prova e al contempo non consente né la loro cancellazione, né il loro utilizzo da parte del titolare[131].

L'interessato, infine, ha diritto di opporsi al trattamento qualora questo si fondi sulle condizioni di liceità dell'interesse pubblico o, per quello che più interessa ai fini di questa trattazione, dell'interesse legittimo[132].

L'opposizione consiste in una dichiarazione di volontà contraria al trattamento, che ha l'effetto di interromperlo definitivamente, salvo che il titolare dimostri che esistono "motivi legittimi cogenti" che giustificano la prosecuzione e che sono prevalenti sugli interessi dell'interessato. È importante notare che, in correlazione con la natura delle basi legali sulle quali può essere esercitato, il diritto di opposizione non necessita che il trattamento opposto sia illegittimo: è quindi un diritto legato all'autodeterminazione della persona, che esercitandolo sceglie a quali trattamenti vuole essere sottoposta e a quali invece no[133].

Nel modello del GDPR, insomma, l'interessato può opporsi per motivi anche meramente personali, purché esplicitate chiaramente[134], e il titolare deve

130 GDPR, art. 18, par. 1 lett. da a) a d).
131 A. RICCI (2017), cit., p. 217.
132 GDPR, art. 21, par. 1.
133 Article 29 Data Protection Working Party, Opinion 15/2011 del 13/6/2011.
134 Garante della privacy, provv. 30 aprile 2003.

astenersi dal trattamento. Il trattamento può continuare solo se il titolare prova che le finalità del trattamento prevalgono sulle esigenze dell'interessato.

Nel rapporto di lavoro, se il trattamento dei dati dei dipendenti avviene sulla base dell'interesse legittimo del datore, l'opposizione è un importante strumento che potrebbe essere esercitato dal lavoratore per impedire indebite intrusioni nella sua sfera personale.

Un ultimo diritto del lavoratore, previsto dall'art. 22 del Regolamento, è di fondamentale importanza per quanto riguarda il management attraverso algoritmi. Tale disposizione prevede infatti al primo paragrafo che:

> *L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.*

L'articolo fa perno su due elementi: il primo è il "trattamento automatizzato", che comprende la "profilazione", definita come "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 […]"[135]: moltissime tecniche di MAA, in particolare quelle di esercizio del potere di controllo[136] rientrano nell'ambito della profilazione, ma in generale è caratteristica intrinseca del management attraverso algoritmi l'automazione dell'esercizio dei poteri datoriali.

Il secondo elemento necessario è che la decisione, la quale incide significativamente sulla persona dell'interessato, sia basata *esclusivamente* sul trattamento automatizzato. Tra le decisioni che sicuramente rientrano nella formulazione del par. 1 si possono individuare i momenti fondamentali del rapporto di lavoro: il licenziamento, quindi, ma probabilmente anche trasferimenti sfavorevoli al lavoratore o la comminazione di sanzioni disciplinari[137].

L'art. 22 costituisce probabilmente lo strumento più promettente con cui il lavoratore può prevenire gli effetti più sfavorevoli del management attraverso algoritmi, ovvero per evitare che i profili automatizzati "esauriscano la base

[135] GDPR, art. 4 par. 1 n. 4.
[136] V. *supra*, cap. 1, par. 2.
[137] J. ADAMS-PRASSL (2019), cit., p. 142.

conoscitiva degli atti che presuppongono una valutazione dell'interessato"[138], quali sono gli atti del datore.

Allo stesso tempo, tuttavia, la formulazione della disposizione presenta alcuni problemi interpretativi che vanno attentamente analizzati.

In primo luogo, non è chiaro quali siano le conseguenze di una eventuale decisione che violi l'indicazione dell'art. 22. Nei fatti, la dottrina prevalente ritiene che il GDPR attribuisca all'interessato un diritto di opposizione al trattamento, che quindi seguirebbe la regola dell'art. 12 par. 3 del Regolamento riguardo alle conseguenze dell'inadempimento del titolare[139]: quest'ultimo, cioè, deve adempiere alla richiesta di opposizione entro un mese dal suo ricevimento e, in caso contrario, è possibile presentare un ricorso presso l'autorità giudiziaria o presso il Garante nazionale.

In secondo luogo, è previsto che il consenso dell'interessato possa far venir meno il diritto di cui all'art. 22[140]. A proposito della validità del consenso nel rapporto di lavoro, tuttavia, si è già detto che essa deve essere limitata a casi eccezionali, tra i quali non sembra proprio poter rientrare quello del trattamento automatizzato: di conseguenza, si deve ritenere che il lavoratore goda sempre e comunque di un diritto di opporsi al trattamento di cui all'art. 22.

Infine, nel momento in cui la disposizione prevede che la decisione debba essere basata "unicamente" sul trattamento automatizzato si potrebbe facilmente aggirare il divieto dell'art. 22 attraverso un banale intervento di conferma da parte di un manager in carne ed ossa, che tuttavia fondi il proprio giudizio unicamente sulle risultanze del processo algoritmico. In questo caso, l'intervento umano non può essere ritenuto sufficiente[141] e il datore di lavoro dovrà provare di aver effettuato quantomeno una reale revisione della decisione suggerita come migliore dall'algoritmo.

7. La dimensione collettiva

Poiché, come si è già detto[142], il GDPR adotta un approccio trasversale e si riferisce al trattamento di dati personali in ogni contesto, i diritti stabiliti dagli

---

138 G. BUTTARELLI (1997), *Banche dati e tutela della riservatezza*, ed. Giuffré, pp. 342-343.
139 A. RICCI (2017), cit., p. 243.
140 GDPR, art. 22 par. 2 lett. c).
141 G. MALGIERI, G. COMANDÉ (2017), cit.
142 V. *supra*, par. 2.

artt. 15-22 del Regolamento spettano al singolo interessato. Nel contesto del lavoro in particolare, tuttavia, non sempre è agevole per il lavoratore attivare questi strumenti: molteplici fattori, come lo squilibrio dei poteri che caratterizza ogni rapporto di lavoro e l'asimmetria informativa, per cui il lavoratore potrebbe essere inconsapevole delle caratteristiche del trattamento a cui è soggetto, potrebbero rendere di fatto rara l'attivazione di diritti come la rettifica o l'opposizione al trattamento[143].

Inoltre, si può affermare che i trattamenti di dati che riguardano un gruppo di persone relativamente omogeneo e che producono conseguenze sul gruppo medesimo hanno una dimensione che trascende la somma dei problemi di privacy individuali: è possibile individuare un concetto di "privacy di gruppo"[144], che senza molte difficoltà si applica ai gruppi di lavoratori all'interno di un'azienda e alle loro rappresentanze sindacali[145].

È per questa ragione che la dimensione collettiva dei diritti alla protezione dei dati personali sul luogo di lavoro deve essere attentamente studiata e, eventualmente, valorizzata: la partecipazione dei rappresentanti dei lavoratori alle decisioni aziendali in materia di privacy è in grado di aumentarne l'efficacia e la condivisione da parte dei lavoratori stessi[146].

Questo già accade nel diritto nazionale: lo Statuto dei Lavoratori, in particolare, coinvolge i sindacati all'art. 4, quando richiede un accordo collettivo per procedere all'installazione di dispositivi di sorveglianza: in tal modo l'assetto di potere può essere riequilibrato e i due soggetti possono pervenire a un accordo anche sulle modalità di esercizio del controllo a distanza che offra una ragionevole tutela ai lavoratori.

Il GDPR non assegna ai sindacati un ruolo altrettanto preminente; tuttavia, vanno evidenziate alcune occasioni per i soggetti collettivi di prendere parte al disegno dei sistemi di trattamento dei dati personali. In particolare, i rappresentanti degli interessati (in questo caso, dei lavoratori) sono esplicitamente contemplati dall'art. 35, in merito alla valutazione d'impatto sulla

---

143 A. MANTELERO (2016), "Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection", *Computer Law and Security Review*, vol. 32 p. 245.

144 L. BYGRAVE (2002), *Data Protection Law. Approaching Its Rationale, Logic and Limits*, ed. Kluwer Law International, parte III.

145 M. FREEDLAND (1999), *Data Protection and Employment in the European Union. An Analytical Study of the Law and Practice of Data Protection and the Employment Relationship in the EU and Its Members*, ed. EC.

146 C. FRITSCH (2015), cit., p. 161.

protezione dei dati personali[147]: se il titolare lo ritiene necessario, essi sono consultati preventivamente sul trattamento e hanno così l'occasione di promuovere le proprie istanze e di partecipare al disegno dell'apparato di protezione dei dati.

Una seconda opportunità potrebbe essere rappresentata dalla nomina del Data Protection Officer che, pur trattandosi di una figura di garanzia per i lavoratori in materia di privacy, è rimessa all'imprenditore[148]. La contrattazione collettiva potrebbe muoversi per chiedere una maggiore voce in capitolo a questo proposito e, di riflesso, poter incidere maggiormente nella valutazione del rischio e nella scelta degli strumenti di *privacy by design* e *privacy by default*.

8. L'apparato sanzionatorio

Un ultimo motivo di interesse della disciplina del GDPR riguarda il suo apparato sanzionatorio. Si è già detto delle disposizioni penali legate allo Statuto dei Lavoratori, che puniscono il datore che trasgredisca, tra gli altri, agli artt. 4 e 8[149].

L'apparato sanzionatorio previsto dal GDPR risulta estremamente più efficace[150]: nel caso in cui il titolare del trattamento trasgredisca alle disposizioni in merito alla prevenzione del rischio, egli è soggetto a una sanzione amministrativa pecuniaria fino a 10.000.000 di Euro o fino al 2% del fatturato dell'anno precedente, se superiore[151]; se invece sono violate le disposizioni riguardanti i principi fondamentali del trattamento, le condizioni di liceità o i diritti degli interessati, le sanzioni possono arrivare fino a 20.000.000 di Euro e fino al 4% del fatturato[152].

Tali sanzioni sono comminate dalle autorità garanti di ogni Stato membro, le quali si devono adoperare affinché le sanzioni siano "effettive, proporzionate e dissuasive"[153]. Nel predisporre le sanzioni, le autorità di controllo devono stabilire l'entità sulla base dei criteri individuati dal GDPR, tra cui rientrano la

147 V. *supra*, par. 5.
148 V. *supra*, par. 4.
149 V. *supra*, par. 5.
150 V. M. RATTI (2017), *Il regime sanzionatorio previsto dal Regolamento*, in G. FINOCCHIARO (2017), cit., pp. 595 e sgg.
151 GDPR, art. 83 par. 4.
152 GDPR, art. 83 par. 5, lett. a) e b).
153 GDPR, art. 83 par. 1.

natura, la gravità e la durata della violazione, il dolo del titolare del trattamento, le misure eventualmente adottate per attenuare il danno provocato, l'adeguatezza delle misure di prevenzione del rischio predisposte, eventuali precedenti, etc.[154] Il procedimento paragiurisdizionale davanti all'autorità è assistito da garanzie di tipo procedurale[155] e la sanzione comminata deve sempre rispondere a un criterio di proporzionalità.

La speditezza del procedimento davanti al Garante e la maggiore adattabilità della sanzione al caso concreto, unitamente all'ampia copertura offerta e agli importi particolarmente elevati che costituiscono un serio deterrente anche per le azienda più grandi rendono il regime sanzionatorio del GDPR particolarmente efficace e garantiscono l'effettività della tutela dei diritti posti in capo al lavoratore.

[154] GDPR, art. 83 par. 2.
[155] GDPR, considerando n. 143.

Capitolo 4. Le prospettive applicative: spunti dalla giurisprudenza e dai provvedimenti del Garante

1. GDPR e lavoro: l'art. 88

Si è già detto in più punti che il GDPR adotta un'impostazione trasversale, e cioè non circoscrive il proprio ambito di applicazione a uno specifico settore, ma si applica a tutti i casi in cui vi è trattamento di dati riferiti a una persona fisica[1]. Questa osservazione, tuttavia, non comporta che il Regolamento o il diritto della privacy europeo si disinteressino delle specificità del rapporto di lavoro: in più occasioni, infatti, il legislatore comunitario ha dimostrato una particolare attenzione per il contesto lavorativo e ha dettato alcune norme rilevanti per gli scopi di questa trattazione, che vanno analizzate nel dettaglio.

Per prima cosa, è necessario sottolineare che non esiste allo stato attuale e non è mai esistita in passato una vera e propria disciplina speciale della privacy sul posto di lavoro[2]. Al contrario, l'origine del rapporto tra diritto della privacy europeo e dimensione sociale viene fatta risalire a una comunicazione con cui la Commissione, già nel 1997, ha riconosciuto che la Direttiva 95/46 era applicabile al rapporto di lavoro[3].

Negli anni successivi, precisamente nel 2001[4] e nel 2004[5], la Commissione procedette a due importanti consultazioni con le parti sociali, volte ad elaborare una direttiva per la protezione dei dati personali dei lavoratori: queste iniziative, tuttavia, non portarono a risultati concreti[6]. Al 2015 risale infine l'importante Raccomandazione del Consiglio d'Europa, già richiamata in precedenza[7], sul

---

[1] V. *supra*, cap. 3, par. 3.

[2] C. DEL FEDERICO (2017), *Il trattamento dei dati personali dei lavoratori*, in P. TULLINI (2017), *Web e lavoro. Profili evolutivi e di tutela*, ed. Giappichelli, p. 63.

[3] Commissione europea, Comunicazione COM (97) 390 final, "The social and labour market Dimension of the Information Society; People First-Next Steps", pp. 8-9.

[4] Commissione europea, Comunicazione "First stage consultation of social partners on the protection of workers' personal data", 2003.

[5] Commissione europea, Comunicazione "Second stage consultation of social partners on the protection of workers' personal data", 2004.

[6] V. anche Parlamento europeo, DG for Internal Policies, studio PE 474.440, "Protection of Personal Data in Work-related Relations", p. 9.

[7] Consiglio d'Europa, Raccomandazione (2015) 5 - v. *supra*, cap. 3 par. 2.

trattamento di dati personali nel contesto occupazionale: essa ribadisce i principi generali che caratterizzano la disciplina della protezione dei dati personali in generale e, soprattutto, elabora una disciplina dedicata al contesto lavorativo.

In particolare, gli articoli dal 14 al 21 contengono una regolamentazione piuttosto dettagliata dell'uso di strumenti tecnologici di controllo, come la sorveglianza della navigazione su Internet, la videosorveglianza, la geolocalizzazione e la raccolta di dati biometrici. Tuttavia, poiché si tratta di una raccomandazione, essa non ha alcuna efficacia vincolante ma un valore di orientamento e di indirizzo: essa può essere tenuta in conto nell'interpretazione della normativa eurounitaria, ma non produce di per sé alcun effetto giuridico[8].

Il GDPR, poi, mostra alcuni importanti segni di apertura alle specificità del contesto lavorativo in due disposizioni specifiche.

In primo luogo, l'art. 9 del Regolamento vieta il trattamento di "categorie particolari di dati personali" – quelli che, nel lessico della precedente Direttiva, erano denominati "dati sensibili"[9]. Non possono, infatti, essere trattati quei dati che "rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, *o l'appartenenza sindacale*[10], […] dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona"[11]. Sono previste alcune eccezioni, assistite da appropriate garanzie, tra cui va considerato il caso in cui "il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale […]"[12]. Il considerando n. 54, comunque, prevede che se si tratta di dati relativi alla salute, questi non possono essere trattati per altre finalità da terzi, tra cui i datori di lavoro.

In secondo luogo, l'art. 88 introduce una clausola molto discussa a favore degli Stati membri esclusivamente dedicata al rapporto di lavoro. Il primo paragrafo recita:

> *Gli Stati membri possono prevedere, con legge o tramite contratti collettivi, norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al*

[8] R. ADAM, A. TIZZANO (2020), cit., p. 160.
[9] G. FINOCCHIARO (2012), cit., pp. 57 e sgg.
[10] Corsivo mio.
[11] GDPR, art. 9 par. 1.
[12] GDPR, art. 9 par. 2 lett. b).

trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro, in particolare per finalità di assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi, di gestione, pianificazione e organizzazione del lavoro, parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro, protezione della proprietà del datore di lavoro o del cliente e ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro, nonché per finalità di cessazione del rapporto di lavoro.

In sostanza, il legislatore europeo ha riconosciuto la possibilità di dettare norme speciali di diritto nazionale attraverso disposizioni di rango primario o contratti collettivi in tutti gli ambiti di incontro tra diritto alla protezione dei dati personali e diritto del lavoro.

Dall'analisi dell'art. 88 possono scaturire almeno due osservazioni. La prima riguarda l'inevitabile scontro tra l'obiettivo di uniformazione del diritto perseguito con lo strumento del regolamento[13] e la tradizionale scarsa disposizione degli Stati membri a cedere all'Unione il potere sul proprio ordinamento lavoristico[14]. Tale scontro si è risolto, in verità, con una sorta di curioso compromesso, per cui un regolamento, atto per definizione obbligatorio in tutti i suoi elementi, prevede esplicitamente che disposizioni di diritto nazionale lo possano completare[15]. Il risultato è che, per quanto riguarda l'ambito del lavoro, il diritto europeo della privacy continuerà a patire differenze di disciplina tra i vari Stati membri[16].

La seconda osservazione riguarda invece gli effetti sulla tutela dei diritti dei lavoratori: alcuni commentatori hanno espresso preoccupazioni riguardo alla flessibilità che l'art. 88 garantirebbe ai legislatori nazionali. In particolare, la formulazione del primo paragrafo non richiede, come sarebbe opportuno e com'è consueto, che le norme di diritto interno siano "più favorevoli ai lavoratori", bensì è sufficiente che esse siano "più specifiche": sarebbe dunque ammissibile una deroga *in peius* al GDPR da parte di una legge o di un accordo collettivo in un determinato Stato membro[17]?

---

13 V. *supra*, cap. 3 par. 2.

14 P.L. DAVIES (1992), *The Emergence of European Labour Law*, in W. MCCARTHY (1992), *Legal Intervention in Industrial Relations: Gains and Losses*, ed. Blackwell, p. 313.

15 A ben vedere, l'obbligatorietà di un regolamento non implica che il suo contenuto sia completo: v. R. ADAM, A. TIZZANO (2020), cit., p. 181.

16 A. BEVITT, C. STACK (2016), "Preparing for the GDPR-advice for employers", *PDP*, vol. 16 n. 6, p. 11.

17 J. ADAMS-PRASSL (2019), cit., p. 150.

In verità, è probabilmente necessario leggere l'apertura del par. 1 alla luce di quanto sancito dal paragrafo successivo, che impone "misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati"[18]: alla luce di questa disposizione, appare improbabile che le garanzie dei lavoratori possano essere ridotte al di sotto di un livello comune di effettività[19].

Avvalora questa posizione l'esame del caso italiano. Il par. 3 dell'art. 88 richiedeva infatti agli Stati membri di inviare alla Commissione una relazione contenente tutte le disposizioni adottate sulla scorta dei paragrafi precedenti. La relazione presentata nel 2019 dal nostro Paese[20] indica solamente poche disposizioni del novellato Codice della privacy, che prevedono che il Garante promuova l'adozione di "regole deontologiche" da parte degli imprenditori[21], che introducono disposizioni di dettaglio per quanto riguarda la ricezione di *curriculum* e il telelavoro[22] e che fanno salvi gli artt. 4 e 8 dello Statuto dei Lavoratori[23].

Tuttavia, non è detto che la risposta sia univoca in tutti gli Stati membri. In attesa che la Corte di Giustizia dell'Unione europea si pronunci sul tema[24], è solamente possibile identificare la soluzione qui proposta come la più ragionevole.

Il quadro normativo applicabile in Italia al trattamento dei dati dei lavoratori è quindi in buona parte quello descritto nei capitoli precedenti: certe forme di controllo dei dipendenti di aziende sono vietate dallo Statuto dei Lavoratori[25]; quando invece i dati possono essere raccolti, al loro trattamento si applica la disciplina generale del GDPR[26] senza rilevanti eccezioni.

Occorre ora verificare in concreto l'utilizzabilità di queste norme per prevenire un uso scorretto delle tecnologie di management attraverso algoritmi: per

---

[18] GDPR, art. 88 par. 2.
[19] C. DEL FEDERICO (2017), cit., p. 67.
[20] Ministero della Giustizia, "Comunicazioni alla Commissione UE – Attuazione a livello nazionale del Regolamento (UE) 2016/679", pp. 14-15.
[21] Codice della privacy, art. 111
[22] Codice della privacy, rispettivamente art. 111-bis e art. 115.
[23] Codice della privacy, artt. 113 e 114.
[24] Risulta infatti pendente davanti alla CGUE un ricorso rilevante a questo proposito: v. Causa C-34/21, Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium v. Ministro della Cultura del Land dell'Assia, prima questione pregiudiziale.
[25] V. *supra*, cap. 2.
[26] Di nuovo, ha importanza fondamentale l'art. 4 comma 3 dello Statuto dei Lavoratori, che rinvia al Codice della privacy e, per suo tramite, al Regolamento 2016/679.

questo fine, sarà necessario esaminare la giurisprudenza italiana ed europea, così come i provvedimenti del Garante della privacy.

2. Le condizioni di liceità e i fini del trattamento

Poiché il GDPR ha iniziato ad applicarsi a partire dal 25 maggio 2018[27], la giurisprudenza disponibile per un'analisi dell'applicazione delle sue disposizioni più importanti è ancora molto scarna. Ciononostante, è possibile tracciare un primo bilancio su tre diversi ambiti in cui la combinazione di diritto italiano ed eurounitario appena evidenziata opera a tutela dei lavoratori interessati dall'esercizio attraverso algoritmi dei poteri datoriali: la liceità del trattamento stesso, il diritto di accesso ai dati e la tutela contro le decisioni automatizzate.

Nel caso specifico del MAA, nella grande maggioranza dei casi i dati utilizzati dagli algoritmi provengono direttamente dagli strumenti di lavoro dei dipendenti, come smartphone, computer e macchinari dotati di sensori: in questi casi non è necessario, ai sensi dell'art. 4 comma 2 dello Statuto dei Lavoratori, concludere alcun accordo con le rappresentanze sindacali o ottenere alcuna autorizzazione per garantire la legittimità della raccolta dei dati[28]. Tuttavia, questo non è sufficiente per assicurarsi che il trattamento sia lecito: ai sensi del comma 3 dello stesso articolo, infatti, i dati devono essere trattati nel rispetto del Codice della privacy e, quindi, del GDPR.

Con riguardo alla liceità del trattamento, essa si deve innanzitutto basare su una condizione prevista dall'art. 6 GDPR: nel caso del rapporto di lavoro, si è detto, l'unica base legale che appare utilizzabile è l'interesse legittimo.

Le ricadute di una tale configurazione sono notevoli: quando ci si trova in presenza degli interessi legittimi confliggenti di lavoratore e datore di lavoro, il punto di equilibrio va ricercato facendo riferimento ai principi dettati dal GDPR di limitazione delle finalità[29], minimizzazione[30] e trasparenza[31].

In primo luogo, quindi, è rilevante il fine al quale è diretto il trattamento dei dati: in virtù di un generale principio di proporzionalità, l'interesse del datore si può ritenere legittimo solo laddove lo stesso fine non poteva essere raggiunto

[27] GDPR, art. 99 par. 2.
[28] V. *supra*, cap. 2 par. 3.
[29] GDPR, art. 5 par. 1 lett. b).
[30] GDPR, art. 5 par. 1 lett. c).
[31] GDPR, art. 5 par. 1 lett. a).

con strumenti meno invasivi. In altri termini, la limitazione del diritto alla riservatezza e al controllo dei dati personali del lavoratore è giustificata solo se viene provata una relazione "ragionevole" tra le misure impiegate e l'importanza dell'obiettivo per il datore di lavoro[32].

Il principio di limitazione delle finalità, poi, prevede che i dati siano raccolti per finalità "determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità"[33]. Tali finalità vanno quindi esplicitate prima dell'inizio del trattamento, in modo tale non soltanto da renderle palesi agli interessati, ma anche da fissare gli esatti confini del trattamento legittimo: tutti i trattamenti esorbitanti rispetto alle finalità predeterminate sono infatti da considerarsi illeciti[34].

Ovviamente, non qualsiasi scopo individuato dal datore può ritenersi lecito, per il solo fatto che i lavoratori ne hanno ricevuto preventiva informazione: è così, per esempio, che dati ricavati da indagini sulle opinioni non potrebbero in ogni caso essere raccolti e utilizzati, in virtù del divieto di cui all'art. 8 dello Statuto dei Lavoratori[35]. Inoltre, è concesso un uso ulteriore dei dati raccolti anche per finalità "compatibili" con quelle comunicate[36]: nel rapporto di lavoro, in particolare, la valutazione di compatibilità deve essere particolarmente rigorosa e deve tenere conto delle aspettative di riservatezza degli interessati. Di conseguenza, strumenti installati per garantire la sicurezza aziendale non potranno essere utilizzati come prova dell'inadempimento del lavoratore, così come dati raccolti per il funzionamento di algoritmi di direzione della prestazione non potranno essere utilizzati, se non con una specifica informativa, per finalità disciplinari[37].

---

32 Corte EDU, sentenza 6 settembre 1989, ric. 12242/1986, Rommelfanger v. Repubblica Federale Tedesca.

33 GDPR, art. 5 par. 1 lett. b).

34 Article 29 Data Protection Working Party, parere 00569/13/EN "Sul principio di finalità", 2/4/2013.

35 F. IAQUINTA, A. INGRAO (2014), cit., p. 1027. È estremamente interessante, a questo proposito, la sentenza Cass. 19 settembre 2016, n. 18302, in *Rivista italiana di diritto del lavoro*, vol. 2 n. 1, con nota di A. INGRAO (2017), "Il controllo disciplinare e la privacy del datore dopo il Jobs Act", in cui la Corte ha riscontrato la violazione dell'art. 8 SL da parte di un software di rilevazione dell'attività dei computer dei lavoratori che elaborava automaticamente una sorta di "profilo" del lavoratore, tenendo conto delle pagine web visitate.

36 GDPR, art. 6 par. 4.

37 Il nuovo contesto creato dall'intersezione tra GDPR e Statuto dei Lavoratori riformato ha portato in realtà a dubitare anche della legittimità dei cd. controlli difensivi: a questo proposito, v. Trib. Roma, ordinanza 13 giugno 2018, n. 57668, con commento di C. OGRISEG (2018), "Inutilizzabilità delle informazioni raccolte tramite gestionali e posta elettronica per mancata informativa al dipendente", *GiustiziaCivile.com*.

In secondo luogo, il principio di minimizzazione impone che il sacrificio della sfera di controllo dei dati personali da parte del lavoratore sia il minimo possibile rispetto alle finalità individuate dal datore di lavoro. La minimizzazione dei dati deve essere realizzata attraverso tecniche di *privacy by design* e *privacy by default*, di cui all'art. 25 GDPR[38]: questo significa che è compito del datore predisporre un sistema di trattamento dei dati il più possibile rispettoso degli interessi dei lavoratori, per esempio anonimizzando dove possibile i dati personali[39].

Non solo gli strumenti, ma anche il tipo di dati effettivamente raccolti deve rispondere al principio di minimizzazione: per esempio, laddove sia possibile utilizzare solo dati generici a fini disciplinari, il datore di lavoro deve astenersi dal raccogliere e trattare dati più specifici che potrebbero ledere la riservatezza del lavoratore[40].

A questo proposito, un filone giurisprudenziale importante ha riguardato i sistemi di registrazione delle presenze sul posto di lavoro: solamente in casi eccezionali si considera proporzionato, e quindi rispondente al principio di minimizzazione, la rilevazione attraverso dati biometrici come, nella maggior parte dei casi portati all'attenzione del Garante, le impronte digitali. Laddove sia possibile, devono essere utilizzati altri meccanismi come badge o codici personali[41].

Infine, ricopre una fondamentale importanza l'informazione riservata ai lavoratori riguardo ai dati raccolti. In base al principio di trasparenza, infatti, il lavoratore deve essere informato con strumenti adeguati e in maniera chiara riguardo ai trattamenti che il datore vuole intraprendere. Tale informativa deve necessariamente precedere l'inizio del trattamento, e non rileva il consenso eventualmente prestato a posteriori dal lavoratore[42].

---

38 V. *supra*, cap. 3 par. 6.

39 A. INGRAO (2018), cit., p. 124.

40 È questo il caso di Garante della privacy, provv. 2 febbraio 2006, rif. [1229854], in cui un datore di lavoro che aveva vietato per politica aziendale l'accesso a internet dai propri dispositivi non si era limitato a raccogliere i dati sull'accesso di un dipendente alla rete per contestargli un'infrazione disciplinare, ma aveva anche indagato sul contenuto dei siti visitati.

41 Garante della privacy, provv. 15 ottobre 2009, rif. [166425].

42 Garante della privacy, provv. 18 maggio 2006, rif. [1299082], in cui il datore aveva svolto controlli a fini disciplinari sui messaggi di posta elettronica di un suo dipendente, alla presenza di costui e senza che questi si opponesse. Non avendo tuttavia inoltrato un'adeguata informativa che indicasse, tra le possibili finalità del trattamento dei dati, quella disciplinare, il Garante ha riconosciuto infine l'illegittimità del trattamento.

Nell'ambito delle tecnologie di management attraverso algoritmi, il rispetto dei principi del Regolamento è di vitale importanza per garantire che il controllo dell'imprenditore non sconfini in aree della vita personale del lavoratore che dovrebbero rimanergli intangibili. In particolare, l'interesse datoriale all'ottimizzazione dei processi produttivi deve essere adeguatamente bilanciato con gli interessi dei lavoratori alla riservatezza: per questa ragione deve essere privilegiato il principio di limitazione del trattamento. In particolare, è necessario che i trattamenti effettuati per migliorare la produttività siano tenuti distinti dal potere disciplinare del datore[43].

3. Il diritto di accesso

Il diritto di accesso dei lavoratori ai propri dati personali raccolti e trattati dal datore di lavoro può essere uno strumento particolarmente efficace per permettere di attivare ulteriori diritti dei dipendenti. In particolare, il lavoratore vanta un interesse ad accedere ai dati conservati nel proprio fascicolo personale, tra i quali rientrano le valutazioni sulla sua professionalità: quando i poteri datoriali sono esercitati, in tutto o in parte, attraverso algoritmi, infatti, potrebbe non essere del tutto chiaro quali parametri sono stati utilizzati per dirigere, controllare e disciplinare il lavoratore.

Il diritto del lavoratore ad accedere al proprio fascicolo, in ogni caso, nell'ordinamento italiano è tutelabile in quanto tale. Secondo la Suprema Corte di Cassazione, infatti, si tratta di un vero e proprio diritto soggettivo che sorge dal rapporto di lavoro e non dipende dallo specifico interesse vantato di volta in volta dal lavoratore rispetto alle informazioni in possesso dell'azienda[44]. Addirittura, l'obbligo del datore di fornire i dati richiesti, stabilito esplicitamente all'art. 15 del GDPR, sarebbe già rinvenibile nei principi di correttezza e buona

[43] Esemplare in questo senso è Garante della privacy, provv. 11 settembre 2014, rif. [3474069], par. 3, con riferimento a un sistema di "work force management" che utilizza i dati di geolocalizzazione dei cellulari aziendali forniti ai lavoratori per coordinare gli interventi sul campo, ma "nessun utilizzo dei dati potrà avvenire per finalità diverse da quelle dichiarate, come ad esempio per scopi disciplinari". V. anche, più di recente, Garante della privacy, provv. 15 aprile 2021, rif. [9586936], in cui, a seguito dell'installazione in un'industria di un sistema di "productivity management" per finalità di ottimizzazione dei processi produttivi, l'azienda aveva utilizzato dati sulla produttività riportabili a lavoratori specifici per scopi disciplinari.

[44] V. Cass. 4 febbraio 2004, n. 2397.

fede che, in base agli artt. 1175 e 1375 c.c., caratterizzano ogni rapporto contrattuale – e quindi, anche il rapporto di lavoro[45].

I diritti del lavoratore al trattamento dei suoi dati, a partire dal diritto di accesso, sono stati considerati dalla nostra giurisprudenza come espressione di un generale diritto all'autodeterminazione, in un'interpretazione sistematica che vede la protezione dei dati personali prima di tutto come controllo su di essi[46].

Molto rilevanti per stabilire gli esatti confini del diritto d'accesso sono anche alcuni provvedimenti del Garante della privacy: innanzitutto, oggetto dell'accesso del dipendente possono essere non solamente i dati oggettivi, ma anche le valutazioni soggettive da parte dei superiori – le cd. "note di qualifica"[47]. Il diritto di accesso non riguarda solamente il fascicolo del dipendente, ma anche tutti gli altri dati "comunque conservati in ogni altro archivio della società": questo significa anche dati estrapolati da altri documenti, posto che l'interessato non ha diritto ad accedere ai documenti nella loro interezza[48].

Il datore di lavoro, che già in precedenza era tenuto ad estrapolare i dati richiesti e fornirli al dipendente "con modalità idonee a renderli agevolmente comprensibili"[49], è ora espressamente tenuto dall'art. 15 par. 3 GDPR a fornire una copia in formato digitale. I dati possono avere qualsiasi forma e non devono necessariamente consistere in documenti scritti: si può infatti trattare di fotografie, videoregistrazioni registrazioni sonore, radiografie, etc.[50]. Possono essere ricompresi nel concetto di "dati personali" anche i messaggi di posta elettronica[51].

Il lavoratore, infine, non ha semplicemente diritto ad accedere ai dati richiesti, ma può anche chiedere che gli siano rese note le occasioni e le finalità per le quali essi sono stati trattati[52].

---

45 V. F. DI MARTINO (2016), nota a Cass. Sez. lav., 7 aprile 2016, n. 6775, *Il Lavoro nella giurisprudenza*, vol. 10, p. 902.
46 A. INGRAO (2018), cit., p. 139.
47 Questo già nel contesto della previgente Direttiva 95/46: v. Garante della privacy, comunicato 17 giugno 1999, secondo cui "può considerarsi come dato personale, dunque, ogni notizia o elemento che fornisce un contributo aggiuntivo di valutazione rispetto ad un soggetto identificato o identificabile".
48 Garante della privacy, provv. 17 gennaio 2008, rif. [1489997].
49 Garante della privacy, provv. 19 dicembre 2001, rif. [41854].
50 Garante della privacy, provv. 2 ottobre 2008, rif. [1557445].
51 Garante della privacy, provv. 23 aprile 2002, rif. [1065065].
52 Garante della privacy, provv. 19 dicembre 2001, rif. [41854].

4. Le decisioni automatizzate e l'art. 22 GDPR

Come accennato in precedenza[53], l'art. 22 del Regolamento rappresenta un'assoluta novità nel panorama del diritto alla protezione dei dati personali. L'effettiva portata applicativa di tale articolo è stata oggetto di intensi dibattiti tra i principali studiosi della materia: da un lato, una parte della dottrina[54] ha inteso valorizzare tale disposizione per fondare un diritto dell'interessato da trattamento automatizzato alla *spiegazione* del processo decisionale; dall'altro, un filone interpretativo piuttosto influente ha invece ritenuto che dall'art. 22 non si potesse ricavare un tale diritto[55] e che, in buona sostanza, questa previsione sarebbe rimasta lettera morta[56].

L'Article 29 Working Party, gruppo di lavoro istituito dalla Commissione per interpretare il Regolamento 2016/679, ha chiarito la natura dell'art. 22 con la pubblicazione delle Linee guida sulle decisioni automatizzate[57]. In base a tale documento, per prima cosa emerge che, nonostante l'espressione "diritto", il primo paragrafo stabilisce un vero e proprio divieto in capo al titolare di adottare decisioni automatizzate che producano effetti giuridici rilevanti, il quale non dipende quindi dall'attivazione del corrispettivo diritto dell'interessato a non essere soggetto a tali decisioni[58].

In secondo luogo, questo divieto generale soffre delle eccezioni indicate dal par. 2: si tratta dei casi in cui il trattamento è necessario per la conclusione o l'esecuzione di un contratto, quelli autorizzati dal diritto dei singoli Stati membri e quelli in cui è presente il consenso esplicito dell'interessato. Si deve escludere,

---

[53] V. *supra*, cap. 3 par. 6.

[54] G. MALGIERI, G. COMANDÉ (2017), cit.; G. MALGIERI (2019), "Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations", *Computer Law and Security Review*, vol. 35 pp. 2 e sgg.; B. GOODMAN, S. FLAXMAN (2016), "EU Regulations on Algorithmic Decision-Making and a "right to Explanation"", *AI Magazine*, vol. 38, n. 3; soprattutto, A. SELBST, J. POWLES (2017), "Meaningful information and the right to explanation", *International Data Privacy Law*, vol. 7 n. 4, pp. 233–242.

[55] L. EDWARDS, M. VEALE (2017), "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For", *Duke Law & Technology Review*, vol. 16, pp. 18-84.

[56] S. WACHTER, B. MITTELSTADT, L. FLORIDI (2017), "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation", *International Data Privacy Law*, vol. 7 n. 2, pp. 76–99.

[57] Article 29 Data Protection Working Party, Documento WP251rev.01, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679", 3/10/2017 rivisto il 6/2/2018.

[58] *Ibid.*, p. 19.

per le ragioni già esaminate in precedenza[59], che il consenso del lavoratore si possa configurare come libero in costanza di rapporto di lavoro.

Decisioni automatizzate potrebbero essere necessarie per concludere o dare esecuzione a un contratto di lavoro, ma le Linee guida interpretano tale eccezione nel senso che la decisione automatizzata deve essere considerata lo strumento più appropriato: se esistono altri strumenti meno invasivi e comunque efficaci, il trattamento non può essere considerato necessario e pertanto l'eccezione dell'art. 22 par. 2 lett. a) non può essere invocata[60]. Un esempio esplicitamente elaborato dalle Linee guida è quello della selezione del personale nei casi in cui pervenga un numero estremamente alto di candidature – decine di migliaia: in questa situazione, il datore potrebbe ritenere impossibile esaminare tutti i curriculum senza l'ausilio di un algoritmo, e di conseguenza il trattamento andrebbe considerato lecito[61].

Infine, è possibile che i legislatori nazionali disciplinino più nel dettaglio l'ambito di applicazione dell'art. 22, garantendo però "misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato"[62]: nella pratica, gli Stati membri adottano approcci molto diversi tra loro, e a questo proposito valgono le stesse osservazioni fatte più sopra riguardo all'art. 88 del Regolamento[63]. In particolare, la maggioranza degli Stati membri ha deciso di non adottare alcuna disposizione di dettaglio: è questo il caso, tra gli altri, dei Paesi scandinavi, della Spagna, del Portogallo e, per quello che più interessa in questa trattazione, dell'Italia[64]. Germania, Austria e Belgio hanno implementato l'art. 22 nella propria legislazione nazionale, ma non hanno previsto specifiche tutele per gli interessati; al contrario, Irlanda e Slovenia hanno introdotto misure di tipo procedurale, come un sistema di notifiche e forme di diritto alla revisione. Solamente Francia e Ungheria, infine, hanno previsto un vero e proprio diritto dell'interessato a conoscere certi parametri dell'algoritmo[65].

---

[59] V. *supra*, cap. 3 par. 4.
[60] Article 29 Data Protection Working Party, "Guidelines", cit., p. 21, con riferimento a EDPS, "Assessing the necessity of measures that limit the fundamental right to the protection of personal data. A Toolkit", 11/4/2017, consultato online il 15/9/2021 all'indirizzo https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf.
[61] *Ivi.* Le cifre qui utilizzate sono in effetti estremamente alte: si potrebbe ammettere la stessa soluzione nel caso in cui pervengano, per esempio, alcune *centinaia* di curriculum?
[62] GDPR, art. 22 par. 2 lett. b).
[63] V. *supra*, par. 1.
[64] G. MALGIERI (2019), cit., p. 6.
[65] *Ivi.*

Le Linee guida, poi, dedicano largo spazio a importanti precisazioni riguardo alle caratteristiche che le decisioni automatizzate devono possedere per rientrare nell'ambito del divieto sancito dall'art. 22.

Innanzitutto, le decisioni in questione devono essere basate "unicamente" sul trattamento automatizzato di dati: a nessuna fase del processo, cioè, deve prendere parte un essere umano. In questo senso, il titolare del trattamento non può *artefare* l'intervento umano[66]: è necessario che l'interventore umano riveda effettivamente il processo decisionale dell'algoritmo e tenga in considerazione nuovi fattori.

Infine, è necessario che la decisione produca "effetti giuridici" o che "incida […] significativamente sulla persona"[67]. Perché la decisione abbia effetti giuridici, si ritiene necessario che incida sui diritti di una persona fisica, riconosciuti dalla legge o da un contratto, oppure il suo status personale. Tra gli effetti giuridici rientra senza dubbio l'estinzione di un contratto[68].

La definizione di incidenza significativa sulla persona è più problematica. In questo caso, la decisione non deve incidere sui diritti della persona, ma deve comunque produrre effetti simili: ancora una volta, si può fare l'esempio di un algoritmo di selezione del personale per un datore di lavoro privato[69], laddove la scelta dell'algoritmo determina la possibilità di essere assunti, ma non incide su alcun diritto del candidato, il quale ancora non ha sottoscritto un contratto di lavoro.

Le precisazioni del Gruppo di lavoro sono di grande rilevanza e consentono di comprendere meglio i margini di applicazione nella pratica dell'art. 22. Ciononostante, in dottrina ancora fino a pochi mesi fa si dubitava della concreta utilizzabilità nelle controversie di lavoro di tale strumento normativo e, in effetti, ad oggi non risultano sentenze né italiane né europee che facciano perno sul divieto di decisioni automatizzate[70].

---

66 "The controller cannot avoid the Article 22 provisions by fabricating human involvement" – Article 29 Data Protection Working Party, "Guidelines", cit., p. 21.
67 GDPR, art. 22, par. 1.
68 Article 29 Data Protection Working Party, "Guidelines", cit., p. 21.
69 GDPR, considerando n. 71.
70 V. R. GELLERT, M. VAN BEKKUM, F. ZUIDERVEEN BORGESIUS (2021), "The Ola & Uber judgments: for the first time a court recognises a GDPR right to an explanation for algorithmic decision-making", *EU Law Analysis*, 28/4/2021, consultato online il 15/9/2021 all'indirizzo https://eulawanalysis.blogspot.com/2021/04/the-ola-uber-judgments-for-first-time.html.

Nel marzo del 2021, tuttavia, il Tribunale di primo grado di Amsterdam, nei Paesi Bassi, ha deciso lo stessi giorno tre cause "gemelle" intentate dai rappresentanti dei lavoratori di due servizi di trasporto passeggeri tramite piattaforma, Uber e Ola[71]. In tutti e tre i casi, i ricorrenti intendevano dimostrare il proprio status di dipendenti delle aziende resistenti, le quali invece sostenevano di fornire semplicemente strumenti informatici a lavoratori autonomi – nel caso di specie, autisti che si mettevano direttamente a disposizione dei clienti.

Nel primo caso Uber e nel caso Ola, i lavoratori intendono attivare il diritto di accesso ai propri dati personali previsto dall'art. 15 GDPR e, poiché sostengono di essere oggetto di decisioni automatizzate, il diritto di spiegazione dell'algoritmo previsto dall'art. 22 GDPR[72].

Nello specifico, nel primo caso Uber i lavoratori provano ad argomentare che l'algoritmo di assegnazione automatica delle corse costituisce un trattamento vietato ai sensi dell'art. 22 GDPR, in quanto inciderebbe in maniera significativa sull'allocazione del lavoro e, pertanto, sulle possibilità di guadagno. Uber non nega che le decisioni sull'assegnazione delle corse sono automatizzate, e anzi lo riconosce nella stessa informativa sulla privacy che rilascia ai suoi utenti[73], ma nega che tali decisioni abbiano effetti giuridici o incidano significativamente sulla persona[74]. Il ricorso degli autisti Uber non riesce ad argomentare in maniera esaustiva sul punto, e pertanto i giudici olandesi decidono di respingerlo con riguardo alla richiesta di spiegazione dell'algoritmo[75].

Il ricorso del caso Ola è maggiormente dettagliato e tiene in considerazione non solamente algoritmi che esercitano il potere direttivo sugli autisti, come quelli esaminati nel primo caso Uber, ma anche altri aspetti legati al controllo e alla disciplina.

---

[71] Si tratta delle cause C/13/687315 / HA RK 20-207, XY v. Uber ("primo caso Uber"); C/13/692003 / HA RK 20-302, XY v. Uber ("secondo caso Uber"); C/13/689705 / HA RK 20-258, XY v. Ola ("caso Ola"). Una traduzione non ufficiale in lingua inglese è disponibile al sito https://ekker.legal/en/2021/03/13/dutch-Court-rules-on-data-transparency-for-uber-and-ola-drivers/, consultato il 16/9/2021.

[72] Primo caso Uber, 3.1.I(iv); caso Ola, 3.1.I(iv).

[73] Uber privacy notice, par. 9, consultata online il 15/9/2021 all'indirizzo https://www.uber.com/legal/it/document/?country=united-states&lang=en&name=privacy-notice.

[74] Primo caso Uber, 4.66.

[75] Primo caso Uber, 4.67 e 5.5.

In primo luogo, i ricorrenti lamentano la violazione dell'art. 22 da parte dello schema di retribuzione dell'azienda, che distribuisce bonus sulla base del trattamento automatizzato di dati come il numero di ore lavorate, la disponibilità ai cambi di turno e il *rating* ottenuto. I giudici riconoscono che si tratti di un'attività di profilazione, e quindi stabiliscono l'attivazione del diritto di accesso ai propri dati da parte dei lavoratori, ma non ritengono che l'influenza del sistema di bonus sulla condotta degli autisti sia tale da avere un effetto giuridico o comunque significativo[76].

Ola si serve di un secondo algoritmo, denominato "Guardian", per intervenire nei casi di irregolarità del servizio. Questo esercizio del potere di controllo, tuttavia, inizia con una segnalazione dell'algoritmo basata sui dati raccolti dai dispositivi dell'autista e del cliente, ma prosegue con l'intervento di un dipendente di Ola, che si deve personalmente mettere in contatto con l'autista. Di conseguenza, nessuna decisione automatizzata può essere riscontrata[77].

Con riguardo all'algoritmo di assegnazione delle corse di Ola vale quanto già detto a proposito di Uber: il trattamento è chiaramente automatizzato, ma non è in grado di incidere sui diritti della persona[78].

Il punto più saliente della sentenza, tuttavia, riguarda il sistema di sanzioni e deduzioni di cui l'azienda si serve per disciplinare i lavoratori nei casi in cui le corse accettate non vadano poi a buon fine. In base alle spiegazioni rese da Ola, è evidente che si tratta di una decisione automatizzata e, come riconosce la Corte, in grado di incidere sui diritti economici di cui gli autisti sotto il contratto di lavoro. Nella fattispecie, poi, l'azienda non ha allegato la presenza delle eccezioni legate all'esecuzione del contratto o al consenso degli interessati: di conseguenza, il trattamento automatizzato deve essere vietato ai sensi dell'art. 22 GDPR[79].

Oltre a ciò, i giudici olandesi riconoscono anche l'obbligo da parte di Ola di fornire ai lavoratori informazioni riguardo ai dati raccolti e, per ciò che più qui interessa, ai meccanismi di funzionamento dell'algoritmo[80]: è la prima volta che

[76] Caso Ola, 4.47. I giudici fanno anche esplicito riferimento alle Linee guida dell'Article 29 Working Party.
[77] Caso Ola, 4.48.
[78] Caso Ola, 4.50.
[79] Caso Ola, 4.51.
[80] Caso Ola, 4.52.

un simile diritto di *spiegazione* viene riconosciuto, e che ciò avvenga nel contesto del lavoro è senz'altro significativo.

Nel secondo caso Uber la situazione è parzialmente diversa: i lavoratori ricorrenti avevano visto il proprio account disattivato in seguito a una generica contestazione di condotte scorrete e chiedevano di conoscere i criteri sulla base dei quali erano stati – nella loro configurazione dei fatti – licenziati dall'azienda.

Il punto centrale, in questo giudizio, è l'intervento umano: Uber sostiene infatti che, dopo aver rilevato attività sospette attraverso i propri algoritmi – che quindi conducono senza dubbio un trattamento automatizzato -, il "Risk team" dell'azienda ha condotto autonome investigazioni e in un caso un dipendente dell'azienda ha contattato per telefono e per posta elettronica un ricorrente, contestando le irregolarità riscontrate[81].

Poiché le modalità così descritte comportano senza dubbio un rilevante intervento umano, come richiesto dalle Linee guida dell'Article 29 Working Party[82], e i ricorrenti non hanno contestato questa affermazione, in base alle norme processuali olandesi la ricostruzione di Uber viene data per pacifica: pertanto, la Corte conclude che non è possibile applicare l'art. 22 GDPR al caso di specie[83].

Queste interessantissime pronunce del Tribunale di Amsterdam non hanno chiaramente nessun impatto diretto sull'applicazione del GDPR in Italia; esse, tuttavia, forniscono all'interprete alcune indicazioni fondamentali. Innanzitutto, viene precisato il contenuto del diritto del lavoratore di cui all'art. 22 del Regolamento: l'impostazione delle Linee guida, strumento di per sé non vincolante, viene sposata in pieno e viene applicata al caso del management attraverso algoritmi. In particolare, si possono ricavare alcune coordinate in merito ai limiti della "significatività" della decisione algoritmica: è molto probabile che quando questa coinvolga il potere disciplinare essa sia sempre rilevante, mentre indicazioni in senso contrario riguardano il potere direttivo. Per quanto riguarda il controllo, nel caso Ola è stato determinante l'intervento umano: la questione rimane largamente aperta e dovrà essere attentamente esaminata in futuro.

[81] Secondo caso Uber, 4.23.
[82] V. *supra*: Article 29 Data Protection Working Party, "Guidelines", cit., p. 21.
[83] Secondo caso Uber, 4.24.

Poi, va registrato con grande interesse che i giudici olandesi hanno accolto le richieste dei ricorrenti con riguardo al "diritto di spiegazione", non previsto esplicitamente da nessuna disposizione del GDPR ma ricavabile, secondo certa dottrina, dall'interpretazione sistematica degli artt. 15 e 22[84].

Infine, è rilevantissimo che i primi casi di applicazione dell'art. 22 GDPR abbiano riguardato proprio il contesto del lavoro. È probabile che, visti i risultati incoraggianti del ricorso Ola, le organizzazioni collettive privilegino in futuro la medesima strategia processuale. Alla prova dei fatti, insomma, l'art. 22 si è dimostrato uno strumento tutto sommato efficace e ha garantito ai lavoratori in questione una tutela piena ed effettiva.

[84] G. MALGIERI (2019), cit., pp. 2-3.

Conclusioni

Il management per algoritmi ha il potenziale per rivoluzionare il mondo del lavoro in modi e con conseguenze che non è ancora possibile comprendere pienamente. Nei contesti in cui tali tecniche vengono già oggi impiegate, come il lavoro su piattaforma e la logistica, gli effetti sulla vita dei lavoratori sono stati molto rilevanti: costante sorveglianza della prestazione, raccolta intrusiva di dati personali, parcellizzazione delle mansioni e, in certi casi, precarizzazione e venir meno del luogo di lavoro come centro degli interessi dei dipendenti e del datore.

I vantaggi offerti dal management attraverso algoritmi, in particolare in termini di efficienza e di capacità di innovazione, potrebbero convincere imprenditori nei settori più diversi ad adottare questo genere di strumenti per esercitare, in maniera più o meno estesa, alcuni dei poteri datoriali. Questa tendenza è già oggi in atto e il potenziale espansivo del management attraverso algoritmi appare notevole, anche con riguardo a settori finora relativamente poco toccati dagli effetti della rivoluzione digitale come i servizi alla persona.

I possibili effetti negativi di queste nuove tecnologie sono senz'altro preoccupanti, ma proprio per questa ragione è importante analizzare il fenomeno con attenzione e valutare gli strumenti normativi già oggi a disposizione.

Innanzitutto, nella categoria del management attraverso algoritmi rientrano tecnologie anche molto diverse fra di loro. Le caratteristiche fondamentali che le accomunano, tuttavia, sono due: l'esercizio del potere direttivo, di controllo o disciplinare e la presenza di un algoritmo che, una volta inseriti i dati necessari, restituisce una decisione automatizzata.

Facendo leva sul concetto di dato, in particolare quando esso è riferibile al lavoratore, è possibile individuare due diversi sistemi di norme entrambi vigenti nel diritto italiano. Lo Statuto dei Lavoratori, in particolare con gli artt. 4 e 8, vieta alcune forme di controllo particolarmente invasive della sfera privata dei dipendenti: si può ritenere che ancora oggi i controlli a distanza siano sottoposti a limitazioni piuttosto stringenti, le quali peraltro garantiscono al sindacato di avere una rilevante voce in capitolo.

Come appena accennato, tuttavia, un elemento fondamentale del management attraverso algoritmi è che non riguarda solamente il potere di controllo e, in generale, la raccolta dei dati dei lavoratori costituisce un momento preliminare rispetto ad ogni impiego di tale tecnologia.

È anche per questa ragione che, pur non dimenticando il fondamentale approccio dello Statuto dei Lavoratori, la disposizione più promettente in vista di una regolamentazione del management attraverso algoritmi appare il diritto alla protezione dei dati personali di matrice eurounitaria, e in particolare il GDPR. L'approccio preventivo del GDPR, infatti, fa i conti con una realtà dove ogni azione dei lavoratori, ogni fase del processo produttivo, ogni comportamento dei clienti produce una grande quantità di dati che possono rientrare nell'interesse dell'azienda ed, eventualmente, essere utilizzati per gestire il personale. Il Regolamento 2016/679 istituisce dei precisi obblighi di prevenzione in capo al titolare del trattamento, cioè il datore di lavoro, a partire da una valutazione del rischio legato al trattamento dei dati.

La logica per cui l'interessato deve poter mantenere il massimo grado possibile di controllo sui suoi dati è particolarmente adatta al contesto del management attraverso algoritmi e il divieto di decisioni automatizzate, posto dall'art. 22 del GDPR, tutela i lavoratori contro alcuni degli utilizzi più discutibili della tecnologia digitale sul posto di lavoro. Le prime decisioni in questo ambito, in particolare, hanno dimostrato un concreto potenziale applicativo che andrà ulteriormente esplorato in futuro.

Si è poi detto che il management attraverso algoritmi viene impiegato sia per lavori *standard*, sia per nuove forme di lavoro legate alla *gig economy*. Il GDPR è una norma ad applicazione generale, che non è cioè rivolta al contesto lavorativo in particolare. Se questo comporta delle inevitabili mancanze, in quanto le esigenze del lavoratore sono indubbiamente diverse da quelle del consumatore o del cittadino nel rapporto con la pubblica amministrazione, l'ambito soggettivo di applicazione risolve uno dei più grandi temi lavoristici legati al lavoro su piattaforma, la qualificazione giuridica dei lavoratori. Poiché, cioè, il GDPR si applica a tutte le persone fisiche, non è rilevante che il lavoratore sia individuato dal diritto nazionale come autonomo o come subordinato.

La dimensione collettiva dovrà giocare un ruolo fondamentale, nel prossimo futuro, per adattare il GDPR al lavoro e per utilizzare al meglio gli strumenti messi a disposizione dal diritto europeo e nazionale. L'impianto del

Regolamento attribuisce agli interessati rilevanti diritti di informazione, di accesso ai dati, di controllo della loro circolazione. In alcuni casi, è anche previsto che rappresentanti degli interessati, cioè dei lavoratori, partecipino al disegno dei dispositivi di privacy: le organizzazioni sindacali potrebbero sfruttare tutti questi strumenti per incidere in maniera significativa sull'implementazione degli algoritmi nell'azienda e per limitare le conseguenze dannose per i dipendenti.

Nel frattempo, la giurisprudenza ha già dato alcune iniziali dimostrazioni di come il fenomeno del management attraverso algoritmi può essere regolato e, in alcuni casi, vietato. Gli sviluppi successivi, sia nelle Corti italiane sia nelle Corti europee, ma anche per quanto riguarda il prezioso contributo dei provvedimenti del Garante della privacy, dovranno essere attentamente seguiti; i primi risultati, in ogni caso, sono incoraggianti per i lavoratori.

Infine, i legislatori europei dovranno probabilmente elaborare una disciplina sistematica e specifica per il contesto del lavoro. Ad oggi, due disposizioni appaiono meritevoli di attenzione in questo senso: la proposta di regolamento della Commissione UE sull'intelligenza artificiale, presentata il 21 aprile scorso[1], e la ancor più recente modifica dello Statuto dei Lavoratori spagnolo dell'11 maggio scorso[2]. La proposta di regolamento introduce una serie di disposizioni applicabili a tutti gli utilizzi ad alto rischio di intelligenza artificiale, tra i quali rientra esplicitamente il contesto dell'impiego, del management dei dipendenti e dell'accesso al lavoro autonomo. Il decreto-legge spagnolo, inoltre, è il primo caso di normativa di un Paese europeo mirata alla disciplina degli algoritmi sul posto di lavoro, ed è particolarmente all'avanguardia in quanto stabilisce un alto standard di trasparenza nel disegno degli algoritmi e potrebbe risolvere alcune delle criticità riguardanti l'approccio forse eccessivamente concentrato sulla prevenzione e sulla fase della raccolta dei dati che caratterizza il GDPR.

Il diritto del lavoro, insomma, sta cercando e in alcuni casi ha già trovato delle risposte convincenti per i nuovi problemi portati dal management attraverso algoritmi. Già oggi esistono delle norme, applicabili in Italia e negli altri Stati membri dell'Unione europea, che potrebbero fornire importantissime tutele ai lavoratori contro le sempre più frequenti invasioni della loro privacy e contro gli usi indesiderabili della tecnologia ai danni della loro autodeterminazione e

[1] Commissione europea, Proposta di Regolamento COM (2021) 206 final "sull'intelligenza artificiale".
[2] Real Decreto-ley 9/2021 dell'11 maggio 2021, consultato online il 20/9/2021 all'indirizzo https://boe.es/diario_boe/txt.php?id=BOE-A-2021-7840.

libertà di pensiero. Starà alla pratica del diritto degli anni a venire scegliere se usare tali strumenti, se elaborarne di nuovi e, in definitiva, che atteggiamento adottare di fronte al management attraverso algoritmi.

Bibliografia

1. Dottrina

AA. VV. (1986), *Rivoluzione tecnologica e diritto del lavoro: Atti dell'VIII Congresso di diritto del lavoro, Napoli, 12-14 aprile 1985*, Giuffré

AA. VV. (2018), *Handbook on European Data Protection Law*, ed. European Union Agency for Fundamental Rights and Council of Europe

ACCIAI, R. (2004), *Il diritto alla protezione dei dati personali*, ed. Maggioli

ADAM, R., A. TIZZANO (2020), *Manuale di diritto dell'Unione europea*, ed. Giappichelli

ADAMS, A. (2018), "Technology and the labour market: the assessment", *Oxford Review of Economic Policy*, vol. 34, n. 3, pp. 355 e sgg.

ADAMS-PRASSL, J., (2019), "What if your boss was an algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work", *Comparative Labor Law & Policy Journal*, vol. 41 n.1, p. 141

AHMED, S., et al. (2016), "Peer-to-peer in the Workplace: A View from the Road", presentato alla CHI Conference on Human Factors in Computing Systems

AIELLO, J. (1993), "Computer Monitoring of Work Performance: Extending the Social Facilitation Framework to Electronic Presence", *Journal of Applied Social Psychology*, vol. 23 n. 7, pp. 537-548

AJUNWA, I., K. CRAWFORD, J. SCHULZ (2017), "Limitless Worker Surveillance", *California Law Review*, vol. 105 n. 6, p. 109, ed. California Law Review

ALES, E., et al. (2018), *Working in Digital and Smart Organizations*, ed. Palgrave MacMillan

ALOISI, A. (2016 a), "'Dependent contractors' in the gig economy – a comparative approach", *American University Law Review*, vol. 66 n. 3

ALOISI, A. (2016 b), "Commoditized workers: Case study research on labour law issues arising from a set of 'on-demand/gig economy' platforms",

Comparative Labor Law & Policy Journal, University of Illinois College of Law, vol. 37, n. 3, pp. 653–690

ALOISI, A., V. DE STEFANO (2020), *Il tuo capo è un algoritmo: contro il lavoro disumano*, ed. Laterza

ALVINO, I. (2016), "I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy", *Labour and Law Issues*, vo. 2 n. 1, pp. 2-45

ANTEBY, M., C. CHAN (2018), "A self-fulfilling cycle of coercive surveillance: Workers' invisibility practices and managerial justification", *Organization Science*, vol. 29 n. 2, pp. 247–263

ANTHES, E. (2017), "The shape of the work to come: Three ways that the digital revolution is reshaping workforces around the world", *Nature*, vol. 550, pp. 316-319

AUTOR, D. (2013), "The 'task approach' to labor markets: an overview", *NBER Working Paper*, n. 18711

AUTOR, D., D. DORN (2013), "The growth of low-skill service jobs and the polarization of the US labour market", *American Economic Review*, vol. 103 n. 5, pp. 1553-1597

BALL, K. (2010), "Workplace surveillance: an overview", *Labor History*, vol. 51 n. 1, pp. 87-106, ed. Routledge

BARASSI, L. (1901), *Il contratto di lavoro nel diritto positivo italiano*, ed. Società editrice libraria

BAROCAS, S., A. SELBST (2014), "Big data's disparate impact", *California Law Review*, vol. 104, pp. 671-732

BATTISTELLI, S. (2021), "Discriminazione per ragioni di affiliazione sindacale: il caso dei rider", *Il lavoro nella giurisprudenza*, n. 8-9, pp. 862-871

BELLAVISTA, A. (1995), *Il controllo sui lavoratori*, ed. Giappichelli, pp. 1-2

BEVITT, A., C. STACK (2016), "Preparing for the GDPR-advice for employers", *PDP*, vol. 16 n. 6

BLANPAIN, R., M. VAN GESTEL (2004), *Use and Monitoring of E-Mail, Intranet and Internet Facilities at Work*, ed. Kluwer Law International

BODIE, M., ET AL. (2016), "The Law and Policy of People Analytics", *Legal Studies Research Paper Series*, n. 2016-6, p. 3, St. Louis University School of Law

BUSNELLI, F. (1999), "Nota introduttiva al commento della l. 31 dicembre 1996, n. 675", *Nuove leggi civili commentate*

BUTTARELLI, G. (1997), *Banche dati e tutela della riservatezza*, ed. Giuffré

BYGRAVE, L. (2002), *Data Protection Law. Approaching Its Rationale, Logic and Limits*, ed. Kluwer Law International

CAPPONI, F. (2015), "La regolazione delle collaborazioni etero-organizzate tra legge e contratto: il caso delle piattaforme di *food delivery*", *Diritto delle relazioni industriali*, vol. 28 n. 4, pp. 1247-1260

CARINCI, M. T. (2016), "Il controllo a distanza dell'attività dei lavoratori dopo il "Jobs Act" (art. 23 D.Lgs. 151/2015): spunti per un dibattito", *Labour and Law Issues*, vol. 2 n. 1

CARUSO, B. (2020), "Tra lasciti e rovine della pandemia: più o meno smart working?", in *Rivista Italiana di Diritto del Lavoro*, n. 2

CENDON, P. (2009), *Il risarcimento del danno non patrimoniale. Parte speciale*, ed. UTET

CESTER, C. (2007), *Il rapporto di lavoro subordinato: costituzione e svolgimento*, ed. UTET

CHIECO, P. (2000), *Privacy e lavoro. La disciplina del trattamento dei dati personali del lavoratore*¸ ed. Cacucci

CRAWFORD, K., et al. (2019), *AI Now 2019 Report*, ed. NYU

CRAWFORD, K., J. SCHULTZ (2014), "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms", *Boston College Law Review*, vol. 55 n. 1, pp. 93-128

CRISAFULLI, V. (1955), "Ancora in tema di libertà costituzionali e rapporti di lavoro subordinato", nota a Pret. Torino 25 luglio 1955, *Rivista giuridica del lavoro*, vol. 2 pp. 524-532

D'ARCANGELO, L. (2020), "L'obbligo di protezione dei dati del lavoratore: adempimento e sanzioni", *Diritti lavori mercati*, vol. 1

DAGNINO, E. (2017), "People Analytics: lavoro e tutele al tempo del management tramite big data", *Labour & Law Issues*, vol. 3 n. 1

DANAHER, J. (2016), "The threat of algocracy: Reality, resistance and accommodation", *Philosophy & Technology*, vol. 29 n. 3, pp. 245–268

DE ANGELIS, L. (2021), "Su forma e prova del lavoro dei riders, anche nella pandemia", *Labor*, n. 2, pp. 59-68

DE LUCA TAMAJO, R., et al. (1988), *Nuove tecnologie e tutela della riservatezza dei lavoratori*, ed. Franco Angeli

DE STEFANO, V. (2016), "The rise of the «just-in-time workforce»: On-demand work, crowdwork and labour protection in the «gig-economy»", Conditions of work and employment series, n.71, ILO

DE STEFANO, V. (2018), "Negotiating the Algorithm: Automation, artificial intelligence and labour protection", Employment Working Paper n. 246

DE STEFANO, V. (2020), "'Masters and Servers': Collective Labour Rights and Private Government in the Contemporary World of Work", *International Journal of Comparative Labour Law and Industrial Relations*, vol. 36 n. 4

DEGRYSE, C. (2016), "Digitalisation of the economy and its impact on labour markets", ETUI Working Paper 2016.02

DEL PUNTA, R. (2016), "La nuova disciplina dei controlli a distanza sul lavoro (art. 23, D. Lgs. n. 151/2015)", *Rivista italiana di diritto del lavoro*, n. 1 pp. 77-109

DI MARTINO, F. (2016), nota a Cass. Sez. lav., 7 aprile 2016, n. 6775, *Il Lavoro nella giurisprudenza*, vol. 10, p. 902 e sgg.

DI RESTA, F. (2018), *La nuova* privacy *europea. I principali adempimenti del regolamento UE 2016/679 e profili risarcitori*, ed. Giappichelli

DURANTI, S. (1972), "Impiego dei mezzi audiovisivi e Statuto dei lavoratori", *Massimario di giurisprudenza del lavoro*, n. 1

EDERY, D., E. MOLLICK (2009), *Changing the game: How video games are transforming the future of business.*, FT Press

EDWARDS, L., M. VEALE (2017), "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For", *Duke Law & Technology Review*, vol. 16, pp. 18-84

ERNST, E. (2018), "The economics of artificial intelligence: Implications for the future of work", *ILO Future of work research paper series*

FINOCCHIARO, G. (2012), *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, ed. Zanichelli

FINOCCHIARO, G. (2017 A), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, ed. Zanichelli

FINOCCHIARO, G. (2017 b), "Introduzione al Regolamento europeo sulla protezione dei dati", *Nuove leggi civili commentate*, vol. 1 pp. 1 e sgg.

FREEDLAND, M. (1999), *Data Protection and Employment in the European Union. An Analytical Study of the Law and Practice of Data Protection and the Employment Relationship in the EU and Its Members*, ed. EC

FRENI, A., G. GIUGNI (1971), *Lo Statuto dei lavoratori*, ed. Giuffré

GAETA, L. (1990), "La dignità del lavoratore e i «turbamenti» dell'innovazione", *Lavoro e diritto*, n. 1 pp. 207 e sgg.

GELLERT, R., M. VAN BEKKUM, F. ZUIDERVEEN BORGESIUS (2021), "The Ola & Uber judgments: for the first time a court recognises a GDPR right to an explanation for algorithmic decision-making", *EU Law Analysis*, 28/4/2021, consultato online il 15/9/2021 all'indirizzo https://eulawanalysis.blogspot.com/2021/04/the-ola-uber-judgments-for-first-time.html

GHEZZI, G., et al. (1972), *Statuto dei diritti dei lavoratori*, ed. Zanichelli

GHEZZI, G. (1956), "Polizia privata nelle imprese e tutela dei diritti costituzionali dei lavoratori", *Rivista trimestrale di diritto e procedura civile*, n. 3 pp. 1003-1026

GHEZZI, G., F. LISO (1986), "Computer e controllo dei lavoratori", *Giornale di diritto del lavoro e relazioni industriali*, n.1 pp. 374 e sgg.

GHEZZI, G., U. ROMAGNOLI (1995), *Il rapporto di lavoro*, ed. Zanichelli

GIANNINI, M. (1974), "Controllo: nozioni e problemi", *Rivista trimestrale di diritto pubblico*, vol. 99 n. 1

GIUGNI, G. (1989), *Lavoro leggi contratti*, ed. Il Mulino

GOODMAN, B., S. FLAXMAN (2016), "EU Regulations on Algorithmic Decision-Making and a 'right to Explanation'", *AI Magazine*, vol. 38, n. 3

GRAHAM, M., I. HJORTH, V. LEHDONVIRTA (2017), "Digital labour and development: Impacts of global digital labour platforms and the gig economy on worker livelihoods", *Transfer: European Review of Labour and Research*, vol. 23 n. 2, pp. 135–162

GUTWIRTH, S., R. LEENES, P. DE HERT, *Reforming European Data Protection Law*, ed. Springer

HERSHBEIN, B., L. B. KAHN (2018), "Do Recessions Accelerate Routine-Biased Technological Change? Evidence from Vacancy Postings", *American Economic Review*, vol. 108 n. 7

IAQUINTA, F., A. INGRAO (2014), "La *privacy* e i dati sensibili del lavoratore legati all'utilizzo di *social networks*. Quando prevenire è meglio che curare", *Diritto delle relazioni industriali*, n. 4 pp. 1027 e sgg.

ICHINO, P. (1986), *Diritto alla riservatezza e diritto al segreto nel rapporto di lavoro*, ed. Giuffré

ICHINO, P. (2018), "Subordinazione, autonomia e protezione del lavoro nella *gig-economy*", *Rivista italiana di diritto del lavoro*, n. 2, pp. 283-303

INGRAO, A. (2017), "Il controllo disciplinare e la privacy del datore dopo il Jobs Act, *Rivista italiana di diritto del lavoro*, vol. 2 n. 1

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

JARRAHI, M. H., et al. (2019), "Platformic management, boundary resources, and worker autonomy in gig work", *Computer Supported Cooperative Work*, n. 1

KARREMAN, D., M. ALVESSON (2004) "Cages in tandem: Management control, social identity, and identification in a knowledge-intensive firm", *Organization*, vol. 11 n. 1, pp. 149–175

KELLOGG, K., M. A. VALENTINE, A. CHRISTIN (2020), "Algorithms at work: the new contested terrain of control", *Academy of Management Annals*, vol. 14 n. 1

KIM, T. W. (2018), "Gamification of Labor and the Charge of Exploitation", *Journal of Business Ethics*, vol. 152, pp. 27-39

LAMBERTUCCI, P. (2016), "La disciplina dei controlli a distanza", *Giurisprudenza italiana*, n. 3, pp. 769-776

LEE, M. K., ET AL. (2015), "Working with Machines: The Impact of Algorithmic and Data-Driven Management on Human Workers", *CHI '15: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pp. 1603-1612

LEO, L. (1981), "Le disposizioni penali dello Statuto dei lavoratori", *Rivista giuridica del lavoro*, n. 4 p. 730 e sgg.

LEVI, K., S. BAROCAS (2018), "Refractive Surveillance: Monitoring Customers to Manage Workers", *International Journal of Communication*, vol. 12, pp. 1166–1188

LOSANO, M. G. (2001), *La legge italiana sulla privacy. Un bilancio dei primi cinque anni*, ed. Laterza

MALGIERI, G. (2019), "Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations", *Computer Law and Security Review*, vol. 35 pp. 2 e sgg.

MALGIERI, G., G. COMANDÉ (2017), "Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation", *International Data Privacy Law*, vol. 7 n. 4, pp. 243-265, OUP

MANTELERO, A. (2016), "Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection", *Computer Law and Security Review*, vol. 32

MAYER-SCHONBERGER, P. (1997), *Generational developement of data protection in Europe?*, in P. AGRE, M. ROTENBERG (1997), *Technology and Privacy*, ed. MIT Press

MAZZOTTA, O., (2019), *Diritto del lavoro*, ed. Giuffré

MCAFEE, A., E. BRYNJOLFSSON (2017), *Machine, Platform, Crowd: Harnessing our Digital Future*, ed. WW Norton & Co.

MCCARTHY, W. (1992), *Legal Intervention in Industrial Relations: Gains and Losses*, ed. Blackwell

MENGONI, L. (1965), "Contratto e rapporto di lavoro nella recente dottrina italiana", *Rivista della Società*, pp. 674 e sgg.

MOORE, P., M. UPCHURCH, X. WHITTAKER, *Humans and Machines at Work*, ed. Palgrave MacMillan.

NERINCKX, S. (2016), "The 'Uberization' of the Labour Market: Some Thoughts from an Employment Law Perspective on the Collaborative Economy", *ERA Forum*, vol. 17 n. 2

O'NEIL, C. (2016), *Weapons of Math Destruction: how Big Data Increases Inequality and Threatens Democracy*, ed. Crown

OGRISEG, C. (2018), "Inutilizzabilità delle informazioni raccolte tramite gestionali e posta elettronica per mancata informativa al dipendente", *GiustiziaCivile.com*

PALUMBO, R., (2020), "Let me go to the office! An investigation into the side effects of working from home on work-life balance", *International Journal of Public Sector Management*, vol. 33 n. 6/7, pp. 771-790

PANETTA, R. (2006), *Libera circolazione e protezione dei dati personali*, ed. Giuffré, vol. 1

PASQUALE, F. (2015), *The Black Box Society: The Secret Algorithms That Control Money and Information*, p. 38, ed. Harvard University Press

PONCE DEL CASTILLO, A., (2020), "COVID-19 contact-tracing apps: how to prevent privacy from becoming the next victim", ETUI Policy Brief n. 5/2020

PROIA, G. (2016), "Trattamento dei dati personali, rapporto di lavoro e l'«impatto» della nuova disciplina dei controlli a distanza", *Rivista italiana di diritto del lavoro*, vol. 1 n. 4 pp. 547 e sgg.

RIVA SANSEVERINO, L. (1958), *Diritto del lavoro*, ed. CEDAM

RODOTÀ, S. (1997), "Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali", *Rivista critica di diritto privato*, n. 1 pp. 583 e sgg.

ROMAGNOLI, U. (1970), "Sulla rilevanza della reticenza del prestatore di lavoro come «culpa in contrahendo», nota a Cass., 30 dicembre 1969 n. 4059, *Giurisprudenza italiana*, n. 1 vol. 1, pp. 1066-1070

ROMEI, R., S. SCIARRA (1995), "The Protection of Employees' Privacy: A Survey of Italian Legislation and Case Law", *Comparative Labour Law Journal*, vol. 17 n. 1

ROSENBLAT, A., L. STARK (2016), "Algorithmic labor and information asymmetries: A case study of Uber drivers", *International Journal of Communication*, vol. 10, pp. 3758–3784

RUBINSTEIN, S. (2011), "Regulating Privacy by Design", *Berkeley Technology Law Journal*, vol. 26 n. 3, pp. 1409 e sgg.

SAMUEL, A. (1967), "Some studies in machine learning using the game of checkers", *IBM Journal*, pp. 601-617

SCHAAR, P. (2013), "Die geplante EU-Datenschutz-Grundverordnung, Auch beim Beschäftigtendatenschutz ist ein Nachbessern erforderlich", *Computer und Arbeit* n. 3

SCHLESINGER, P. (2021) *Trattato di diritto civile e commerciale*, ed. Giuffré, vol. 3

SELBST, A., J. POWLES (2017), "Meaningful information and the right to explanation", *International Data Privacy Law*, vol. 7 n. 4, pp. 233–242

SEPE, O., (2010), voce "Controlli", *Enciclopedia Giuridica*, ed. Treccani, vol. 4

SICA, S., V. D'ANTONIO, G. RICCIO (2016), *La nuova disciplina europea della* privacy, ed. Wolters Kluwer

SITZIA, A. (2016), "Il controllo (del datore di lavoro) sull'attività dei lavoratori: il nuovo articolo 4 st. Lav. e il consenso (del lavoratore)", *Labour and Law Issues*, vol. 2 n. 1 pp. 83 e sgg.

SITZIA, A., G. CINÀ (2020), "Subordinazione ed etero-organizzazione: rider e "debolezza economica" in una prospettiva comparata", *La nuova giurisprudenza civile commentata*, n. 4

SMURAGLIA, C. (1960), "Progresso tecnico e tutela della personalità del lavoratore", *Rivista giuridica del lavoro*, n. 1

SMURAGLIA, C., (1967), *La persona del prestatore nel rapporto di lavoro*, ed. Giuffré

TAYLOR, F. W. (1911), *The Principles of Scientific Management*, ed. Harper

TAYLOR, P., G. MULVEY, J. HYMAN, P. BAIN (2002), "Work organisation, control and the experience of work in call centres", *Work, Employment & Society*, vol. 16 n. 1, pp. 133–150

TEBANO L. (2016), "La nuova disciplina dei controlli a distanza: quali ricadute sui controlli conoscitivi?", *Rivista Italiana di diritto del lavoro*, n. 3 p. 345 e sgg.

TENE, O., J. POLONETSKY (2012), "Privacy in the Age of Big Data: A Time for Big Decisions", *Stanford Law Review Online*, vol. 64 n. 63, pp. 63-69

THALER, R. H., C. R. SUNSTEIN (2009), *Nudge: Improving decisions about health, wealth, and happiness*, ed. Penguin

TREMOLADA, M. (1993), *Il licenziamento disciplinare*, ed. CEDAM

TREU, T. (1990), voce "Statuto dei lavoratori", in *Enciclopedia del diritto*, ed. Treccani, vol. XLIII p. 1051

TROJSI, A. (2013), *Il diritto del lavoratore alla protezione dei dati personali*, ed. Giappichelli

TROJSI, A. (2016), "Controllo a distanza (su impianti e strumenti di lavoro) e protezione dei dati del lavoratore, *Variazioni su temi di diritto del lavoro*, n. 4 pp. 667 e sgg.

TULLINI, P. (2017), *Web e lavoro. Profili evolutivi e di tutela*, ed. Giappichelli

TULLINI, P., *Controlli a distanza e tutela dei dati personali del lavoratore*, ed. Giappichelli

VALENTINE, M., R. HINDS (2021), "'Rolling Up the Leaf Node' To New Levels of Analysis: How Algorithmic Decision-Making Changes Roles, Hierarchies, and Org Charts", *Stanford Engineering WP*

VALLAS, S., A. KOVALAINEN (2019), *Work and Labor in the Digital Age*, ed. Emerald

WABER, B. (2013), *People Analytics*, ed. Pearson

WACHTER, S., B. MITTELSTADT, L. FLORIDI (2017), "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation", *International Data Privacy Law*, vol. 7 n. 2, pp. 76–99

WARREN, S., L. BRANDEIS (1890), "The right to privacy", *Harvard Law Review*, vol. 4 n. 5, pp. 193-220

ZATTI, P. (2009), *Maschere del diritto. Volti della vita*, ed. Giuffré

ZUBOFF, S. (2015), "Big other: surveillance capitalism and the prospects of an information civilization", *Journal of Information Technology*, 30, pp. 75–89

2. *Articoli di giornale*

Lohr, S., "'The Beginning of a Wave': A.I. Tiptoes Into the Workplace", *The New York Times* 5/8/2018, consultato online il 20/8/2021 all'indirizzo https://www.nytimes.com/2018/08/05/technology/workplace-ai.html?searchResultPosition=4

Waters, R., "Transformation is crucial when digital disruption is the norm", *Financial Times* 30/9/2015

Sonnemaker, T., "Amazon is deploying AI cameras to surveil delivery drivers '100% of the time'", *Business Insider*, 3/2/2021, consultato online il 20/8/2021 all'indirizzo https://www.businessinsider.com/amazon-plans-ai-cameras-surveil-delivery-drivers-netradyne-2021-2?r=US&IR=T.

Vinci, A., Amazon, gli autisti Usa sorvegliati da una telecamera: sono obbligati a firmare il «consenso biometrico», *Corriere della Sera*, 26/3/2021, consultato online il 20/8/2021 all'indirizzo https://www.corriere.it/tecnologia/21_marzo_26/amazon-autisti-usa-sorvegliati-una-telecamera-sono-obbligati-firmare-consenso-biometrico-cb073d88-8d6f-11eb-90de-f8af7075b4bc.shtml

Kaplan, E., "The Spy who Fired Me: The Human Costs of Workplace Monitoring", *Harper's Magazine* 3/2015

Morosi, S., "Amazon brevetta il braccialetto elettronico che controlla i lavoratori: scoppia la polemica", *Corriere della Sera*, 1/2/2018, consultato online il 20/8/2021 all'indirizzo https://www.corriere.it/cronache/18_febbraio_01/amazon-brevetta-braccialetto-elettronico-che-controlla-lavoratori-scoppia-polemica-6eacf7d2-0760-11e8-8886-af603f13b52a.shtml

Baraniuk, C., "How algorithms run Amazon's warehouses", *BBC Future*, 18/8/2015, consultato il 20/8/2021 all'indirizzo https://www.bbc.com/future/article/20150818-how-algorithms-run-amazons-warehouses

Dave, P., "Companies bet on AI cameras to track social distancing, limit liability", *Reuters* 27/4/2020, consultato online il 20/8/2021 all'indirizzo https://www.reuters.com/article/us-health-coronavirus-surveillance-tech-idUSKCN22914R.

Ramsaroop, C., "Reality Check 101: Rethinking the impact of automation and surveillance on farm workers", sul blog *Data & Society: Points*, https://medium.com/@ramsaroopchris?p=c6e501c3b9a3

Goldstein, J., "The future of work looks like a UPS truck", podcast di National Public Radio, consultato online il 20/8/2021 all'indirizzo https://www.npr.org/ sections/money/2014/05/02/308640135/episode-536- the-future-of-work-looks-like-a-ups-truck

Robinson, C., "Exploring portable ratings for gig workers", 2/2/2018, consultato online il 10/9/2021 all'indirizzo https://medium.com/doteveryone/exploring-portable-ratings-for-gig-workers-5632fd9b262e

Peck, D., "We are watching you at work", *The Atlantic*, 12/2013, consultato online il 20/8/2021 all'indirizzo https://www.theatlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681/.

3. Documenti consultati

Article 29 Data Protection Working Group, Opinione 2/2017 "sul trattamento dei dati sul posto di lavoro", versione italiana

Article 29 Data Protection Working Party, "Opinion 2/2017 on data processing at work", p. 4, adottata l'8 giugno 2017, consultata online il 18/9/2021 all'indirizzo https://ec.europa.eu/newsroom/article29/items/610169

Article 29 Data Protection Working Party, "Statement on the role of a risk-based approach in data protection legal frameworks", 30/5/2014

Article 29 Data Protection Working Party, Documento WP251rev.01, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679", 3/10/2017 rivisto il 6/2/2018

Article 29 Data Protection Working Party, Opinion 15/2011 del 13/6/2011

Article 29 Data Protection Working Party, parere 00569/13/EN "Sul principio di finalità", 2/4/2013

Article 29 Data Protection Working Party, WP 242 rev.01, "Guidelines on the right to data portability"

Commissione europea, Comunicazione "First stage consultation of social partners on the protection of workers' personal data", 2003

Commissione europea, Comunicazione "Second stage consultation of social partners on the protection of workers' personal data", 2004

Commissione europea, Comunicazione COM (97) 390 final, "The social and labour market Dimension of the Information Society; People First-Next Steps"

Commissione europea, Report COM(2003) 265 final, "First report on the implementation of the Data Protection Directive (95/46/EC)"

Consiglio d'Europa, "Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data", n. 108/2018

EDPS, "Assessing the necessity of measures that limit the fundamental right to the protection of personal data. A Toolkit", 11/4/2017, consultato online il 15/9/2021 all'indirizzo https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf

ETUC, "ETUC position in the General Data Protection Regulation. Improving the protection of workers' data"

European Data Protection Supervisor, "Guidelines on the Rights of Individuals with regard to the Processing of Personal Data", 25/2/2014, consultato online il 10/9/2021 all'indirizzo https://edps.europa.eu/sites/default/files/publication/14-02-25_gl_ds_rights_en.pdf

European Data Protection Supervisor, "Guidelines on the Rights of Individuals with regard to the Processing of Personal Data", 25/2/2014

European Data Protection Supervisor, Opinion 7/2015. "Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability", 19/11/2015

Garante della privacy, provvedimento 23/11/2006 "Linee-guida per il trattamento dei dati dei dipendenti privati"

Ministero del Lavoro, Comunicato stampa del 18 giugno 2015, consultato online il 9/4/2021 all'indirizzo https://www.lavoro.gov.it/stampa-e-media/Comunicati/Pagine/20150618-Controlli-a-distanza.aspx
Ministero della Giustizia, "Comunicazioni alla Commissione UE – Attuazione a livello nazionale del Regolamento (UE) 2016/679"

Parere del Comitato Economico e Sociale Europeo INT/823, "Il mercato unico digitale - Tendenze e prospettive per le PMI"

Parlamento europeo, DG for Internal Policies, studio PE 474.440, "Protection of Personal Data in Work-related Relations"

Ringraziamenti

Grazie a questi cinque anni, perché li ho potuti condividere con le persone a cui voglio bene.