DSL

1-2024

Data protection e sicurezza sul lavoro: un documento di valutazione dei rischi (DVR) anche per la *privacy*?**

di Lucia D'Arcangelo*

1. *Delimitazione del campo d'indagine*

Sul tema del lavoro automatizzato il quadro regolatorio è caratterizzato da varie fonti normative, dalla cui esegesi interpretativa, svolta in altra sede[1], è emerso il ruolo centrale del Regolamento sulla protezione dei dati personali (UE) 2016/679[2] (d'ora in poi: Gdpr).

* Lucia D'Arcangelo è professore associato di Diritto del lavoro presso il Dipartimento di Giurisprudenza dell'Università di Napoli Federico II. *lucia.darcangelo@unina.it*

** Il saggio è stato preventivamente assoggettato alla procedura di referaggio prevista dalle regole editoriali della Rivista.

[1] Mi permetto di rinviare al mio *Diritti di informazione e dati personali nel lavoro automatizzato. Rilievi sistematici sulla normativa applicabile*, in "Diritti lavori mercati", 2023, n. 2, pp. 347-371.

[2] Si tratta dei seguenti provvedimenti legislativi: decreto legislativo 27 giugno 2022, n. 104, che ha dato attuazione in Italia alla direttiva (UE) 2019/1152 sulla trasparenza delle condizioni di lavoro; proposta di direttiva COM (2021) 762 final sul lavoro mediante piattaforme digitali; proposta di regolamento sull'intelligenza artificiale COM (2021)0206 final (ora: Legge sull'intelligenza artificiale, IA Act). Si rammenta che il testo dovrebbe, nelle previsioni, essere approvato in via definitiva nel mese di marzo o aprile e dopo la pubblicazione in Gazzetta ufficiale entrerà in vigori trascorsi due anni. Sul testo dell'IA Act, si rinvia, per tutti, al contributo di A. ALAIMO, *Il Regolamento sull'Intelligenza Artificiale dalla proposta della Commissione al testo approvato del Parlamento. Ha ancora senso il pensiero pessimistico?*, in "federalismi.it", n. 25/2023, p. 133 ss. Con riferimento al tema della trasparenza, si veda la sezione ricerche del n. 1/2023 di "Diritto delle relazioni industriali" e da ultimo E. DAGNINO, C. GAROFALO, G. PICO, P. RAUSEI (a cura di), *Commentario al d.l. 4 maggio 2023, n. 48 cd. "decreto lavoro", convertito con modificazioni in l. 3 luglio 2023, n. 85*, Adapt University Press, 2023; in relazione anche alle piattaforme digitali, tra le varie voci bibliografiche più recenti, cfr. R. RAINONE, *Obblighi informativi e trasparenza del lavoro nelle piattaforme digitali*, in "federalismi.it" n. 3/2024; M. DELFINO, *Lavoro mediante piattaforme digitali, dialogo sociale europeo e partecipazione sindacale,* in "federalismi.it", n. 25/2023; P. MONDA, *The Notion of the Worker in EU Labour Law: "Expansive Tendencies" and Harmonisation Techniques*, in "Diritti lavori mercati – International", n. 2, 2022; nonché, ampiamente, A. DONINI, *Il lavoro attraverso le piattaforme digitali*, Bononia University Press, 2019.

In tale contesto, si propone una riflessione sul problema della sicurezza dell'ambiente di lavoro di una fabbrica intelligente *(smart factory)*[3], dal punto di vista della garanzia dei requisiti minimi di legalità algoritmica, con particolare riguardo alla individuazione di modelli di tutela dei dati personali applicabili al rapporto di lavoro.

Il ricorso a tecnologie di automazione digitalizzata e/o robotica (anche basate sull'intelligenza artificiale) nello svolgimento dell'attività lavorativa, come vedremo appena più dettagliatamente nel prossimo paragrafo, indubbiamente arreca enormi vantaggi alla produttività aziendale, in termini *sia* qualitativi *sia* quantitativi. Del resto, come noto, l'adozione di nuovi meccanismi di produzione fa parte delle normali esigenze di riassetto dell'azienda e rientra nell'esercizio della libertà di iniziativa economica (art. 41 Cost.), di creazione di un assetto organizzativo, amministrativo e contabile adeguato alla natura dell'attività d'impresa (art. 2086 c.c.)[4].

Tuttavia, è un dato oramai acquisito che le nuove tecnologie impattano sui diritti fondamentali dei lavoratori[5], ed è fortemente avvertita l'esigenza di individuare adeguate forme di bilanciamento tra poteri datoriali e diritti dei lavoratori[6].

In questo nuovo ecosistema del lavoro, caratterizzato da un vero e proprio mutamento di paradigma dell'impresa di matrice fordista e dell'organizzazione stessa del lavoro, in primo luogo, emerge la necessità di tutelare i lavoratori dalla raccolta massiccia e pervasiva di qualsiasi dato che attiene alla loro sfera personale, sgombrando il campo da tentativi di iper-regolarizzazione legislativa a favore di architetture normative più snelle e, in qualche misura, semplificatorie.

A tal fine, e sulla scorta di modelli già collaudati in altri settori della materia giuslavoristica, tempo addietro si è prospettato l'accostamento tra la regolamentazione europea sui dati personali e la disciplina in materia di salute e sicurezza nei luoghi di lavoro (d.lgs. n. 81/2008) per quanto attiene al profilo della strumentazione di tutela[7].

Con la presente indagine si intende proseguire tale percorso, dapprima con riguardo ai profili caratterizzanti l'ambiente di lavoro intelligente, al fine di metterne in rilievo i vantaggi e soprattutto i potenziali rischi. Successivamente, ci

[3] In tema, v. per tutti, M. FAIOLI, *Mansioni e macchina intelligente*, Giappichelli, Torino, 2018.

[4] Su questo aspetto, cfr. M. TIRABOSCHI, *Nuovi modelli della organizzazione del lavoro e nuovi rischi*, in "Diritto della sicurezza sul lavoro", 2022, 1, I, pp. 146-147.

[5] M. DELFINO, *Intelligenza artificiale, robotica e diritti fondamentali*, in "Italian Labour Law e-Journal", vol. 1, n. 2, 2023.

[6] U. GARGIULO, *Intelligenza Artificiale e poteri datoriali: i limiti normativi e ruolo dell'autonomia collettiva*, in "federalismi.it", n. 29/2023.

[7] Accostamento, è appena il caso di osservare, con cui non si intende sostenere che la disciplina sui dati personali sta dentro *o* fuori la materia della sicurezza sul lavoro. Sul punto, sia consentito rinviare al mio *I controlli a distanza dopo il Jobs Act. Dallo Statuto dei lavoratori alla disciplina sulla protezione dei dati personali*, in "Massimario di giurisprudenza sul lavoro", 2016, 10, pp. 638-650. Su tale profilo, più recentemente, si veda M. PERUZZI, *Intelligenza artificiale e lavoro*, Giappichelli, Torino, 2023, p. 75 ss.; A. INGRAO, *Manuale operativo per la protezione dei dati personali dei lavoratori*, Biblion edizioni, 2022, p. 20.

si sofferma sull'applicabilità nel rapporto di lavoro dei principi posti a garanzia della legalità algoritmica, con l'obiettivo, specifico, di verificare la configurabilità di un modello di *data protection* del lavoro automatizzato sul paradigma del sistema di sicurezza sul lavoro delineato nel d.lgs. n. 81/2008[8].

2. *Vantaggi e rischi dell'ambiente di lavoro intelligente*

Nelle realtà produttive che ricorrono a tecniche di automazione basate sull'intelligenza artificiale, l'integrazione tra lavoro umano e tecnologia realizza un coordinamento di persone, processi e strumenti di lavoro fondato sul "digital supply chain", un sistema di fornitura interconnesso, in grado di sincronizzare la domanda di un prodotto e la sua disponibilità, per soddisfare nei tempi attesi le richieste dei consumatori.

E' così, che, l'idea di fornitura tradizionalmente intesa quale sequenza di fasi di lavoro isolate l'una dall'altra, senza trasparenza delle informazioni e con scarsa sincronizzazione delle operazioni, cede il passo ad un sistema produttivo automatizzato, che appare in grado di soddisfare in maniera quasi simultanea esigenze di sostenibilità della gestione del lavoro e della produttività, dell'ambiente in generale e di quello lavorativo in particolare, per il benessere psicofisico di tutti i lavoratori[9].

Tecnologie *hardware* e *software* ri-configurano i sistemi di produzione rendendoli evolutivi e adattivi; l'organizzazione del lavoro va incontro, a sua volta, a nuove esigenze di evoluzione e adattamento, mentre le imprese che hanno già riprogettato la propria organizzazione, avvalendosi di architetture digitali integrate sulla base di una vera e propria sinergia tra macchine, informazioni e persone, sono notevolmente aumentate rispetto alle più tradizionali organizzazioni fordiste.

Le metodologie impiegate[10] rientrano nel più vasto ambito delle tecnologie abilitanti del piano Industria 4.0 e si basano sulla produzione di un flusso

[8] Si tiene a sottolineare che la nostra indagine si svolgerà entro i predetti confini. Pertanto, gli approfondimenti dei temi contigui e i richiami bibliografici saranno esclusivamente limitati a quanto utile a questi fini. Per uno sguardo sull'impatto delle nuove tecnologie sull'organizzazione del lavoro, si veda, per tutti, P. PASCUCCI, *Le nuove coordinate del sistema prevenzionistico*, in "Diritto della sicurezza sul lavoro", 2023, 2, I, spec. p. 44, dove osserva che «Come l'impetuoso impatto delle tecnologie sull'organizzazione del lavoro impone nuovi adeguamenti dei presidi prevenzionistici, volti soprattutto a contrastare i riflessi che le varie forme di intelligenza artificiale producono sui lavoratori che operano mediante piattaforme, ponendo a repentaglio quella che l'art. 2087 c.c. chiama la loro «personalità morale» e che altro non è se non la loro dignità», menzionando, tra i vari obblighi del datore di lavoro, quello di «cessare immediatamente l'uso del sistema automatizzato ove la valutazione d'impatto individui rischi per la salute e la sicurezza o per i diritti fondamentali che non possano essere evitati né attenuati».

[9] D. GAROFALO, *Lavoro, impresa e trasformazioni organizzative*, in AA.VV., *Frammentazione organizzativa e lavoro: rapporti individuali e collettivi. Atti delle Giornate di studio di Diritto del lavoro. Cassino, 18-19 maggio 2017*, Milano, Giuffrè, 2018, p. 171 ss.

[10] Sulle tecnologie attualmente in uso, dal sistema *Internet of Things (IoT)*, alla robotica, alla manifattura additiva e *digital reality,* alle piattaforme digitali, all'intelligenza artificiale, si veda il report Tecnologie_Abilitanti-ICT_Position-Paper-S3-2021-2027 reperibile sul sito *https://europa.regione.campania.it*.

informativo che si autoalimenta, con una autonomia variabile, a seconda della strumentazione utilizzata (*analitycs, machine learning*) e della scelta di abilitare o meno logiche predittive.

Una volta raccolte, le informazioni vengono storicizzate e analizzate per entrare a far parte del patrimonio informativo dell'azienda, che si autorigenera producendo dati utili per decisioni probabili e future, in un processo di apprendimento continuo basato sulla interconnessione tra i vari reparti aziendali, che è funzionale a rendere l'azienda stessa in grado di prendere decisioni in tempo reale o, in alcuni casi, addirittura in via anticipata, come nel settore della manutenzione, per evitare ritardi che possono rallentare i ritmi di produttività.

Questo è il principale vantaggio di un'impresa connessa: l'ottimizzazione della produttività dovuta alla trasparenza nella comunicazione interattiva tra i vari settori e tra i suoi stessi componenti, intesi come macchine e processi che diventano reciprocamente accessibili, rendendo l'impresa un soggetto commerciale agile in termini di risposta alla domanda del prodotto. Inoltre, il monitoraggio continuo della produzione attraverso il controllo non solo delle macchine e dei processi ma anche dei lavoratori, incide sulla qualità della produzione, contribuendo ad una riduzione degli scarti, ad un aumento dell'efficienza della produzione e, in proporzione, ad una riduzione dell'impatto ambientale, cui consegue pure una diminuzione dei costi.

Il rovescio della medaglia, tuttavia, è rappresentato dalle conseguenze sull'organizzazione del lavoro e sul *well being* dei lavoratori[11].

Da questo punto di vista, l'algoritmizzazione determina una frammentazione spazio-temporale del processo produttivo che consente di mantenere le connessioni informatiche in stato di perenne attività, tanto all'interno quanto all'esterno dei luoghi di lavoro[12], con una sovrapposizione tra tempi di lavoro e tempi di non lavoro che comporta la reperibilità costante del lavoratore.

[11] Per inciso, va detto che ulteriori conseguenze riguardano la disoccupazione diffusa e l'aggravamento delle disuguaglianze. Su questo versante si delinea l'area dei rischi cd. sociali: primo fra tutti, la destabilizzazione del sistema economico e sociale, che si percepisce come un effetto quasi fisiologico delle tecnologie intelligenti e di tutto ciò che esse comportano, dall'alterazione dei processi produttivi alla frammentazione dell'organizzazione del lavoro e alla riduzione delle mansioni. Sulla questione dei rischi (e dei diritti) sociali la letteratura è copiosa, si veda, per tutti, il contributo di D. GAROFALO, *I diritti sociali nella bufera della pandemia*, in "Working Paper Adapt", University Press, n. 5/2023; M. FRANZINI, *Intelligenza artificiale e prospettive del lavoro: il ruolo delle istituzioni economiche*, in "Giornale italiano di psicologia", 1, 2018, pp. 125-129; e ampiamente, R. RIZZA, *Politiche di* welfare *e nuovi rischi sociali*, in R. RIZZA, F. BONVICINI (a cura di), *Attori e territori del* welfare. *Innovazioni nel* welfare *aziendale e nelle politiche di contrasto all'impoverimento*, Franco Angeli, Milano, 2014, pp. 13-28.

[12] M. MAGNANI, *I tempi e i luoghi di lavoro. L'uniformità non si addice al post-fordismo*, in "WP C.S.D.L.E. "Massimo D'Antona".IT", n. 404/2019, p. 2 ss. che evidenzia come oggi «non conta più solo lo spazio fisico di lavoro (cd. biosfera), peraltro anch'esso rivoluzionato, ma anche quello aggiuntivo chiamato suggestivamente "infosfera" (con il cloud, i social network, ecc.)»; nello stesso senso L. NOGLER, *Gli spazi di lavoro nelle città tra innovazioni tecnologiche e "regressioni" interpretative*, in A. OCCHINO (a cura di), *Il lavoro e i suoi luoghi*, Vita e Pensiero, Milano, 2018, p. 38; più ampiamente, sulla trasformazione del tempo di lavoro nel quadro normativo eurounitario di riferimento, v. M. TIRABOSCHI (a cura di), *Bilancio e prospettive di una ricerca*, Adapt University Press, 2021, vol. I, p. 91 ss.

In questa dimensione di connettività diffusa si verifica un aumento dello stress lavorativo, con conseguente diminuzione della qualità del lavoro prestato e un corrispondente abbassamento dei livelli di *well being* aziendale[13]. A ciò contribuisce, peraltro, il controllo a distanza dell'attività lavorativa effettuato *sia* tramite i consueti impianti di videosorveglianza *sia* attraverso gli strumenti di lavoro e/o i dispositivi indossabili, che, com'è noto, a differenza dei primi, non rientrano nel perimetro applicativo delle garanzie procedurali per i lavoratori stabilite dall'art. 4, comma 1, dello Statuto dei lavoratori.

Va da sé, poi, che la razionalità algoritmica segue regole e percorsi propri della tecnologia che (solo) l'intervento umano può controllare, almeno fino ad un certo punto. Quanto sappiamo, infatti, è che la conoscibilità e il livello di comprensione del procedimento decisionale della macchina algoritmica diminuiscono di pari passo con il grado di autonomia dell'allenamento algoritmico[14], cosicché il punto di non ritorno è dato dal raggiungimento della cd. opacità algoritmica[15], che non lascia adito ad alcuna forma di sillogismo aristotelico, dove nessun ragionamento di tipo deduttivo può essere applicato, nessuna spiegazione, di questo o di quel risultato, può essere invocata[16].

Questo meccanismo quasi clorofilliano di "assorbimento e rilascio" di dati conferisce all'algoritmo intelligente un «carattere trasformativo, la capacità cioè di generare profondi e dirompenti cambiamenti – che – è connesso ai suoi gradi di autonomia»[17]. Di qui l'importanza di comprendere che la progettazione, la programmazione, e quindi la produzione di tecniche di automazione intelligente hanno un rilievo non indifferente in termini di impatto sui diritti fondamentali dei lavoratori.

In tal senso, da una parte, è condivisibile che trattandosi di un fenomeno di ampiezza globale non si può prescindere da un inquadramento di regole altrettanto «globali», secondo cui la prospettiva auspicabile può essere «una raccolta (..) che estragga da Carte, Convezioni, Dichiarazioni, protocolli, risoluzioni il *proprium* di una normazione responsabilizzante, (…) una autentica Costituzione algoritmica (…)»[18]; ma da un'altra parte, pur mantenendo fede all'auspicio di una normazione di principio a livello sovranazionale, si ritiene possibile qualche tentativo di regolazione giuridica da parte dei tradizionali circuiti di governo legislativo

[13] Sul legame tra iperconessione e stress da lavoro correlato v. M.C. CATAUDELLA, *Tempo di lavoro e tempo di disconnessione*, in "Massimario di giurisprudenza del lavoro", 2021, 4, pp. 853-872. Tra i più comuni, la sindrome *burnout*. In tema, v. D. VERDUCCI, *Oltre il* job burnout. *A partire dalle* helping professions, in "Lavoro Diritti Europa", n. 3/2023.

[14] V. *infra*, nota 32.

[15] Principalmente, v. S.J. RUSSELL, P. NORVIG, *Intelligenza artificiale. Un approccio moderno*, 4° ed., vol. I e II, F. AMIGONI (a cura di), Pearson, London, 2021; M. BODEN, *L'intelligenza artificiale*, in D. MARCONI (a cura di), Mulino, Bologna, 2019.

[16] Siamo nell'ambito della "*strong* AI", v. F. URICCHIO, Robot tax: *modelli di prelievo e prospettive di riforma*, in "Giurisprudenza italiana", luglio 2019, p. 1751.

[17] G. COMANDÈ, *Intelligenza artificiale e responsabilità tra liability e accountability. Il carattere trasformativo dell'IA e il problema della responsabilità*, in "Analisi Giuridica dell'Economia", 2019, 1, p. 173 ss.

[18] Così, A. CELOTTO, *Come regolare gli algoritmi. Il difficile bilanciamento tra scienza, etica e diritto*, in "Analisi Giuridica dell'Economia", 2019, 1, pp. 58-59.

nazionale, proprio in considerazione del grado di frammentazione dell'attuale cornice eurounitaria di riferimento[19].

In questa direzione, ci soffermiamo dapprima sui principi generali in tema di legalità algoritmica.

3. *La legalità algoritmica nel rapporto di lavoro: i principi applicabili*

Nel rapporto di lavoro trovano applicazione due principi fondamentali idonei a garantire requisiti minimi di legalità algoritmica: prevenzione e *accountability*. Entrambi sono di derivazione europea e hanno fonte comune nel Gdpr.

Il principio di prevenzione è noto all'ambito della sicurezza nei luoghi di lavoro sin dai tempi della legislazione degli anni Cinquanta, appunto conosciuta come legislazione prevenzionistica[20], mentre il secondo ha radici meno antiche ma ugualmente solide nel contesto normativo della *data protection*.

Al funzionamento dell'algoritmo nel rapporto di lavoro possono trovare applicazione alcuni criteri derivati dalla recente elaborazione della giurisprudenza, in particolare amministrativa, la quale ha individuato nella conoscibilità, non esclusività e non discriminazione, i tre pilastri della legalità algoritmica. Su di essi, si precisa sin da ora, ci si soffermerà con il limitato obiettivo di evidenziarne l'essenza valoriale elaborata, specificatamente, dai medesimi giudici amministrativi, senza entrare nel merito del dibattito dottrinale (e giurisprudenziale) relativo al rapporto di lavoro, che a tutt'oggi è in corso di sviluppo (v. i*nfra*, par. 3.2.).

3.1. *Prevenzione e* accountability

Con riferimento al principio di prevenzione, esso obbliga il titolare del trattamento ad adottare una serie di misure volte a prevenire le conseguenze

[19] Ci si riferisce, oltre al testo sulla intelligenza artificiale (IA Act) e alla Proposta di direttiva sulle piattaforme digitali, su cui si rinvia ai relativi richiami bibliografici della nota 2, al Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio del 13 dicembre 2023, che prevede l'armonizzazione delle norme in materia di accesso equo ai dati e al loro utilizzo (cd. Data Act); al Regolamento UE 2022/868, del Parlamento europeo e del Consiglio del 30 maggio 2022, in tema di governance europea dei dati che prevede l'istituzione di un mercato interno di dati (cd. Data Governance Act); ai Regolamenti (UE) sui mercati digitali (cd. Digital Market Act) e sui servizi digitali (Digital Service Act), approvati contestualmente dal Parlamento europeo e dal Consiglio il 5 luglio 2022.

[20] Per un *excursus* storico della tutela della salute e sicurezza sul lavoro, a partire dal periodo del fascismo, si veda, da ultimo, M. MORELLO, *La tutela della salute e della sicurezza sul lavoro nell'Italia fascista*, in "Diritto della sicurezza sul lavoro" Quaderno, 2024, 1.

negative che possono verificarsi dall'uso di strumenti tecnologici idonei a ledere la dignità e le libertà fondamentali della persona[21].

Fil rouge del Gdpr, la logica della prevenzione connota la regolamentazione sui dati nell'organizzazione di lavoro imprimendole quel carattere prevenzionale che caratterizza la disciplina in materia di salute e sicurezza nei luoghi di lavoro (art. 2087 c.c. e d.lgs. n. 81/2008).

La *ratio* prevenzionistica accomuna le due normative (Gdpr e d.lgs. n. 81/2008) e ad un tempo ne giustifica l'accostamento giacché ambedue le regolamentazioni hanno ad oggetto la tutela della persona nell'ambiente di lavoro sebbene sotto due aspetti differenti: il Gdpr per la protezione dei dati, il d.lgs. n. 81/2008 per la protezione della salute fisica e psichica.

Se di parallelismo[22] si può parlare, questo attiene, infatti, come si è detto a suo tempo, alla filosofia di fondo che contraddistingue i due corpi normativi, sebbene la regolamentazione sulla protezione dei dati privilegia un approccio di tipo individualistico e non collettivo come prevede invece il testo italiano sulla sicurezza, nonostante «anche l'art. 21 della Raccomandazione del Comitato dei Ministri del Consiglio d'Europa R(2015)5 del 1 aprile 2015 – in attuazione dell'art. 8 CEDU – valorizza i principi di informazione e consultazione in questa materia»[23].

Questa sorta di parallelismo – dall'angolazione che si è scelto di privilegiare – fa intravedere la possibilità di estendere il modello della prevenzione partecipata sulla sicurezza nei luoghi di lavoro alla prevenzione del rischio *privacy,* il che significa, anzitutto, promuovere in ambito sindacale[24] la diffusione della cultura della *privacy* nel rapporto di lavoro, nell'ottica di favorire lo sviluppo di una dimensione partecipata della tutela *ex ante* del rischio *privacy* (v. *infra*, par. 4).

La tutela *ex ante*, in particolare, consiste nella previsione di misure finalizzate a evitare la produzione del rischio[25] riducendo la possibilità del suo verificarsi direttamente alla fonte.

---

[21] Esso è richiamato anche in più di una disposizione dell'AI Act. Si vedano le disposizioni del Titolo III, Capo 2, della proposta di regolamento sull'IA, in particolare gli artt. da 8 a 15, rimasti pressoché invariati a seguito dell'intervento della Legge sull'IA, che riguardano l'individuazione di precise misure di prevenzione per la fase di progettazione e realizzazione dei sistemi di IA ad alto rischio (nel testo il rischio è suddiviso in quattro differenti categorie: inaccettabile, alto, limitato, minimo), nonché l'emendamento all'art. 14, par. 1, della Legge sull'IA, che sottolinea che la supervisione umana deve essere «proporzionale ai rischi associati a tali sistemi».

[22] A. INGRAO, *Manuale operativo per la protezione dei dati personali dei lavoratori,* cit., p. 20. Su questo specifico aspetto mi sia consentito rinviare anche al mio, *I controlli a distanza dopo il Jobs act. Dallo Statuto dei lavoratori alla disciplina sulla protezione dei dati personali*, in "Massimario di giurisprudenza sul lavoro", 2016, 10, p. 645.

[23] A. INGRAO, *Manuale operativo per la protezione dei dati personali dei lavoratori*, cit., p. 67 ss. Su tale aspetto, che esula dai nostri ristretti confini d'indagine, per tutti, si rinvia ai contributi pubblicati in U. GARGIULO, P. SARACINI (a cura di), *Parti sociali e innovazione tecnologica*, "Quaderni Diritti lavori Mercati", n. 15/2023.

[24] In tal senso, da ultimo su questo profilo, v. U. GARGIULO, *Intelligenza Artificiale e poteri datoriali*, cit., p. 22. Ampiamente, sul ruolo dell'autonomia collettiva, in specie aziendale, nell'attuale panorama del lavoro digitalizzato, anche L. IMBERTI, *La contrattazione collettiva aziendale di fronte alle sfide della rivoluzione digitale e ai processi di cambiamento organizzativo*, in "federalismi.it", n. 25/2022.

[25] A. SANTOSUOSSO, *Scienza e tecnologia, se il criterio è il "rischio": problemi e condizioni*, in "Agendadigitale.eu", 17 dicembre 2021, consultabile al link *https://www.agendadigitale.eu/cultura-digitale/scienza-tecnologia-e-societa-problemi-e-condizioni-del-rischio-come-criterio/*.

Si parla, in tal senso, di carattere «primario» della prevenzione[26], che costituisce il paradigma del d.lgs. n. 81/2008, e che nella protezione dei dati analogamente obbliga il datore di lavoro, quale titolare del trattamento dei dati del lavoratore, ad intervenire sull'insorgenza del rischio, nel momento dell'organizzazione del lavoro, attraverso l'adozione di alcune misure generali di cd. *accountability*[27].

Il principio di *accountability* nel contesto della *data protection* è considerato, insieme alla prevenzione, il secondo pilastro del Gdpr e viene interpretato, secondo il linguaggio adoperato dal legislatore unionale, come criterio generale di responsabilizzazione.

Esso viene inteso come dovere di "dare conto di", nel senso che il titolare del trattamento deve dimostrare di aver adottato tutte le misure necessarie e opportune, in conformità a quanto previsto dal Gdpr.

In tal senso, l'*accountability* promuove un decisionismo responsabile proponendosi come uno strumento di algoretica finalizzato a coniugare legalità e tecnologia.

In realtà, il principio di *accountability* non rappresenta una novità introdotta dal Gdpr. Nell'ambito della *data protection* esso risale al 1980, alle OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data che richiamavano lo Accountability Principle secondo cui «A data controllere should be accountable for complying with measures which give effect to the principles stated above» e da allora è stato in più occasioni ripreso dai vari documenti europei che si sono succeduti nella materia[28] anche in relazione al particolare profilo del trasferimento dei dati all'estero[29].

L'*accountability* coinvolge aspetti quali l'affidabilità e la competenza aziendale nella gestione dei dati personali e la sua declinazione nell'ambito del Gdpr può

[26] Sul concetto di prevenzione come "prevenzione dei rischi alla fonte" e come "protezione dal danno conseguente ad un rischio programmato", si veda P. PASCUCCI, *Infortunio sul lavoro, tra prevenzione, protezione, organizzazione ed effettività*, in G. CANAVESI, E. ALES, (a cura di), *La tutela antinfortunistica oggi. Seminari Previdenziali Maceratesi – 2019*, Editoriale scientifica, Napoli, 2021, p. 55 ss. Ampiamente, sul tema, S. BUOSO, *Principio di prevenzione e sicurezza sul lavoro*, Giappichelli, Torino, 2020.

[27] Sul tema si veda G. FINOCCHIARO, *Il principio di* accountability, in "Giurisprudenza italiana" 2019, p. 2278 ss.; più ampiamente, A. SARTORI, *Il controllo tecnologico sui lavoratori. La nuova disciplina italiana tra vincoli sovranazionali e modelli comparati*, Giappichelli, Torino, 2020.

[28] G. COMANDÈ, *Intelligenza artificiale e responsabilità tra liability e accountability. Il carattere trasformativo dell'IA e il problema della responsabilità*, cit., p. 186 e ivi anche nota 42. Per il rilievo pubblicistico del principio di *accountability* nell'ambito della trasparenza e anticorruzione della pubblica amministrazione che proprio negli anni '80 nacque per rispondere alla necessità da parte dei governi di rendere conto delle azioni pubbliche nei riguardi dei cittadini.

[29] Si pensi, ad esempio, all'adozione dei Codici aziendali obbligatori (Binding Corporate Rules - BCRs). Le organizzazioni sarebbero tenute a dimostrare, con l'adozione di suddetti codici, di aver adottato ogni misura idonea a rispettare i parametri prestabiliti dall'autorità ogni volta che si impegnano in attività rischiose come il trasferimento di dati al di fuori dell'Eurozona. Allorché le aziende siano munite dei BCRs, sarebbero, inoltre, esentate dal dovere di comprovare la documentazione presso gli organi di controllo, beneficiando in tal modo di maggiore flessibilità. Ampiamente, in tema di *accountability*, v. G. FINOCCHIARO, *Il principio di* accountability, cit., p. 2278 ss.; A. SARTORI, *Il controllo tecnologia sui lavoratori*, cit., p. 39 ss.

essere colta, in particolare, negli articoli 24, 25, 35 del Gdpr in tema di valutazione d'impatto dei rischi *privacy* (di cui si dirà nel prossimo paragrafo).

3.2. *Conoscibilità, non esclusività, non discriminazione*[30]

Per quanto riguarda gli altri tre criteri di trasparenza algoritmica, su quello di *conoscibilità*, si è pronunciato il Consiglio di Stato con la sentenza n. 2270 del'8 aprile 2019, nella quale ha affermato il principio generale secondo cui la regola algoritmica non può lasciare margini di discrezionalità – non avendo l'elaboratore informatico capacità discrezionale – e che la discrezionalità amministrativa «senz'altro non può essere demandata al software».

Di particolare rilievo è il riconoscimento dell'importanza, in sede decisoria pubblica, di almeno due garanzie minime che devono sempre essere rispettate: la piena conoscibilità dell'algoritmo e dei criteri applicati per il suo funzionamento; l'imputabilità della decisione all'organo titolare del potere, il quale avrà anche il dovere di verificare la logicità e legittimità della decisione algoritmica.

Sulla necessità che l'algoritmo sia conoscibile[31], sempre il Consiglio di Stato ha sostenuto che «Tale conoscibilità dell'algoritmo deve essere garantita in tutti gli aspetti: dai suoi autori al procedimento usato per la sua elaborazione, al meccanismo di decisione, comprensivo delle priorità assegnate nella procedura valutativa e decisionale e dei dati selezionati come rilevanti», specificando che «non può assumere rilievo l'invocata riservatezza delle imprese produttrici dei meccanismi informatici utilizzati i quali, ponendo al servizio del potere autoritativo tali strumenti, all'evidenza ne accettano le relative conseguenze in termini di necessaria trasparenza» (Cons. Stato, sent. del 4 febbraio 2020, n. 881, punto 10)[32].

In relazione a questo ultimo aspetto va evidenziato, peraltro, che la formazione di algoritmi è rimessa a società e *start-up* private, per cui potrebbero

[30] Sul tema si veda G. MARCHIANÒ, *La legalità algoritmica nella giurisprudenza amministrativa,* in "Il diritto dell'economia", 2020, 3, pp. 229-258; G. PESCE, *Il giudice amministrativo e la decisione automatizzata. Quando l'algortimo è opaco*, in "judicium.it".

[31] Sul problema della conoscibilità algoritmica nel rapporto di lavoro, cfr., senza pretesa di esaustività, in generale: R. COVELLI, *Lavoro e intelligenza artificiale: dai principi di trasparenza algoritmica al diritto alla conoscibilità*, in "Labour & Law Issues", 2023, 9(1); M. MARAZZA – F. D'AVERSA, *Dialoghi sulla fattispecie dei "sistemi decisionali o di monitoraggio automatizzati" nel rapporto di lavoro (a partire dal Decreto Trasparenza)*, in "Giustiziacivile.com", 2022; A. TOPO, Circolazione di informazioni, dati personali, profilazione e reputazione del lavoratore, in C. PISANI, G. PROIA, A. TOPO, *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Giuffrè, Milano, 2022, spec. p. 406; C. SPINELLI, *La trasparenza delle decisioni algoritmiche nella proposta di Direttiva UE sul lavoro tramite piattaforma*, in "Lavoro Diritti Europa", 2022, 2; M.P. AIMO, *Dalle schedature dei lavoratori alla profilazione tramite algoritmi: serve ancora l'art. 8 dello Statuto dei lavoratori?*, in "Lavoro e Diritto", 2021, 3-4, Nonché, per una prospettiva più ampia: G. RESTA, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in "Politica del diritto", 2019, 2. Sul problema della trasparenza, nella giurisprudenza di merito, cfr. Trib. Palermo, 31 marzo 2023, Trib. Palermo, 20 giugno 2023, Trib. Torino, 5 agosto 2023, che hanno dichiarato antisindacale, *ex* art. 28 St. lav., il comportamento delle società per non aver fornito le informazioni previste dal decreto trasparenza.

[32] Nello stesso senso il Consiglio di Stato si è pronunciato anche successivamente con le sentenze nn. 5117 del 23 maggio 2023; 6236 del 8 settembre 2021; 1206 del 9 febbraio 2021.

sorgere problemi relativi a diritti di proprietà intellettuale e industriale, dai quali potrebbe conseguire l'impossibilità di accedere ai procedimenti di formazione dell'algoritmo con il pericolo che la decisione amministrativa venga devoluta alla sensibilità e alla competenza di società *legal tech* private esperte nella raccolta di grandi quantità di dati e il cui obiettivo difficilmente sarebbe quello di garantire imparzialità e trasparenza nel processo decisionale[33].

Dunque, il principio di conoscibilità attiene al diritto di ciascuno *sia* di conoscere l'esistenza di processi automatizzati nei suoi confronti *sia* di ottenere le informazioni sulla logica utilizzata nel procedimento. Esso costituisce diretta applicazione dell'art. 42 della Carta Europea dei diritti fondamentali, in specie nella parte in cui afferma che quando la pubblica amministrazione intende adottare una decisione che può avere effetti avversi su di una persona, essa ha l'obbligo di sentirla prima di agire, di consentirle l'accesso ai suoi archivi e documenti, e infine ha l'obbligo di motivare le ragioni della propria decisione.

Il principio di conoscibilità trova attuazione nel Gdpr, in particolare nell'art. 22 che stabilisce il divieto di decisioni completamente automatizzate, disposizione, quest'ultima, dalla quale deriva anche il principio di *non esclusività*, in base al quale – sostengono i giudici amministrativi nella menzionata pronuncia n. 881/2020 – la decisione algoritmica non deve prescindere dal controllo umano (*human in the loop*)[34]. Entrambi i principi risentono della «visione antropocentrica» della IA richiamata dalla Commissione UE nella Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni dell'aprile 2019 e dei rilievi etici in essa illustrati a garanzia di un funzionamento dell'algoritmo «affidabile», che prevede il ricorrere dei seguenti sette requisiti fondamentali: intervento e sorveglianza umana, robustezza tecnica e sicurezza, riservatezza e *governance* dei dati, trasparenza, diversità, non discriminazione ed equità, benessere sociale e ambientale, *accountability*[35].

Strettamente collegato ai primi due è anche il principio di *non discriminazione*[36], che viene richiamato dai giudici di Palazzo Spada in relazione al considerando n.

[33] F. PATRONI-GRIFFI, *La decisione robotica e il giudice amministrativo*, in "giustizia-amministratva.it", 2018.

[34] Sul profilo della sorveglianza umana, nelle relazioni di lavoro, si rinvia ai contributi di L. ZAPPALÀ, *Appunti su linguaggio, complessità e comprensibilità del lavoro 4.0: verso una nuova procedimentalizzazione dei poteri datoriali*, in "WP CSDLE "Massimo D'Antona". IT", n. 462/2022, spec. p. 23 ss., e *Informatizzazione dei processi decisionali e diritto del lavoro: algoritmi, poteri datoriali e responsabilità del prestatore nell'era dell'intelligenza artificiale*, in "WP CSDLE "Massimo D'Antona". IT", n. 446/2021, spec. pp. 12 ss.

[35] L. FLORIDI, *The Fourth Revolution, How the Infosphere is Reshaping Human Reality*, Oxford University Press, 2014; U. PAGALLO, *Il diritto nell'età dell'informazione*, Giappichelli, Torino, 2014; J. KAPLAN, *Artificial Intelligence*, Oxford University Press, 2017 (trad. it. ed. Luiss, 2017).

[36] Il tema delle conseguenze discriminatorie derivanti dall'algoritmo del lavoro è molto ampio e come si è già detto in precedenza (v. *supra,* par. 3.1.), anche l'approfondimento dei suddetti aspetti esula dai ristretti confini del presente lavoro. Pertanto, sul punto, si rinvia a: M. BARBERA, *Discriminazioni algoritmiche e forme di discriminazione*, in "Labour & Law Issues", 2021, vol. 7, 1.; A. PERULLI, *La discriminazione algoritmica: brevi note introduttive a margine dell'ordinanza del Tribunale di Bologna*, in "Lavoro Diritti Europa", 2021, 1, p. 1 ss.; M.V. BALLESTRERO, *Ancora sui rider. La cecità discriminatoria della piattaforma*, in "Labor", 2021, 1, p. 104; da ultimo, C. FALERI, *Management algoritmico e asimmetrie informative di ultima generazione*, in "federalismi.it", n. 3/2024. In giurisprudenza

71 del Gdpr, che richiede al titolare del trattamento l'utilizzo di procedure matematiche o statistiche appropriate per la profilazione, al fine di garantire che possano essere rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori che potrebbero causare effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale[37].

Sul versante del rapporto di lavoro automatizzato, possiamo verificare che i criteri finora esaminati trovano applicazione attraverso interventi di raccordo normativo con la regolamentazione sui dati personali, a cominciare dal principio di *accountability* del titolare del trattamento, che, insieme a quello di prevenzione si declina nel generale obbligo, per il datore di lavoro, di adottare le misure necessarie e adeguate alle particolarità dell'organizzazione del lavoro allo scopo di rendere effettiva l'attuazione delle norme del Gdpr poste a tutela dei lavoratori quali soggetti eventualmente interessati da processi di automazione.

4. *La valutazione dei rischi per la salute e sicurezza come modello di riferimento per la prevenzione del rischio* privacy

Nello specifico, tale obbligo si attua prima di tutto nella redazione del documento di valutazione d'impatto (DPIA) (art. 35, paragrafo 1, Gdpr), che prevede una valutazione delle conseguenze negative sui diritti e le libertà fondamentali delle persone fisiche interessate da un trattamento di dati derivante dall'uso di nuove tecnologie.

In particolare, la valutazione d'impatto si rende obbligatoria per il datore di lavoro, ai sensi dell'art. 35, paragrafo 3, nei seguenti casi: se si tratta di un trattamento di dati svolto con modalità automatizzate (lett. *a*); se riguarda categorie particolari di dati (lett. *b*); in presenza di una videosorveglianza svolta in maniera sistematica che comprende spazi accessibili al pubblico (lett. *c*).

si segnalano le principali pronunce: Trib. Bologna, 31 dicembre 2020, in "Rivista italiana di diritto del lavoro", 2021, II, p. 175 ss., con nota di G. GAUDIO, *La CGIL fa breccia nel cuore dell'algoritmo di Deliveroo: è discriminatorio*, in "Diritto delle relazioni industriali", 2021, p. 204 ss., con nota di M. FAIOLI, *Discriminazioni digitali e tutela giudiziaria su iniziativa delle organizzazioni sindacali*, in "Argomenti di diritto del lavoro", 2021, p. 771 ss., con nota di M. BIASI, *L'algoritmo di Deliveroo sotto la lente del diritto antidiscriminatorio…e del relativo apparato rimediale*; Trib. Palermo, 17 novembre 2023.

[37] Sul problema della conoscibilità algoritmica, v. anche, senza pretesa di esaustività: R. COVELLI, *Lavoro e intelligenza artificiale: dai principi di trasparenza algoritmica al diritto alla conoscibilità*, cit.; M. MARAZZA – F. D'AVERSA, *Dialoghi sulla fattispecie dei "sistemi decisionali o di monitoraggio automatizzati" nel rapporto di lavoro*, cit.; A. TOPO, Circolazione di informazioni, dati personali, profilazione e reputazione del lavoratore, in C. PISANI, G. PROIA, A. TOPO, *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Giuffrè, Milano, 2022, spec. p. 406; C. SPINELLI, *La trasparenza delle decisioni algoritmiche nella proposta di Direttiva UE sul lavoro tramite piattaforma*, in "Lavoro Diritti Europa", 2022, 2; M.P. AIMO, *Dalle schedature dei lavoratori alla profilazione tramite algoritmi: serve ancora l'art. 8 dello Statuto dei lavoratori?*, in "Lavoro e Diritto", 2021, 3-4. Nonché, per una prospettiva più ampia: G. RESTA, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, cit., p. 2 ss.

In verità, anche se il legislatore unionale non precisa in maniera esplicita se tali condizioni devono ricorrere contestualmente ai fini dell'obbligo del DPIA o se deve ritenersi sufficiente anche una sola di esse, ci sembra di poter optare per questa seconda soluzione in considerazione della incidenza sulle libertà fondamentali e sui diritti dei lavoratori.

Possono consistere in trattamenti automatizzati che danno luogo ad effetti discriminatori, ad esempio, le attività di *recruiting* del personale attraverso la selezione di *curricula* o anche la raccolta di dati sanitari relativamente alle visite mediche periodiche svolte dal medico competente in azienda, compresa la conservazione e l'aggiornamento delle relative cartelle sanitarie. O anche, la profilazione dei lavoratori tramite il trattamento di dati attinenti ad aspetti comportamentali come le informazioni sul rendimento professionale rilevabili da modelli di profilazione con sistemi GPS e *wereable device* per agevolare i lavoratori durante l'esecuzione della prestazione, e ancora, le attività di timbratura degli ingressi e delle uscite dei dipendenti attraverso la sorveglianza di spazi eventualmente esposti al pubblico che determina la raccolta di una mole indiscriminata di informazioni.

Relativamente alle ipotesi di lavoro automatizzato anche l'Autorità Garante per la *privacy* ha precisato che il documento d'impatto è obbligatorio in presenza di «trattamenti nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti» (Provvedimento 11 ottobre 2018, n. 467).

In particolare, il DPIA deve indicare anzitutto le tipologie di strumenti utilizzati per la raccolta dei dati dei lavoratori, le relative caratteristiche, nonché le finalità che intende perseguire e la *ratio* del trattamento ovvero deve specificare qual è l'interesse legittimo del datore di lavoro (nuove assunzioni, tutela del patrimonio aziendale, aumento della produttività, salute e sicurezza dei lavoratori) (art. 35, paragrafo 7, lett. *a)*, Gdpr); deve altresì motivare la necessità del trattamento e la sua proporzionalità rispetto agli scopi da perseguire (lett. *b)*, individuando i rischi possibili di lesione del diritto alla protezione dei dati dei lavoratori (lett. *c)*, e le misure che intende predisporre per evitare o ridurre il rischio d' impatto negativo (lett. *d)*.

Sotto il profilo procedurale la valutazione d'impatto di cui all'art. 35 Gdpr sembra, in parte, simile alla valutazione dei rischi contemplata dal d.lgs. n. 81/2008 (artt. 28 e 29), ma se ne differenzia sul piano dei soggetti che vi partecipano.

La valutazione dei rischi (DVR) si basa sul coinvolgimento dei vari attori della sicurezza: dal responsabile del servizio di prevenzione e protezione, al/ai rappresentante/i della sicurezza, al medico competente, che collaborano, ciascuno per la parte di propria competenza alla stesura del relativo documento (art. 29, comma 1, del d.lgs. n. 81/2008).

La valutazione d'impatto (DPIA) è svolta invece dal titolare del trattamento che «si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno» (art. 35, par. 2, Gdpr).

Tuttavia, al successivo paragrafo 9, si legge «Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto», di tal che si intende che è mera facoltà del titolare avviare una «consultazione» sulle misure da intraprendere, con gli interessati o i loro rappresentanti.

Questa disposizione può essere letta, ai nostri fini, congiuntamente con l'art. 88 Gdpr, paragrafo 1, quando afferma che gli Stati membri «possono prevedere, con legge o tramite contratti collettivi disposizioni più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro», se non altro nella prospettiva di ribadire il ruolo di centralità che potrebbe avere il fenomeno sindacale nella *data protection*, sul presupposto che la previsione di un modello di prevenzione del rischio *privacy* partecipata[38] consentirebbe una condivisione democratica della tutela dei lavoratori sul piano della garanzia di integrità dei propri diritti fondamentali (v. *supra*, par. 3.1.).

Nel proseguire la nostra indagine, ma volendo cedere a qualche ulteriore suggestione interpretativa, potremmo pensare di considerare come modello per la prevenzione partecipata del rischio *privacy* il sistema della sicurezza e salute dei lavoratori delineato nel d.lgs. n. 81/2008.

Esemplificando, al datore di lavoro, in qualità di titolare del trattamento dei dati dei lavoratori, spetterebbe il compito di redigere un "documento di valutazione del rischio *privacy* (DVRP)" analogamente a quanto stabilito in materia di sicurezza sul lavoro sulla redazione del documento di valutazione dei rischi (DVR) (art. 28 del d.lgs. n. 81/2008).

In esso andrebbero indicate anzitutto le generali misure tecniche e organizzative valutate dal datore di lavoro come «adeguate» a «dimostrare che il trattamento è effettuato conformemente al Regolamento» (art. 24 Gdpr), nonché le misure volte ad assicurare la protezione dei dati fin dalla progettazione e per impostazione predefinita (art. 25 Gdpr), che consiste nell'obbligo di indicare le tipologie delle misure da adottare (pseudonomizzazione, minimizzazione dei dati) finalizzate a garantire la concreta attuazione dei principi generali di legittimità del trattamento di cui all'art. 5 Gdpr.

In tale documento di valutazione dei rischi andrebbe prevista, inoltre, l'indicazione del soggetto responsabile della protezione dei dati (DPO) (art. 37 Gdpr), che deve essere individuato "in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa in materia di protezione dei dati (…)" oltre che della capacità di assolvere i compiti specificati al successivo art. 39 del regolamento.

[38] A. INGRAO, *Manuale operativo per la protezione dei dati personali dei lavoratori*, cit. pp. 68-72.

Quanto alla partecipazione sindacale nel sistema di protezione dei dati, tenendo presente la figura del/i rappresentante/i per la sicurezza (artt. 47 ss. del d.lgs. n. 81/2008), si potrebbe immaginare un meccanismo analogo per la individuazione del/i rappresentante/i dei lavoratori per la *privacy* (RLP).

Con riguardo alla valutazione d'impatto di cui all'art. 35 Gdpr, anch'essa potrebbe confluire nel documento dei rischi (DVRP) oppure, in considerazione della complessità di tale obbligo che viene imposto essenzialmente nelle ipotesi di trattamenti automatizzati di dati che generano la profilazione dei soggetti interessati, il relativo documento, volendo, potrebbe costituire un *addendum* della valutazione dei rischi (DVRP).

Quanto, infine, all'adempimento dell'obbligo *by design by default,* questo può essere certificato, in alternativa, dall'autorità di controllo o da specifici organismi accreditati (art. 42 Gdpr), come avviene anche per l'obbligo generale di garantire l'adeguatezza delle misure adottate, il cui adempimento può essere attestato dall'adesione a codici di condotta aziendali (art. 40 Gdpr).

L'obiezione che si può sollevare ad un tale modello di valutazione partecipata del rischio *privacy* è che, così facendo, si rischia di procedimentalizzare in modo eccessivo l'esercizio del potere datoriale. Tuttavia, si può affermare che il potere del datore di lavoro è già procedimentalizzato nello Statuto dei lavoratori, con particolare riferimento ai controlli a distanza (art. 4) e agli accertamenti sanitari (art. 5), attraverso un gioco di rinvii normativi con il Codice (artt. 113, 114).

In tale cornice, la regolamentazione europea sui dati personali interviene, da un lato, con disposizioni procedimentali finalizzate a rendere operativi gli obblighi a carico del titolare del trattamento, nel nostro caso, del datore di lavoro; da un altro lato, essa attribuisce – forse non del tutto casualmente – agli Stati membri la facoltà di prevedere attraverso leggi o contratti collettivi norme più specifiche con riferimento all'ambito dei rapporti di lavoro (art. 88 Gdpr).

Per quel che riguarda, poi, la veste giuridica che potrebbe avere un impianto di tutele basato sulla valutazione del rischio *privacy* come quello che si è appena rappresentato, si potrebbe propendere per un intervento legislativo a livello nazionale di riordino della sicurezza dei dati personali nel rapporto di lavoro, verosimilmente da realizzare nell'immediatezza di futuri interventi di sistemazione del quadro normativo europeo di riferimento.

5. *Una osservazione conclusiva*

Si chiude il cerchio di questa riflessione osservando che: mentre nel campo delle scienze umane e sociali si discute di algoretica, mentre la tecnologia prosegue impavida e mentre le istituzioni europee lavorano alacremente sulla (e per) la legalità algoritmica[39], alcune imprese di intelligenza artificiale si cimentano nella

[39] Cfr., *supra*, nota 19.

costruzione di modelli di sicurezza dei dati. La *startup* britannica DeepMind[40], ad esempio, ha approvato un modello di costituzione robotica ispirandosi alle tre leggi di Isaac Asimov[41] (un robot: 1. non può recare danno agli esseri umani, né può permettere che, a causa del suo mancato intervento, gli esseri umani ricevano danno; 2. deve obbedire agli ordini impartiti dagli esseri umani, tranne nel caso che tali ordini contrastino con la Prima Legge; 3. deve salvaguardare la propria esistenza, purché ciò non contrasti con la Prima e la Seconda Legge) e i robot che sono stati prodotti sono addestrati per comprendere l'ambente circostante e affrontare eventuali compiti organizzativi[42].

Questo significa che la sostituzione della macchina all'uomo è già attuata. Del resto, se si guarda alle discipline sportive (calcio, tennis, rugby, football, pallacanestro, pallavolo, ecc.), già oggi il giudizio dell'arbitro umano è subordinato all'utilizzo di supporti tecnologici e, d'altra parte, la stessa cosa si può dire con riferimento al campo sanitario e della giustizia[43].

Il problema, quindi, non è la tecnologia in sé, ma come questa viene impiegata dall'uomo: la scelta di affidare a sistemi intelligenti alcune attività è frutto del libero arbitrio dell'uomo che ha il compito di comprendere e decidere come utilizzarla[44]. Perciò, non è importante – almeno non solo – chiedersi che cosa ne sarà del mondo nei prossimi decenni, piuttosto, è importante adoperarci per capire come è meglio che la tecnologia funzioni *con* e *per* l'uomo[45], avendo contezza che il dato personale "grazie" alla trasformazione tecnologica è diventato ciò che identifica la persona: nel rapporto di lavoro è quell'informazione che costruisce l'identità del lavoratore.

[40] Si tratta della nuova divisione AI di Google nata dalla fusione con Google Brain, costituita da un gruppo di ricercatori e ingegneri che dal 2017 lavorano sulla creazione di modelli di intelligenza artificiale generativa.

[41] Le tre leggi della robotica sono state formulate dal biochimico e scrittore sovietico (naturalizzato statunitense) Isaac Asimov nel 1942, nello stesso racconto in cui appare per la prima volta la parola "robotica" (*Runaround*, incluso nella raccolta *Io, Robot*, pubblicata inizialmente nel 1950 (ora: *Io, Robot,* Mondadori, 2021 con traduzione di V. Latronico).

[42] I robot realizzati da DeepMind sfruttano modelli di intelligenza artificiale di grandi dimensioni integrando due modalità algoritmiche: un modello di linguaggio visivo (VLM) e un modello di linguaggio di grandi dimensioni (LLM) che agisce come decisore, selezionando un compito adeguato che il robot può eseguire.

[43] M. LUCIANI, *La decisione giudiziaria robotica*, in A. CARLEO, *Decisione robotica*, Il Mulino, Bologna, 2019, p. 63 ss.

[44] Con riferimento al rapporto tra decisione giudiziaria e intelligenza artificiale, v. M. DELL'UTRI, *Giudizio umano, giudizio artificiale*, in "giustiziainsieme.it" del 23 gennaio 2024 «Il futuro dei rapporti tra l'uomo (e dunque il giudice) e l'intelligenza artificiale non è affidato allo sviluppo di quest'ultima (ai cui percorsi, occorre ribadire, non è sensatamente consentito associare immagini fantasiose, o inquietanti vaneggiamenti), quanto alla responsabilità di ciascuno, a cui, con sempre maggiore urgenza, è richiesto di coltivare in modo continuativo la qualità dei propri saperi (…)».

[45] Per le implicazioni etiche, senza pretesa di esaustività, ultimamente, v. D. LAMBERT, *Robotica e intelligenza artificiale*, Queriniana, Brescia, 2023; A. PATRONI GRIFFI (a cura di), *Bioetica, diritti e intelligenza artificiale*, Mimesis Quaderni di Bioetica, Milano, 2023.

Abstract

L'introduzione nell'ambiente di lavoro delle nuove tecnologie di automazione digitalizzata e/o robotica (anche basate sull'intelligenza artificiale) pone l'esigenza di applicare le disposizioni previste dal Regolamento europeo 2016/679 in materia di tutela dei dati personali. In assenza di una cornice nazionale di riferimento per la protezione e sicurezza dei dati nel rapporto di lavoro, questa indagine propone di adottare la normativa sulla sicurezza del lavoro come modello di riferimento per la valutazione del rischio privacy.

The introduction of new digitalised automation and/or robotic technologies (also based on artificial intelligence) into the working environment poses the need to apply the provisions of the European Regulation 2016/679 regarding the protection of personal data. In the absence of a national refernce framework for data protection and security in the employment relationship this investigation proposes to adopt workplace safety legislation as a reference model for assessing privacy risk.

Parole chiave

Dati personali, Sicurezza, Prevenzione, Valutazione, Rischio privacy, Documento (DVRP)

Keywords

Personal data, Safety, Prevention, Assessment, Privacy risk, Document (DVRP)