



FOCUS LAVORO, PERSONA, TECNOLOGIA
17 DICEMBRE 2025

Circolazione vs protezione dei dati
personali e autodeterminazione
informativa tra GDPR, DGA e AI Act
per una nuova stagione delle politiche
attive del lavoro

di Silvia Ciucciovino

Professoressa ordinaria di Diritto del lavoro
Università degli Studi di Roma Tre

Circolazione vs protezione dei dati personali e autodeterminazione informativa tra GDPR, DGA e AI Act per una nuova stagione delle politiche attive del lavoro*

di Silvia Ciucciovino

Professoressa ordinaria di Diritto del lavoro
Università degli Studi di Roma Tre

Abstract [It]: Il contributo analizza l'evoluzione delle politiche attive del lavoro in Italia, focalizzandosi sul ruolo della digitalizzazione, interoperabilità e portabilità dei dati personali nel mercato del lavoro. Viene approfondito il rapporto tra la necessità di condivisione e circolazione dei dati per l'efficienza delle PAL e la tutela della privacy, esaminando inoltre l'impatto dell'intelligenza artificiale e delle nuove normative europee e italiane sul trattamento dei dati personali nei sistemi di IA applicati alle PAL. L'Autrice propone una riflessione sulle prospettive di governance multi-authority e sulle tecniche di trattamento dei dati per garantire autodeterminazione informativa e cittadinanza digitale, suggerendo il rafforzamento di forme collettive di tutela degli interessi nel mercato del lavoro digitale.

Title: Circulation vs. protection of personal data and informational self-determination under the GDPR, DGA, and Ai Act: towards a new era of active labour market policies

Abstract [En]: The paper analyses the evolution of labour market policies in Italy, focusing on the role of digitalisation, interoperability and portability of personal data in the labour market. It explores the relationship between the need for data sharing and circulation for the efficiency of labour policies and the protection of privacy, also examining the impact of artificial intelligence and new European and Italian regulations on the processing of personal data in AI systems applied to labour policies. The Author offers a reflection on multi-authority governance perspectives and data processing techniques to ensure informational self-determination and digital citizenship, suggesting the strengthening of collective forms of protection of interests in the digital labour market.

Parole chiave: politiche attive del lavoro, digitalizzazione, privacy, autodeterminazione informativa, tutele collettive

Keywords: labour policies, digitalisation, privacy, informational self-determination, collective forms of protection

Sommario: **1.** Digitalizzazione, interoperabilità, portabilità dei dati della persona nel mercato del lavoro: i tre pilastri del d. lgs. 150/2015. **1.1.** La collaborazione informativa 10 anni dopo: il SIISL e il “fascicolo sociale e lavorativo del cittadino”. **2.** La tensione dialettica tra condivisione informativa, circolazione e protezione dei dati personali nelle politiche attive del lavoro ancora alla ricerca di un (difficile) equilibrio tra GDPR e DGA. **3.** IA e mercato del lavoro: l'impostazione dell'EU AI Act e della l. 132/2025 a confronto. **4.** I tratti di specialità della disciplina del trattamento dei dati personali nei sistemi di IA e i possibili risvolti per le politiche attive del lavoro. **5.** Nuove prospettive di bilanciamento degli interessi in gioco nel sistema multi-Authority della IA. **6.** Conclusioni.

*Articolo sottoposto a referaggio. Il presente contributo è destinato al volume “*Mercato del lavoro, politiche attive e formazione nella doppia transizione*” a cura di A. ALAIMO, L. CORAZZA, V. SPEZIALE, L. TEBANO, di prossima pubblicazione per la Collana di Diritto del Lavoro di Franco Angeli.

1. Digitalizzazione, interoperabilità, portabilità dei dati della persona nel mercato del lavoro: i tre pilastri del d. lgs. 150/2015

Il ridisegno organico - in parte (ancora) inattuato, in parte fallito - delle politiche attive del lavoro che il d. lgs. 14 settembre 2015 n. 150 si proponeva di realizzare, poggiava le sue fondamenta in larga misura sulla collaborazione informativa digitalizzata dei diversi enti, istituzioni e attori che, a vario titolo, detengono dati rilevanti per le politiche attive del lavoro e i servizi per il lavoro. La digitalizzazione, l'interoperabilità delle banche dati e la portabilità dei dati della persona nel mercato del lavoro rappresentano i tre pilastri del ridisegno della governance e della filosofia di fondo delle politiche attive del lavoro (PAL) che il legislatore nel 2015 si era proposto di realizzare. La messa in rete e lo scambio informativo tra i diversi soggetti pubblici e privati¹ investiti della responsabilità delle politiche del lavoro, era vista come essenziale e funzionale a promuovere “l'effettività dei diritti al lavoro, alla formazione ed all'elevazione professionale previsti dagli articoli 1, 4, 35 e 37 della Costituzione ed il diritto di ogni individuo ad accedere a servizi di collocamento gratuito, di cui all'articolo 29 della Carta dei diritti fondamentali dell'Unione europea” (art. 1, d. lgs. 150/2015). In questo quadro la *collaborazione informativa digitale* riveste un ruolo strategico e costituzionalmente rilevante, anche ai fini della libera circolazione delle persone², all'interno di un sistema in cui la digitalizzazione rappresenta ormai una necessità irrinunciabile della *governance* delle politiche del lavoro nella società digitale³. Ma anche uno strumento indispensabile di realizzazione della cittadinanza attiva delle persone⁴ e di corretta rappresentazione della identità digitale personale⁵, tanto che si parla di diritto all'esistenza digitale “che condiziona e permette l'esercizio dei diritti individuali e sociali e incide sul rapporto con i pubblici poteri”⁶.

Come noto, gran parte dell'architettura istituzionale configurata dal d. lgs. n. 150 stenta ancora ad essere compiutamente attuata⁷, ma la visione sottostante, che interessa evidenziare ai fini del presente scritto, è

¹ Cfr. la Rete nazionale delle politiche del lavoro di cui alla art. 1, c. 2, d. lgs. 150/2015 come modificato dal d.lgs. n. 185 del 2016.

² Sul rilievo costituzionale ex artt. 4 e 120 Cost dello scambio informativo v. già l'art. 15 d. lgs. n. 276/2003 sulla Borsa continua del lavoro.

³ F. FAINI, *Data society. Governo dei dati e tutela dei diritti nell'era digitale*, Milano, 2019, *passim*

⁴ F. FAINI, *Diritto all'esistenza digitale*, in *BioLaw Journal, Rivista di BioDiritto*, 2019, n. 3, pp. 96 ss.; G. RESTA, *Identità personale e identità digitale*, in *Dir. Inf.*, 2007, pp. 511 ss.; G. RESTA, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Politica del diritto*, 2019, pp. 199 ss.; S. RODOTÀ, *Il diritto di avere diritti*, Laterza, Bari, 2012, p. 384.

⁵ G. PINO, *L'identità personale*, in S. RODOTÀ e P. ZATTI (diretto da), *Trattato di Biodiritto*, Giuffrè, Milano, 2010, pp. 297 ss.

; G. AZZARITI, *Stefano Rodotà e l'uso costituzionalmente orientato delle nuove tecnologie*, in *Costituzionalismo.it*, 2022, n. 2, pp. 1 ss.; L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina Editore, Milano, 2017; A. MORELLI, *Persona e identità personale*, in *BioLaw Journal, Rivista di BioDiritto, Special Issue*, 2019, n. 2, pp. 45 ss.

⁶ F. FAINI, *Diritto all'esistenza digitale*, *cit.*, p. 98.

⁷ P.A. VARESI, *Il sistema nazionale di servizi per l'impiego e politiche attive del lavoro: aspetti strutturali*, in *VTDL* 2022, n. 4, pp. 607 ss.; G. SCARANO, *Cosa significa innovare lì dove siamo più indietro: la digitalizzazione dei Centri per l'impiego*, in *E&L*, 2025, n. 2, pp. 93 ss.

chiara e fondata su tre pilastri strettamente interrelati tra loro: a) la visione sistemica, governata e digitalizzata dei servizi per il lavoro e delle PAL; b) la creazione di un sistema informativo unitario dei servizi per il lavoro grazie all'interoperabilità delle banche dati dei diversi soggetti pubblici che compongono la rete nazionale delle politiche del lavoro, lo scambio informativo e la connessa accessibilità reciproca delle banche dati (artt. 13, 14, 9⁸, 12⁹, 15); c) l'idea di ricomposizione sulla persona del lavoratore dei dati che lo riguardano e in possesso dei diversi enti, destinati ad alimentare il fascicolo elettronico del lavoratore (artt. 14 e 15).

In particolare la collaborazione informativa è declinata dal d. lgs. 150/2015 attraverso la realizzazione di un vero e proprio patrimonio informativo comune (*data lake*)¹⁰ basato sulla interoperabilità dei soggetti della rete (attraverso il “sistema informativo unitario delle politiche del lavoro”). La confluenza di questi dati è prevista per legge e quindi, in linea teorica, è obbligatoria e fonda un interesse legittimo delle persone all'efficiente implementazione degli scambi informativi di dati corretti e rilevanti per l'erogazione di politiche attive *data-driven* e per servizi effettivi ed efficaci.

Dovrebbero affluire al sistema informativo unitario, questa volta “sulla base di specifiche convenzioni” anche i dati contenuti in ulteriori sorgenti informative: le banche dati reddituale, catastali, le banche dati delle Anagrafi nazionali degli studenti e degli studenti universitari e dei laureati¹¹. Si prevede, inoltre, la diretta accessibilità dei dati delle Comunicazioni Obbligatorie raccolti dal Ministero del Lavoro, da parte di Regioni, INPS, INAIL e INL per le attività di rispettiva competenza¹². Nonché l'accessibilità ai dati da parte di altri soggetti interessati, ad esempio agenzie formative o gli stessi datori di lavoro, “allo scopo di certificare i percorsi formativi seguiti e le esperienze lavorative effettuate¹³. Inoltre, per fini di orientamento e monitoraggio degli esiti occupazionali dei giovani in uscita dai percorsi formativi e di

⁸ L'art. 9 c. 3, d. lgs. 150/2015 prevede che INPS “garantisce al Ministero del lavoro e delle politiche sociali, all'ANPAL e all'ISFOL (oggi INAPP) il pieno accesso ai dati contenuti nei propri archivi gestionali” per il monitoraggio e la valutazione delle politiche pubbliche di rispettiva competenza.

⁹ L'art. 12, c. 1 lett. c), d. lgs. 150/2015 prevede per i soggetti accreditati per i servizi al lavoro a livello regionale l'“obbligo di interconnessione con il sistema informativo di cui all'articolo 13 del presente decreto, nonché l'invio all'ANPAL di ogni informazione utile a garantire un efficace coordinamento della rete dei servizi per le politiche del lavoro”.

¹⁰ Il patrimonio informativo comune è costituito dal sistema informativo dei percettori di ammortizzatori sociali, dall'archivio informatizzato delle comunicazioni obbligatorie relative ai rapporti di lavoro, dai dati relativi alla gestione dei servizi per il lavoro e delle politiche attive del lavoro (incluse le schede anagrafiche e professionali dei lavoratori), dal sistema informativo della formazione professionale e dalla piattaforma informativa del reddito di cittadinanza (oggi da intendersi riferita al Sistema informativo per l'inclusione sociale e lavorativa- SIISL) (art. 13, c. 2), oltre che dai dati relativi alle schede anagrafico-professionali nella disponibilità delle regioni e delle province autonome di Trento e di Bolzano (art. 13, c. 2 bis, d. lgs.150/2015).

¹¹ Art. 13, c. 2 bis, d. lgs.150/2015.

¹² Art. 13, c. 4, d. lgs. 150/2015.

¹³ Art. 13, c. 5, d. lgs. 150/2015.

istruzione, si prevede una collaborazione informativa, da effettuarsi sulla base di apposita convenzione, tra Ministero del Lavoro, Ministero dell'Istruzione e del Merito e Ministero dell'Università e Ricerca¹⁴. Come noto, tale sistema a sua volta è destinato ad alimentare il “fascicolo elettronico del lavoratore”¹⁵, contenente le informazioni professionalmente rilevanti allo stesso riferite, quali: percorsi educativi e formativi, periodi lavorativi, versamenti contributivi, periodi di sospensione dal lavoro, fruizione di provvidenze pubbliche e/o ammortizzatori sociali (art. 14). Ciò implica che il patrimonio informativo non deve esaurirsi nello scambio informativo tra enti e non deve essere confinato all’arricchimento degli archivi pubblici, ma va *restituito* agli interessati, ai singoli cittadini, che quindi devono poter vedere ricostituite e unificate sulla loro persona le informazioni pertinenti che li riguardano, in quanto contribuiscono alla rappresentazione della identità digitale professionale, a cui ormai va riconosciuto un valore costituzionale¹⁶. Il d. lgs. 150 in definitiva rappresenta la fonte normativa che tutela il bene giuridico della ricomposizione della identità digitale professionale delle persone e conseguente riappropriazione da parte delle stesse del proprio capitale informativo digitalizzato, da cui dipende la tutela della stessa identità digitale professionale in un mondo interconnesso e digitalizzato, in cui si rischia la distorsione non soltanto informativa, ma identitaria della persona¹⁷.

La valenza sistematica e ideale del fascicolo è quindi dirompente, in quanto sta a segnare una svolta concettuale nella modalità consueta di trattamento dei dati presenti negli archivi pubblici, spesso frammentati, dispersi, difficilmente “consultabili” e di cui il singolo cittadino difficilmente riesce a rivendicare una titolarità, mentre è visto prevalentemente come un “interessato”, al di fuori però di una reale autodeterminazione informativa. Gli enti che raccolgono i dati sono preoccupati spesso più di custodirli in sicurezza (effetto *lock-in*)¹⁸, che non di ostenderli e condividerli per la consapevolezza e l’orientamento professionale dei singoli e per l’efficiente gestione e programmazione delle politiche da cui dipende il godimento dei diritti sociali.

¹⁴Art. 15, c. 6, d. lgs. 150/2015.

¹⁵ Il fascicolo sostituisce il libretto formativo del cittadino (già previsto dall’art. 2, c. 1, lett. i), d. lgs. 276/2003 e D.M. 10 ottobre 2005): cfr. art. 4, c. da 64 a 68, l. n. 92/2012 e d. lgs. n. 13/2013. S. CIUCCIOVINO, M. FAIOLI, A. TOSCANO, *Oltre il concetto di Blockchain: tecnica sociale di regolazione, fascicolo elettronico e nuovi diritti del lavoratore*. Editoriale, *Focus Blockchain, politiche pubbliche e regole*, in *Federalismi.It, Focus Lavoro persona tecnologia*, 2021, n. 2, pp. iv ss.

¹⁶ Cfr. retro nt. 4 e 5; S. CIUCCIOVINO, *Apprendimento e tutela del lavoro*, Giappichelli, Torino, 2013.

¹⁷ Basti qui il rinvio all’opera di S. RODOTÀ, *Il diritto di avere diritti*, cit., che, a fronte dei rischi di una società dove la tecnologia sta creando una diversa immagine dell’uomo creando un’identità frammentata “dispersa” e “inconoscibile”, avanza l’idea nuova di cittadinanza come patrimonio di diritti che accompagna la persona. A. TROJSI, *Il diritto del lavoratore alla protezione dei dati personali*, Giappichelli, Torino, 2013.

¹⁸ Cfr. G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in G. RESTA, V. ZENO ZENCOVICH (a cura di), *Governance of/through big data*, Vol. II, Roma Tre Press, 2023, p. 607, che menziona la “*posizione culturalmente e assiologicamente sovraordinata*” del compendio normativo concernente il trattamento dei dati personali, che “*ha retto per lungo tempo il sistema europeo di governo dei dati*” relegando in posizione minore altri segmenti di disciplina, “*come quello relativo all’accesso ai dati, al riutilizzo delle informazioni del settore pubblico, o alla stessa proprietà intellettuale*”. Parlano di “*GDPR Totem*” G. RESTA, V. ZENO ZENCOVICH, *Rise and Fall of Tracing Apps*, in G. RESTA, V. ZENO ZENCOVICH (a cura di), *Governance of/through big data*, cit., p. 635.

Si può dire, nel complesso, che la collaborazione informativa digitalizzata è mirata alla migliore personalizzazione, pianificazione, valutazione delle PAL e all'efficienza del mercato del lavoro, anche in vista del superamento del *mismatch* (art. 1, c. 3, d. lgs. 150/2015)¹⁹: tutte finalità di pubblico interesse²⁰, ancorché rimesse nell'attuazione a soggetti privati accreditati o autorizzati.

Dal punto di vista della normativa di protezione dei dati personali, il d. lgs. 150/2015 fornisce, ex art. 5.1 e 6.1 lett. e), GDPR, la base giuridica del trattamento²¹ e la coerenza rispetto al principio di finalità, della gestione del patrimonio informativo comune da parte di ciascuno dei soggetti partecipanti al sistema informativo unitario. Inoltre, poiché la raccolta e il trattamento dei dati per le PAL, avvengono per la soddisfazione di un interesse pubblico di rilevanza costituzionale, ricorrono i presupposti per la speciale disciplina che il GDPR detta quando il trattamento è finalizzato ai fini di “archiviazione nel pubblico interesse”. In questi casi è consentito derogare - con le dovute garanzie a tutela dei diritti e delle libertà dell'interessato - al divieto di trattamento dei dati particolari, nonché al principio di “limitazione delle finalità” (permettendo l'“ulteriore trattamento” non incompatibile con le finalità legittime iniziali²²) e al principio di “limitazione della conservazione”. Sulla compatibilità dello scambio informativo con la normativa sulla protezione dei dati personali, anche alla luce di altre fonti normative europee ispirate alla circolazione dei dati, si tornerà *funditus* nel §§ 2 e 4.

¹⁹ A. ALAIMO, R. DE MEO, *Politiche attive del lavoro e formazione nella doppia transizione: impresa, sindacato e contrattazione collettiva*, in *GIDLRI*, n. 4, 2025; S. CIUCCIOVINO, *Contrattazione collettiva e politiche attive del lavoro*, in *GDLRI*, 2021, n. 172, 4, p. 641; S. CIUCCIOVINO, *Trasformazioni tecnologiche e professionalità soggettiva nella prospettiva del mercato del lavoro*, in *RGL*, 2025, 2, pp. 202 ss.

²⁰ Le finalità di interesse pubblico sono individuate dal d. lgs. 150/2015: nella più agevole verifica e controllo del rispetto dei livelli essenziali delle prestazioni che devono essere garantiti su tutto il territorio nazionale e del monitoraggio delle politiche occupazionali e del lavoro da parte del Ministero del lavoro (art. 3); nel monitoraggio e valutazione delle politiche pubbliche di competenza di INAPP (art. 10, comma 3); nella gestione coordinata a livello amministrativo dei servizi per il lavoro e delle politiche attive del lavoro di competenza delle Regioni anche per garantire il rispetto dei livelli essenziali di prestazione e l'“efficace coordinamento della rete dei servizi per le politiche del lavoro” (artt. 11 e 12, c.1); nel monitoraggio e valutazione da parte del Ministero del lavoro sulla gestione delle politiche attive e i servizi per il lavoro nonché dei risultati conseguiti dai soggetti pubblici o privati accreditati a svolgere tali funzioni, al fine di una migliore programmazione e correzione delle politiche e delle strategie di intervento (art. 16), ma anche per fini di monitoraggio sulle politiche attive e passive del lavoro ai fini statistici (art. 14, c. 3).

²¹ A. TROJSI, *Trasparenza e 'base giuridica' secondo il GDPR: profili d'interesse (anche) giuslavoristico*, in *DML*, 2023, n. 3, pp. 639 ss.

²² L'art. 5.1 lett. b) GDPR prevede, a proposito del requisito di limitazione delle finalità, che i dati sono “raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»).

1.1. La collaborazione informativa 10 anni dopo: il SIISL e il “fascicolo sociale e lavorativo del cittadino”

Molti ostacoli politici e difficoltà tecnico-operative si sono frapposte alla realizzazione della cooperazione informativa digitalizzata immaginata dal d. lgs. 150/2015. L’ambiziosa riforma legislativa si è scontrata con resistenze degli attori coinvolti, con il decentramento regionale delle competenze, con preoccupazioni di *compliance* rispetto alla normativa *privacy* e con problemi oggettivi di funzionamento che ne hanno inibito a lungo il decollo. Il PNRR nell’ambito del Programma nazionale per la garanzia dell’occupabilità dei lavoratori (GOL) e del Piano nuove competenze, a sua volta ha rappresentato un’occasione non colta per l’implementazione di sistemi di scambio delle informazioni²³, infatti i riferimenti alla digitalizzazione del mercato del lavoro all’interno del PNRR sono pochi e scarni. E’ pur vero che parallelamente è stato avviato, su impulso del PNRR, l’ampio progetto di realizzazione della Piattaforma Digitale Nazionale Dati (PDND) per l’interoperabilità dei sistemi informativi delle pubbliche amministrazioni, anche in attuazione del principio del *once only*²⁴, all’interno della quale potrebbe forse nel prossimo futuro trovare nuova linfa e spinta propulsiva il sistema informativo per le politiche attive del lavoro.

Negli anni più recenti, d’altro canto, hanno preso corpo alcune infrastrutture e strumenti digitali che, pur non costituendo attuazione diretta delle disposizioni del d. lgs. 150, ne configurano omologhi funzionali, almeno a delimitati fini. Ci si riferisce innanzitutto al Sistema informativo per l’inclusione sociale e lavorativa – SIISL²⁵ - introdotto dal d.l. 4 maggio 2023, n. 48 conv. in l. 3 luglio 2023 n. 85, che ha concretizzato una prima forma di digitalizzazione e cooperazione informativa del mercato del lavoro quale piattaforma per gestire la condizionalità dei beneficiari dell’Assegno di inclusione (ADI) e del Supporto per la formazione e lavoro (SFL). Successivamente e più recentemente il SIISL è andato espandendo le proprie funzionalità per supportare anche un’utenza più ampia, includendo i percettori di NASPI e DIS-COLL²⁶. Fino a prevedere, con il d.l. 31 ottobre 2025 n. 159 (art. 14), il vero e proprio obbligo per tutti i datori di lavoro che chiedono benefici contributivi sulle assunzioni, comunque denominati, finanziati con risorse pubbliche, di pubblicare *previamente* su SIISL “la disponibilità della posizione di lavoro”. Lo stesso obbligo è esteso alle Agenzie del lavoro che sono tenute alla pubblicazione

²³ M. FAIOLI, *Matchmaking. Tecnologia avanzata, regole e mercato del lavoro*, in *LD*, 2023, n. 2, pp. 333 ss.; P. BOZZAO, *L’intermediazione del lavoro nel programma GOL: potenzialità e criticità*, 2023, n. 2, pp. 259 ss.

²⁴ In conformità all’art. 50-ter d.lgs. n. 82/2005. Cfr. il DPCM (Dipartimento per la trasformazione digitale) del 22 settembre 2022 “Obblighi e termini di accreditamento alla Piattaforma digitale nazionale dati (PDND)” e la successiva direttiva del Sottosegretario alla Presidenza del Consiglio 5 dicembre 2023 “Misure per l’attuazione dell’articolo 50-ter del decreto legislativo 7 marzo 2005, n. 82” contenente gli indirizzi operativi per l’utilizzo della PDND.

²⁵ SIISL è stato progettato per facilitare la comunicazione e la collaborazione tra diversi enti a livello locale e nazionale. E’ composto da: Ministero del lavoro e delle Politiche Sociali, INPS, ANPAL, CPI, Patronati e CAF, Agenzie per il lavoro, Agenzie formative, Ministero dell’istruzione e del Merito e Ministero dell’Università e della Ricerca.

²⁶ D.l. 7 maggio 2024 n. 60 conv. In l. n. 95/2024.

su SIISL “di tutte le posizioni di lavoro che gestiscono”. Si intravede in questa previsione, più che la realizzazione del sistema informativo unitario, un principio di realizzazione della Borsa continua nazionale del lavoro di cui all’art. 15 d. lgs. n. 276/2003, ma con la non trascurabile differenza che, mentre il sistema della Borsa doveva essere alimentato da tutte le informazioni utili a tale scopo “immesse liberamente” nel sistema stesso sia dagli operatori pubblici e privati, autorizzati o accreditati, sia direttamente dai lavoratori e dalle imprese; l’impostazione del SIISL appare più dirigistica, accentrata e fondata sulla obbligatorietà del conferimento delle informazioni da parte delle imprese e delle Agenzie per il lavoro, che sembra rievocare, piuttosto, il regime del collocamento pubblico del passato.

Dal canto suo il fascicolo elettronico del lavoratore è rimasto fino ad oggi ineffettivo, salve alcune importanti sperimentazioni aziendali e settoriali²⁷, benché il legislatore abbia continuato a farvi riferimento per la formazione obbligatoria in apprendistato²⁸ e in materia di salute e sicurezza sul lavoro²⁹. Recentemente, con l’art. 5 d.l. 159/2025 (di modifica del c. 14 dell’art. 37 d. lgs. 81/2008), si è prevista la registrazione delle competenze acquisite in esito alla formazione per la sicurezza sul lavoro “nel fascicolo elettronico del lavoratore”, ma anche all’interno “del fascicolo sociale e lavorativo del cittadino”, di cui però non sono fornite ulteriori specifiche. Un richiamo alla registrazione delle competenze nel “fascicolo elettronico del lavoratore nell’ambito del sistema informativo unitario delle politiche attive del lavoro” è previsto inoltre dal D.M. 9 luglio 2024 recante la disciplina dell’individuazione, validazione e certificazione delle competenze relative alle qualificazioni di titolarità del Ministero del Lavoro³⁰.

Le speranze di un prossimo decollo del fascicolo elettronico, dunque, non sono ancora del tutto sopite.

2. La tensione dialettica tra condivisione informativa, circolazione e protezione dei dati personali nelle politiche attive del lavoro ancora alla ricerca di un (difficile) equilibrio tra GDPR e DGA

Il sistema delle PAL accoglie una visione dinamica dei dati delle persone riferiti al loro status professionale, che punta alla circolazione informativa, in controtendenza rispetto alla visione statica e prevalentemente protettiva che caratterizza nel campo del lavoro, e non solo, l’approccio giuridico classico al trattamento dei dati. La sfida che pone un sistema moderno di PAL è innanzitutto quella di superare l’idea della protezione e l’effetto *lock-in* dei dati personali professionali da parte dei titolari del trattamento, senza rinunciare ovviamente alle garanzie dei diritti fondamentali. Sarebbe opportuno

²⁷ Si rinvia sul punto a S. CIUCCIOVINO, *Microcredenziali e “certificazioni” delle competenze dei lavoratori nella prospettiva dell’apprendimento permanente*, in *Federalismi.It, Focus Lavoro persona tecnologia*, 2025, n. 14, pp.164 ss.

²⁸ Art. 46, d. lgs. n. 81/2015.

²⁹ Art. 37, c. 14, d. lgs. n. 81/2008.

³⁰ S. CIUCCIOVINO, *Microcredenziali e “certificazioni” delle competenze dei lavoratori nella prospettiva dell’apprendimento permanente*, *cit.*

abbracciare in modo più deciso un'accezione dinamica dei dati³¹ nel mercato del lavoro, dove la rappresentazione digitale dell'identità professionale personale e la portabilità/circolazione costituiscono forme di creazione di valore sociale.

Un simile sviluppo di approccio del resto riflette la traiettoria evolutiva che ha imboccato la tutela giuridica della *privacy* nel tempo, passando dalla visione statica dei primordi, al dinamismo dei dati come interesse giuridicamente rilevante³² e che ha visto il concetto di diritto alla solitudine (*the right to be let alone*) evolversi, attraverso la logica dei diritti fondamentali, in un più compiuto diritto alla autodeterminazione informativa, segnato dall'avvento del Regolamento UE 2016/679, che implica il potere consapevole dell'interessato nella gestione dei dati che lo riguardano³³. Con l'accrescersi della *dataficazione* del mondo reale, il potere dei dati nella c.d. *datasfera*³⁴ è anche quello di generare ulteriori diritti, accrescere la capacitazione, determinare l'accesso (o l'esclusione) dai sistemi di protezione sociale e di welfare³⁵ e dalle PAL, a seconda dei criteri di *clusterizzazione* adottati, dei sistemi di profilazione³⁶, di *microtargeting*, nonché in base alla storicizzazione delle informazioni che descrivono le caratteristiche soggettive e i percorsi delle persone. Nel campo del welfare e delle politiche attive, i dati degli individui e la *memoria informativa* che li riguarda diventano essenziali fattori abilitanti delle prestazioni sociali.

Ci stiamo addentrando ora in un'ulteriore fase evolutiva dell'approccio regolativo ai dati, specie a seguito della emanazione del Regolamento europeo 2022/868 relativo alla *governance* europea dei dati (*Data Governance Act - DGA*), che a sua volta si inserisce all'interno di un più vasto pacchetto digitale europeo³⁷.

³¹ A. TROJSI, *Sull'impatto giustavoristico del Data Governance Act. Riflessioni sistemiche a prima lettura del Regolamento (UE) 2022/868*, in *Federalismi.it Lavoro Persona Tecnologia*, 2023, n. 4, p. 282.

³² S. RODOTÀ, *Il diritto di avere diritti*, cit., 397; A. TROJSI, *Il diritto del lavoratore alla protezione dei dati personali*, Giappichelli, Torino, 2013; C. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *Federalismi.it*, 2018, n. 22, pp. 4 ss.; C. COLAPIETRO, A. IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale Scientifica, Napoli, 2017, pp. 85 ss.

³³ F. FAINI, *Data society. Governo dei dati e tutela dei diritti nell'era digitale*, cit.; A. TROJSI, *Il diritto del lavoratore alla protezione dei dati personali*, cit.; L. D'ARCANGELO, *La tutela del lavoratore nel trattamento dei dati personali*, Aracne, Roma, 2024.

³⁴ V. ZENO ZENCOVICH, *La "Datasfera". Regole giuridiche per il mondo digitale*, in L. SCAFFARDI (a cura di), *I "profili" del diritto. Regole, rischi e opportunità nell'era digitale*, Dossier VII - Diritto Pubblico Comparato ed Europeo, Giappichelli, Torino, pp. 99 ss.

³⁵ M. D'ONGHIA, *Intelligenza artificiale, Regolamento UE 2024/1689 e diritti previdenziali*, in corso di pubblicazione in *Federalismi, Focus Lavoro Persona Tecnologia*.

³⁶ A. TROJSI, *The confirmed, indeed reinforced, Centrality of the GDPR for the Protection of Workers' Personal Rights in the light of subsequent EU Legislative Acts*, *ILLeJ*, 2024, vol. 17, n. 2, p. 361.

³⁷ Di cui fanno parte, per ciò che interessa ai fini del presente studio, oltre al DGA e all'AI Act - Regolamento europeo sull'intelligenza artificiale (UE) 2023/1689, almeno il Digital Markets Act (Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022) volto a regolare il libero mercato e limitare gli abusi di potere economico degli oligopoli digitali organizzati in piattaforme e il Digital Services Act (Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022) sul mercato unico dei servizi digitali che detta un quadro regolatorio per il contrasto degli illeciti in rete e la responsabilità per i contenuti informativi. Sull'intero pacchetto digitale e sulla portata del DGA in particolare si rinvia a G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., pp. 605 ss.

Il DGA disciplina l'accesso ai dati del settore pubblico e introduce meccanismi di incentivazione alla condivisione dei dati anche in possesso di operatori privati³⁸.

Lo scopo del DGA, infatti, è quello di favorire la circolazione in sicurezza dei dati, in particolare, quelli in possesso degli enti pubblici in una prospettiva di sviluppo di una società e di una economia dei dati antropocentriche, affidabili e sicure (Cons. 3). Prevede un regime di "altruismo" dei dati, per il riutilizzo di alcune categorie di dati protetti detenuti da enti pubblici e per la fornitura di servizi di intermediazione dei dati e di servizi basati sull'altruismo, cioè sul conferimento volontario per fini di interesse pubblico o generale anche per il miglioramento delle politiche pubbliche. L'idea sottesa è che la circolazione e riutilizzo "dei dati generati o raccolti da enti pubblici o altre entità a carico dei bilanci pubblici debbano apportare benefici alla società" (Cons. 6). Il DGA promuove la diffusione delle tecniche per bilanciare le esigenze di circolazione con quelle di protezione, quali le tecniche di anonimizzazione, la *privacy* differenziale, la generalizzazione, la pseudonimizzazione, l'utilizzo di dati sintetici o metodi analoghi.

Il DGA ha trovato attuazione in Italia con il d. lgs. 7 ottobre 2024 n. 144, ispirato ad un certo minimalismo regolativo che, oltre ad attribuire ad AgId (Agenzia per l'Italia digitale) le competenze nazionali in materia, ha dettato il regime sanzionatorio per la violazione del Regolamento.

Ai fini del presente scritto, importa sottolineare come tale atto contribuisca ad inaugurare, unitamente al pacchetto digitale europeo, una diversa prospettiva dell'approccio ai dati. La dottrina vi ha ravvisato una nuova fase evolutiva del diritto alla *privacy*, ispirata "*al concetto di diritto del "governo" dei dati, cioè di guida e di accompagnamento promuovente la circolazione e l'uso condiviso degli stessi (dunque, non inibente od oppositivo rispetto a questa), guardata come foriera di opportunità e non soltanto come rischio*"³⁹. Il che è destinato a produrre una inesorabile incrinatura della primazia concettuale e assiologica rivestita storicamente dalla normativa di protezione dei dati personali in ambito europeo, con l'emergere di un modello più complesso "*dove le istanze di protezione dei dati coesisteranno con pari dignità con quelle di libero accesso e riutilizzo dei dati medesimi*"⁴⁰.

L'evoluzione di impostazione non porta, ovviamente, a destrutturare la protezione dei dati personali, ma semmai a rivalutare il profilo di garanzia di circolazione dei dati, pur presente nel GDPR, ma meno coltivato nell'interpretazione più diffusa, rispetto al profilo della protezione degli stessi. L'evoluzione concettuale, d'altra parte, non mette in discussione la centralità del GDPR anche nella nuova stagione regolativa della *data law*⁴¹, ma richiede di proiettare lo sguardo verso un panorama più ricco, articolato e

³⁸ E. SIGNORINI, *Il regolamento (UE) 2022/868 sulla governance dei dati e le sue possibili ricadute sulle misure di inclusione lavorativa delle persone con disabilità*, in *Federalismi.it Lavoro Persona Tecnologia*, 2023, n. 9, pp. 257 ss.

³⁹ A. TROJSI, *Sull'impatto giuslavoristico del Data Governance Act. Riflessioni sistemiche a prima lettura del Regolamento (UE) 2022/868*, cit., p. 283.

⁴⁰ G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., p. 608.

⁴¹ A. TROJSI, *The confirmed, indeed reinforced, Centrality of the GDPR for the Protection of Workers' Personal Rights in the light of subsequent EU Legislative Acts*, cit.

complesso di “dati”, rispetto alla dicotomia classica dato personale/dato non personale⁴², che porta a ragionare sulla circolazione dei dati, come espressione non soltanto di un interesse individuale, ma anche di un più ampio interesse sociale e collettivo.

Il cambiamento di prospettiva innescato dal DGA dovrebbe riuscire a contaminare le PAL, almeno quelle in mano pubblica⁴³, modificando la postura, anche mentale oltre che regolativa, da assumere in relazione al *capitale informazionale* dell’individuo destinatario delle politiche attive, così come in relazione alla gestione, all’uso e al riutilizzo dei dati presenti nelle banche dati dei soggetti della Rete nazionale di cui si è trattato nel precedente § 1. Proprio questo cambiamento culturale potrebbe fornire lo slancio necessario a realizzare finalmente la filosofia di fondo del d. lgs. 150 e ad inaugurare una nuova stagione delle PAL. Si tratta, ovviamente, di ragionare in termini di compatibilità tra GDPR e DGA⁴⁴, tra normativa di protezione dei dati e collaborazione informativa propria della normativa di funzionamento delle PAL, per ricercare soluzioni, anche operative, in grado di far convivere i due paradigmi: da un lato quello della protezione dei dati personali e, dall’altro lato, quello della circolazione e condivisione delle informazioni. Avendo ben presente che, se è indubbio che la protezione dei dati personali è strettamente legata al valore costituzionale della dignità della persona, non di meno l’effettività del funzionamento dei servizi al lavoro e delle politiche attive è strettamente collegata ai valori costituzionali di tutela del lavoro e di libera circolazione delle persone.

Il bilanciamento tra protezione e circolazione dei dati, non è effettuato direttamente dal legislatore se non in minima parte, dal momento che di solito le previsioni che richiedono la collaborazione informativa, l’accesso e lo scambio dei dati ripropongono la consueta formula criptica che lascia impregiudicato il rispetto delle disposizioni della normativa in materia di protezione dei dati personali, lasciando così all’interprete l’onere di trovare le soluzioni in termini di compatibilità tra i due plessi normativi⁴⁵.

Certo è che la normativa vigente legittima il trattamento anche senza il consenso dell’interessato dei dati conferiti ai servizi per il lavoro e ai soggetti istituzionali e regionali deputati alle politiche attive, in quanto si tratta di trattamento di dati personali effettuato per l’esecuzione di un compito di interesse pubblico o

⁴² In base alla definizione dell’art. 2 DGA per “dato” si intende “qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva”, mentre per dato personale si fa espresso rinvio al GDPR.

⁴³ Sulla distinzione tra politiche attive pubbliche e private v. S. CIUCCIOVINO, *Contrattazione collettiva e politiche attive del lavoro*, GDLRI, 2021, n. 172, 4, p. 641.

⁴⁴ A. TROJSI, *The confirmed, indeed reinforced, Centrality of the GDPR for the Protection of Workers’ Personal Rights in the light of subsequent EU Legislative Acts*, cit.

⁴⁵ Per la Borsa continua del lavoro cfr. l’art. 15 e l’art. 16 del d. lgs. n. 276/2003 prevedono che gli standard tecnici e i flussi informativi di scambio tra i sistemi, devono avvenire “nel rispetto delle disposizioni della l. 31 dicembre 1996, n. 675”. In questo caso però abbiamo un’accessibilità diretta da parte dei privati, in quanto vale un principio di continua e diretta alimentazione della borsa da parte dei singoli lavoratori e delle imprese e da parte degli operatori pubblici e privati, accreditati o autorizzati, tenuti a conferire alla borsa i dati acquisiti dai lavoratori e dalle imprese (art. 15, c. 3, d. lgs. n. 276/2003 e oggi l’art. 14, d.l. 31 ottobre 2025 n. 159).

connesso all'esercizio di pubblici poteri⁴⁶ e per la comunicazione fra titolari che effettuano trattamenti di dati personali.

Ulteriori norme forniscono la base giuridica del trattamento dei dati personali, anche particolari, degli studenti per fini di orientamento, formazione e inserimento professionale e lavoro⁴⁷ e dei lavoratori quando si tratta di esercitare diritti, poteri, obblighi in materia di diritto del lavoro e sicurezza e protezione sociale⁴⁸.

Si può dire, quindi, che la collaborazione informativa tra soggetti pubblici e privati di cui al d. lgs. 150/2015 si basa su una solida base giuridica con connessa liceità del relativo trattamento dei dati personali acquisiti per dette finalità. Il punto non riguarda tuttavia, la base giuridica in sé, quanto la concreta delimitazione degli ambiti e delle caratteristiche del trattamento rispetto ai principi di finalità, correttezza, proporzionalità e il faticoso superamento culturale della concezione dominicale e proprietaria dei dati personali da parte dei titolari del trattamento.

Le preoccupazioni connesse alla tutela della *privacy* hanno finito per compromettere la trasparenza del mercato del lavoro, mantenendo segregati in archivi chiusi dei singoli enti i dati fondamentali che descrivono le qualità professionali delle persone, frammentando così l'identità professionale del lavoratore in tante tessere di un *puzzle* difficilmente ricomponibile.

Probabilmente una più forte affermazione dei principi di circolazione e riutilizzo dei dati ai sensi del DGA consentirebbe di superare alcune resistenze e preoccupazioni connesse alla *compliance* rispetto all'apparato normativo sulla protezione dei dati⁴⁹. A tali norme occorre oggi fare riferimento, in una logica meno difensiva e protezionistica del passato, anche per la corretta implementazione dell'architettura di *governance* e scambio informativo previsto dal d. lgs. 150/2015. Senza considerare gli ulteriori scenari che potrebbero aprirsi qualora l'Italia decidesse di adottare, su questo fronte, politiche per l'uso "altruistico"

⁴⁶ L'art. 2-ter d. lgs. 196/2003 prevede che serva come base giuridica del trattamento una norma di legge, di regolamento o di atto amministrativo generale.

⁴⁷ E' ammessa la comunicazione e la diffusione, su richiesta degli interessati, pure a privati e per via telematica di dati personali degli studenti al fine di agevolare l'orientamento, da parte delle istituzioni del sistema nazionale di istruzione, dei centri di formazione professionale regionale e delle istituzioni di alta formazione e università, quando si tratti di dati relativi agli esiti formativi, intermedi e finali, degli studenti. Tali dati possono essere successivamente trattati esclusivamente per le predette finalità (art. 96 Codice privacy).

⁴⁸ L'art. 9 GDPR consente la deroga al divieto di trattamento dei dati personali particolari che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, così come il trattamento di dati genetici e 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. È esentato dal divieto generale altresì il trattamento reso necessario da finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali (art. 9.2, lett. h), purché tali dati siano trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale. Per un approfondimento si rinvia a A. MARESCA, S. CIUCCIOVINO, I. ALVINO, *Regolamento UE 2016/679 e rapporto di lavoro*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, 311 ss., Napoli, Editoriale Scientifica, 2017, pp. 311 ss.

⁴⁹ Per un approfondimento nella prospettiva del mercato del lavoro Trojsi 2023b, 283.

dei dati, in un'ottica di restituzione a vantaggio della collettività del valore dei propri dati, previsto appunto dal DGA come opzione politica e regolativa dei Governi nazionali, da notificare alla Commissione (art. 16, DGA⁵⁰), ma che il legislatore italiano non ha ancora adottato.

3. IA e mercato del lavoro: l'impostazione dell'EU AI Act e della l. 132/2025 a confronto

Il tema dei dati del mercato del lavoro, della loro condivisione, uso e riutilizzo si colora di ulteriore complessità al cospetto dell'impiego dell'Intelligenza Artificiale (IA) nel contesto delle PAL. Occorre muovere dall'assunto che l'utilizzo della IA per fini di politica attiva del lavoro e funzionamento del mercato del lavoro è prevista espressamente dal Regolamento europeo (EU) 2023/1689 (AI Act), che include i relativi sistemi di IA, elencandoli nell'Allegato III, tra quelli di cui si presume l'alto rischio. Si tratta quindi di applicazioni lecite; mentre sono vietati - per quanto qui interessa - i sistemi di rilevazione delle emozioni sul luogo di formazione e di lavoro tramite la biometria⁵¹, salvo che per motivi medici o di sicurezza (art. 5.1, lett. f), così come sono vietati i sistemi di categorizzazione biometrica che classificano le persone fisiche sulla base dei loro dati biometrici per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale (art. 5.1, lett. g); nonché i sistemi di *social scoring* che effettuano la valutazione o la classificazione delle persone fisiche o di gruppi di persone per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note, inferite o previste, in cui il punteggio sociale comporti un trattamento pregiudizievole o sfavorevole in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti, oppure un trattamento pregiudizievole o sfavorevole ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità (art. 5.1, lett. c)⁵².

⁵⁰ L'altruismo dei dati consiste nella possibilità per gli interessati di rendere disponibili su base volontaria, a fini di altruismo dei dati, i dati personali che li riguardano detenuti da enti pubblici. Spetta agli Stati stabilire le informazioni necessarie che devono essere fornite agli interessati in merito al riutilizzo dei loro dati nell'interesse generale. Si pensi ad esempio agli impieghi che potrebbero essere fatti in campo sanitario, per la vivibilità delle città, ecc. Sull'altruismo dei dati v. ampiamente G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., pp. 619 ss.

⁵¹ L. TEBANO, *Poteri datoriali e dati biometrici nel contesto dell'AI Act*, in *Federalismi.it, Focus Lavoro Persona Tecnologia*, 2023, n. 25, pp. 198 ss.; C. TOSCANO, *Il divieto di utilizzo di sistemi di intelligenza artificiale per l'inferenza degli stati emotivi nei contesti lavorativi alla luce delle Linee guida della Commissione europea sull'AI Act*, in *Federalismi.it Lavoro Persona Tecnologia*, Paper, 28 maggio 2025.

⁵² In proposito si vedano le Linee guida della Commissione del 4 febbraio 2025, in attuazione dell'articolo 96, paragrafo 1, lettera b), dell'AI Act. Le Linee guida riportano come caso esemplificativo di un trattamento di *social scoring* vietato dall'art. 5.1. lett. c) quello di una Agenzia del lavoro pubblica che utilizza un sistema di IA per attribuire un punteggio alle persone disoccupate sulla base di un colloquio e di una valutazione al fine di determinare se una persona debba beneficiare di un sostegno statale all'occupazione, quanto tale punteggio si basa non soltanto su caratteristiche personali pertinenti, quali l'età e l'istruzione, ma anche su variabili raccolte o inferite da dati e contesti senza alcun evidente collegamento con lo scopo della valutazione, quali lo stato civile, i dati sanitari per le malattie croniche, la dipendenza, ecc. (§ 166 delle Linee Guida).

In larga misura le applicazioni elencate dal § 4 “Occupazione, gestione dei lavoratori e accesso al lavoro autonomo”, dell’allegato III sono comprese nelle attività di somministrazione, di intermediazione, di ricerca e selezione del personale, di supporto alla ricollocazione professionale, così come definite dall’articolo 2 del d. lgs. n. 276/2003, svolte dalle Agenzie del lavoro di cui all’articolo 4, nonché dagli ulteriori soggetti, compresi i siti internet, che operano in base ai regimi particolari di autorizzazione e di accreditamento di cui agli articoli 6 e 7 del d. lgs. n. 276/2003, ma anche da parte degli stessi soggetti pubblici deputati all’incontro domanda offerta (piattaforma SIISL o i sistemi regionali automatizzati di incontro domanda offerta).

Per quanto riguarda le applicazioni elencate dal § 3 “Istruzione e formazione professionale” è possibile ricomprendervi almeno una parte dei servizi e delle misure di politica attiva del lavoro, come definite dall’art. 18 del d. lgs. n. 150/2015, messe in atto dai soggetti privati accreditati dalle regioni, nonché la formazione professionale continua, ivi compresa quella finanziata dai fondi interprofessionali di cui all’articolo 118 della l. n. 388/2000, nonché dai fondi bilaterali di cui all’articolo 12, c. 4, del d. lgs. n. 276/2003⁵³. Inoltre le applicazioni previste dal § 5 “Accesso a servizi privati essenziali e a prestazioni e servizi pubblici essenziali e fruizione degli stessi”, relativi ai sistemi destinati a essere utilizzati dalle autorità pubbliche o per conto di autorità pubbliche per valutare l’ammissibilità delle persone fisiche alle prestazioni e ai servizi di assistenza pubblica essenziali, possono attecchire ai sistemi automatizzati di gestione delle condizionalità all’accesso di provvidenze pubbliche.

La classificazione ad alto rischio dell’Allegato III è inderogabile per i sistemi di IA che effettuano una profilazione di persone fisiche (art. 6.3 AI Act) ed è molto probabile che un sistema di IA applicata alle risorse umane e alle PAL si basi su una preventiva profilazione delle persone fisiche⁵⁴. Quando invece i sistemi, pur compresi nell’allegato III, non dovessero presentare un rischio “significativo” di danno per la salute, la sicurezza o per i diritti fondamentali delle persone fisiche, oppure non fossero destinati ad influenzare materialmente il processo decisionale, fuoriuscirebbero dall’area dell’alto rischio. In particolare non è considerato ad alto rischio il sistema di IA che si ponga in una posizione di complementarità rispetto ad un processo decisionale più ampio oppure quando sia destinato ad ottimizzare gli esiti di processi decisionali umani già conclusi.

L’inclusione nell’area di alto rischio ha come conseguenza l’applicabilità degli obblighi previsti dal Capo III del Regolamento che, in linea di massima si aggiungono a quelli già previsti dal GDPR⁵⁵ qualora vengano trattati dati personali o dati misti. La natura complementare dei due plessi normativi è prevista

⁵³ S. CIUCCIOVINO, *Risorse umane e intelligenza artificiale alla luce del regolamento (UE) 2024/1689, tra norme legali, etica e codici di condotta*, in *DRI*, 2024, 3, pp. 573 ss.

⁵⁴ M.T. CARINCI, A. INGRAO, *L’impatto dell’AI Act sul diritto del lavoro*, 2024, n. 184, 4, pp. 465 ss.

⁵⁵ Art. 2.7. Sul punto M. PERUZZI, *IA e obblighi datoriali di tutela del lavoratore: necessità e declinazioni dell’approccio riskbased*, in *Federalismi.it Lavoro Persona Tecnologia*, 2024, n. 30, pp. 225 ss.

espressamente dall'AI Act in via generale (Cons. 10, 69), anche nell'ottica di evitare duplicazioni di adempimenti per i *deployer*⁵⁶. Per quanto riguarda le applicazioni nel campo delle politiche attive e del mercato del lavoro, ciò implica che le disposizioni dell'AI Act vanno ad integrarsi con quelle già adottate ai fini della valutazione di impatto della *privacy* (DPIA) e con quelle di massima applicabili a fronte di processi decisionali automatizzati relativi alle persone fisiche, compresa la profilazione, di cui all'art. 22 del GDPR. Poiché nei sistemi ad alto rischio è richiesta la valutazione preliminare di impatto sui diritti fondamentali (Fundamental Rights Impact Assessment - FRIA)⁵⁷ che compete al *provider* e al *deployer* qualora si tratti di un organismo di diritto pubblico o un ente privato incaricato di un pubblico servizio (art. 27 AI Act), potranno essere trovate sovrapposizioni e punti di contatto con la DPIA.

Rispetto alla impostazione dell'AI Act, la l. 23 settembre 2025 n. 132 delinea una via italiana alla regolazione dell'IA. Essa è destinata ad applicarsi, in via complementare all'AI Act, a tutti coloro che, in Italia, sono impegnati nella ricerca, nella sperimentazione, nello sviluppo, nell'adozione, nell'applicazione e nell'utilizzo di sistemi di IA (v. art. 1 e 3, l. 132/2025). Il quadro normativo a livello italiano si deve ancora completare, in quanto la legge contiene deleghe al Governo per l'emanazione di ulteriori disposizioni, che dovranno essere adottate con successivi decreti legislativi e atti regolamentari.

La prevalente impronta regolativa della l. 132 è quella di fornire risposte alle molte preoccupazioni connesse all'uso della IA in diversi contesti d'uso, che polarizzano ormai da tempo il dibattito pubblico e scientifico. La legge avrebbe l'ambizione di creare un quadro più chiaro e orientare l'applicazione dei sistemi di IA, fissando regole di principio e criteri di utilizzo *fair*. Il Regolamento europeo da questo punto di vista non è di agevole gestione: è, sì, direttamente applicabile come disciplina uniforme per gli Stati dell'UE, ma allo stesso tempo è impostato come regolazione di sicurezza del prodotto che addossa le principali responsabilità ai *providers* (produttori dei sistemi)⁵⁸.

Viceversa, la legge italiana trascina l'apparato regolativo essenzialmente sul piano dell'adozione e utilizzazione dei sistemi (quindi nella prospettiva prevalente dei *deployers* pubblici e privati), intervenendo sulle finalità d'uso in generale e in diversi ambiti specifici: sanità, lavoro, professioni intellettuali, pubblica amministrazione, attività giudiziaria e *copyright*, rinviando alla decretazione delegata l'ulteriore

⁵⁶ L'art. 27 in materia di valutazione di impatto sui diritti fondamentali per i sistemi di IA ad alto rischio prevede che “Se uno qualsiasi degli obblighi di cui al presente articolo è già rispettato mediante la valutazione d'impatto sulla protezione dei dati effettuata a norma dell'articolo 35 del regolamento (UE) 2016/679 o dell'articolo 27 della direttiva (UE) 2016/680, la valutazione d'impatto sui diritti fondamentali di cui al paragrafo 1 del presente articolo integra tale valutazione d'impatto sulla protezione dei dati”.

⁵⁷ A. MANTELERO, M. PERUZZI, *L'AI Act e la gestione del rischio nel sistema integrato delle fonti*, in RGL, 2024, n. 4, pp. 527 ss.; A. MANTELERO, *Sub art. 35*, in R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA (a cura di), *Codice della privacy e data protection*, Giuffrè, Milano, 2021, pp. 532 ss.; O. POLLICINO, *La disciplina dell'intelligenza artificiale*, Giuffrè, Milano, 2025.

⁵⁸ S. CIUCCIOVINO, *Risorse umane e intelligenza artificiale alla luce del regolamento (UE) 2024/1689, tra norme legali, etica e codici di condotta*, cit.

adeguamento in materia di servizi bancari, finanziari, assicurativi e di pagamento. Nel fare ciò costruisce un vero e proprio codice nazionale di criteri di impiego della IA, che si sovrappone a quello europeo (e quindi deve tener conto anche del complesso sistema regolativo dell'AI Act fondato sul rischio). Tutto ciò si deve, chiaramente, integrare con la disciplina nazionale già vigente e con le ulteriori fonti europee applicabili.

La legge contiene alcune disposizioni di principio, molte delle quali invero sono in parte ripetitive di principi ordinamentali interni e sovranazionali che potevano considerarsi già pienamente applicabili agli impieghi della IA. Ciò ubbidisce, come detto, ad un proposito rassicurante più che autenticamente dispositivo del nostro legislatore, evidentemente con l'ambizione di creare quella fiducia nell'IA e garanzia di antropocentrismo, diventato ormai un caposaldo concettuale a livello nazionale ed europeo. Si veda, ad esempio, il richiamo dell'art. 1 all'"utilizzo corretto, trasparente e responsabile, in una dimensione antropocentrica, dell'intelligenza artificiale, volto a coglierne le opportunità". Il richiamo dell'art. 3 al "rispetto dei diritti fondamentali e delle libertà previste dalla Costituzione, del diritto dell'Unione europea e dei principi di trasparenza, proporzionalità, sicurezza, protezione dei dati personali, riservatezza, accuratezza, non discriminazione, parità dei sessi e sostenibilità". Il richiamo nell'art. 4 ad un utilizzo della IA che garantisca "il trattamento lecito, corretto e trasparente dei dati personali e la compatibilità con le finalità per le quali sono stati raccolti, in conformità al diritto dell'Unione europea in materia di dati personali e di tutela della riservatezza".

Più problematiche sono le regole precettive sull'utilizzo della IA contenute nel provvedimento, sia di carattere generale, sia di carattere settoriale per gli usi in alcuni campi. Dal punto di vista lavoristico il principale problema che pone la legge 132 consiste nel fatto che sembra circoscrivere obiettivamente gli utilizzi dell'IA, mentre l'approccio europeo è piuttosto quello di considerare leciti tutti i sistemi di IA, salve le ipotesi tassativamente vietate perché considerate a rischio inaccettabile (come, ad esempio, il *social scoring* e l'inferenza delle emozioni tramite la biometria nei luoghi di formazione e di lavoro).

L'impostazione della legge italiana, al contrario, quasi in un rovesciamento della piramide del rischio, sembra voler circoscrivere e ridisegnare il perimetro dell'impiego legittimo dei sistemi di IA, in senso apparentemente più restrittivo di quello ammesso a livello europeo. Non è dato comprendere fino a che punto ciò sia stato fatto con un preciso intento restrittivo o risulti soltanto quale effetto indiretto di norme tese a sottolineare gli utilizzi *fair* dell'IA di cui si è detto. Fatto sta che la l. 132, da un lato, introduce veri e propri limiti all'utilizzo della IA e, dall'altro lato, pone norme che, indicando le finalità d'uso della IA, finiscono apparentemente per funzionalizzarne l'impiego verso scopi predefiniti dallo stesso legislatore. Esempi di veri e propri limiti di utilizzo li troviamo in ambito giudiziario, dove la sperimentazione e l'impiego dei sistemi di intelligenza artificiale negli uffici giudiziari ordinari viene subordinata alla

preventiva autorizzazione del Ministero della giustizia, sentite le Autorità nazionali per l'IA almeno fino alla piena applicazione dell'AI Act (art. 15); laddove fino ad oggi esperienze, anche virtuose, di impiego in ambito giudiziario sono avvenute per iniziativa spontanea e pionieristica in talune magistrature. Anche per le professioni intellettuali si pongono limiti di impiego, consentendo l'utilizzo dell'IA soltanto per "l'esercizio delle attività strumentali e di supporto all'attività professionale e con prevalenza del lavoro intellettuale oggetto della prestazione d'opera" (art. 13), difficile poi stabilire come verrà misurata la prevalenza.

Più complicata invece è l'interpretazione delle norme che pongono finalità d'uso in certi settori, come ad esempio per il lavoro, L'art. 11 afferma che l'IA è impiegata "per migliorare le condizioni di lavoro, tutelare l'integrità psicofisica dei lavoratori, accrescere la qualità delle prestazioni lavorative e la produttività delle persone in conformità al diritto dell'Unione europea". Ne parrebbero di converso esclusi tutti i numerosi e ulteriori impieghi, ammessi espressamente dall'Allegato III dell'AI Act, proprio per le PAL, per l'orientamento professionale, per l'incontro tra domanda e offerta di lavoro, per la valutazione dei cv dei candidati, per il recruitment.

Norme di questo tipo, che ritroviamo anche se in forma meno problematica in ambito sanitario (art. 7) e di uso nella p.a. (art. 14), pongono due questioni interpretative non trascurabili. Innanzitutto, c'è da chiedersi se utilizzi diversi da quelli espressamente contemplati dalla norma italiana siano a questo punto legittimi, il che è davvero paradossale per una legge che dichiara di voler promuovere lo sviluppo e l'utilizzo dell'intelligenza artificiale ... nei settori produttivi, la produttività in tutte le catene del valore e le funzioni organizzative, nonché quale strumento utile all'avvio di nuove attività economiche e di supporto al tessuto nazionale produttivo..." (art. 5). Il secondo problema, da non trascurare, consiste nel fatto che norme incomplete di questo tipo rischiano di indebolire la base giuridica di liceità del trattamento dei dati personali, che - come già detto - rappresenta un presupposto fondamentale del Codice Privacy e del GDPR, cui non si sottraggono i sistemi di IA, e che potrebbe creare più problemi di quanto già non porti con sé, in generale, l'integrazione tra l'IA Act e il GDPR.

Ciò vale in modo speciale per il settore delle politiche attive e della interconnessione e scambio dati utile al mercato del lavoro, di cui al d. lgs. 150/2015 tramite sistemi di IA, che indubbiamente è lecito per l'AI Act in quanto compreso nelle applicazioni elencati dall'Allegato III, sebbene di norma ad alto rischio, mentre non è espressamente contemplato dalla normativa interna. Sembra però di poter interpretare il silenzio della disciplina interna in senso non escludente, anche perché condivisibilmente è stato osservato

come non sia consentito agli Stati membri prevedere divieti ulteriori rispetto a quelli contemplati dall'AI Act⁵⁹.

Può allora ritenersi legittimo, pur nel silenzio della l. 132, l'impiego della IA per il funzionamento delle politiche attive e del mercato del lavoro, nel rispetto dei limiti previsti dall'AI Act, anche perché l'intelligenza artificiale costituisce la frontiera più avanzata di quel processo di digitalizzazione che rappresenta uno degli assi portanti dell'architettura normativa delle politiche attive del lavoro (*retro* § 1). L'adozione di sistemi di IA in questo campo può rappresentare anche una via per assicurare una migliore e più efficace realizzazione della funzione di interesse pubblico, in quanto può garantire una maggiore e più ampia accessibilità alle misure e agli interventi, in linea con i valori di efficienza, pari opportunità ed efficacia del servizio pubblico⁶⁰. E' chiaro, peraltro, che i sistemi di IA nel campo delle politiche attive del lavoro dovranno ubbidire, oltre che ai requisiti previsti dall'AI Act, anche ai limiti e requisiti di impiego previsti dal legislatore italiano con la l. 132/2025. Tra questi va ricordato il divieto di discriminazione algoritmica (art. 11, c. 3), l'obbligo di trasparenza e di tutela dei dati personali, l'assolvimento della preventiva informazione (art. 11, c. 2, l. 132/2025 e art. 1 *bis* d. lgs. 152/1997), e più in generale la salvaguardia dei principi di tutela dei diritti fondamentali e delle libertà costituzionali richiamati dall'art. 3 l. 132/2025. Il problema, quindi, non è tanto l'*an*, quanto piuttosto il *quomodo* dell'impiego della IA nel campo del mercato del lavoro e delle politiche attive, su cui ci soffermerà in particolare nel prossimo paragrafo.

4. I tratti di specialità della disciplina del trattamento dei dati personali nei sistemi di IA e i possibili risvolti per le politiche attive del lavoro

L'AI Act rinvia integralmente alla normativa vigente europea in materia di diritto fondamentale alla protezione dei dati personali. Quest'ultima fornisce agli interessati la garanzia di un trattamento sostenibile e responsabile dei loro dati, anche qualora essi siano combinati con dati non personali. Il rapporto tra le due fonti normative - AI Act e GDPR - è, dunque, ispirato alla piena integrazione e complementarità ed, anzi, la concorrente applicazione del GDPR ai sistemi di IA dovrebbe costituire di per sé garanzia dell'utilizzo corretto e proporzionato dei dati, atto a prevenire gli abusi della IA⁶¹.

⁵⁹ Per questa notazione cfr. AA.VV., *Intelligenza artificiale Commentario*, a cura di A. MANTELETO, G. RESTA, G.M. RICCIO, Wolters Kluwer Italia, Milano, 2025, *Sub art. 1*, pp. 3 ss. (spec. 10) che sottolinea come il legislatore europeo abbia optato per la tecnica dell'unificazione giuridica per i divieti e per i requisiti specifici dei sistemi ad alto rischio (lett. b) e c) dell'art. 1, c. 2), in quanto il mancato rimando alla diversa tecnica dell'armonizzazione (prevista invece per le lett. a) d) ed e) dell'art 1, c.2.) sta proprio a segnalare "un divieto per gli Stati membri di introdurre ulteriori pratiche vietate, nonché ulteriori obblighi o requisiti per i sistemi di intelligenza artificiale ad alto rischio".

⁶⁰ G. RESTA, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Politica del diritto*, 2019, pp. 199 ss.

⁶¹ Art. 15.5 AI Act. A. TROJSI, *The confirmed, indeed reinforced, Centrality of the GDPR for the Protection of Workers' Personal Rights in the light of subsequent EU Legislative Acts*, *cit.*

L'integrazione delle fonti comporta, in particolare, che i fornitori e i *deployers* dei sistemi di IA siano tenuti ad assolvere agli obblighi giuridici previsti dalla normativa sulla protezione dei dati personali nel loro ruolo di titolari o responsabili del trattamento qualora i sistemi di IA comportino il trattamento di dati personali. Da parte loro, gli interessati godono dei diritti e delle garanzie previsti dal GDPR, ivi compresi i diritti connessi al processo decisionale esclusivamente automatizzato relativo alle persone fisiche, compresa la profilazione, di cui all'art. 22 del GDPR. Ciò vuol dire, peraltro, che il Regolamento IA non può fornire di per sé la base giuridica di trattamento dei dati richiesta dall'art. 22.2. lett. b) GDPR, quale condizione per il trattamento automatizzato, ma occorre che il trattamento trovi una base giuridica legittima autonoma *al di fuori* dell'AI Act.

In un'ottica di razionalizzazione degli adempimenti, l'integrazione tra le due fonti porta all'“assorbimento” di una serie di obblighi richiesti dall'AI Act negli analoghi e corrispondenti adempimenti previsti dal GDPR. Emblematico, a tal proposito, è l'art. 27 AI Act che esonera il *deployer* dall'effettuazione della valutazione di impatto (FRIA) sul sistema IA, ritenendola compresa e quindi assorbita dalla valutazione d'impatto sulla protezione dei dati (DPIA), effettuata a norma dell'articolo 35 GDPR o dell'art. 27 della direttiva (UE) 2016/680⁶².

Ciò detto occorre, tuttavia, mettere in evidenza anche alcuni tratti di spiccata specialità che la normativa *privacy* assume all'interno della infrastruttura regolativa della IA. Una specialità che emerge come portato, in primo luogo, della chiara tensione dell'AI Act a potenziare, più di quanto già non faccia il GDPR, il controllo sulla *qualità* dei dati⁶³, a monte del sistema (dati di input, dati di prova) e nei processi elaborativi (dati di convalida, dati di addestramento).

In secondo luogo, la specialità emerge in relazione alle particolari regole di trattamento dei dati previste dall'AI Act indirizzate ad evitare le tipiche distorsioni e discriminazioni (anche nelle nuove forme della *proxy discrimination*⁶⁴ o della discriminazione indiretta algoritmica⁶⁵), che possono scaturire dalla logica inferenziale dei sistemi di IA, da combattere anche mediante una speciale adeguata gestione quali/quantitativa delle grandi moli di dati che alimentano i sistemi di IA.

In terzo luogo la specialità del regime di protezione dei dati nei sistemi di IA si manifesta attraverso l'attenuazione in “ambiente controllato” di alcuni principi del GDPR, ammessa e tollerata per non frenare

⁶² A. MANTELERO, M. PERUZZI, *L'AI Act e la gestione del rischio nel sistema integrato delle fonti*, in RGL, 2024, n. 4, pp. 527 ss.

⁶³ M. BASSINI, *Intelligenza artificiale e diritti fondamentali: considerazioni preliminari*, in M. BIASI (a cura di), *Diritto del lavoro e intelligenza artificiale*, Giuffrè, Milano, 2024, pp. 23 ss.

⁶⁴ A. LO FARO, *Algorithmic Decision Making e gestione dei rapporti di lavoro: cosa abbiamo imparato dalle piattaforme*, in *Federalismi.it Lavoro Persona Tecnologia*, 2022, n. 25, p. 196.

⁶⁵ M. PERUZZI, *La discriminazione algoritmica*, in *Equal*, 2024, n. 1, pp. 7 ss.; G. GAUDIO, *Le discriminazioni algoritmiche*, in *LDE*, 2024, n. 1, pp. 2 ss.

l'innovazione e permettere la sperimentazione di sistemi di IA mirati a ricavare benefici collettivi e a meglio realizzare gli interessi pubblici.

Diversi riferimenti normativi contribuiscono a delineare questo speciale approccio alla gestione dei dati personali nell'AI Act.

Innanzitutto l'art. 26 nei sistemi ad alto rischio corresponsabilizza il *deployer*, qualora esso abbia il dominio sui dati, nell'effettuazione del controllo sulla qualità sugli stessi che, di base, compete al *provider*. Qui emerge, oltre che il controllo qualitativo, il controllo quantitativo sui dati di input, che deve essere indirizzato a verificare la sufficiente rappresentatività dei dati e delle tecniche matematico statistiche di trattamento al fine di minimizzare degli errori. L'esigenza di prevenire errori e distorsioni algoritmiche con i conseguenti potenziali effetti discriminatori, porta alla riconfigurazione del classico principio di minimizzazione dei dati personali tipico della normativa *privacy*, per consentirne l'adattamento al particolare ambiente normativo dell'intelligenza artificiale. A dire il vero uno spunto di questa necessità di adattamento alla specificità dei sistemi automatizzati già si trova nel GDPR (Cons. 71)⁶⁶, ma è ripreso con maggior vigore dall'AI Act all'art. 26, laddove prevede che “nella misura in cui esercita il controllo sui dati di input, il *deployer* garantisce che tali dati di input siano pertinenti e sufficientemente rappresentativi alla luce della finalità prevista del sistema di IA”. La logica di questo criterio è meglio esplicitata dal Cons. 67 dove si precisa che “dati di alta qualità e l'accesso a dati di alta qualità svolgono un ruolo essenziale nel fornire una struttura e garantire le prestazioni di molti sistemi di IA, in particolare quando si utilizzano tecniche che prevedono l'addestramento di modelli, al fine di garantire che il sistema di IA ad alto rischio funzioni come previsto e in maniera sicura e che non diventi una fonte di discriminazione vietata dal diritto dell'Unione”. Ancora, riguardo al set di dati di addestramento, convalida e prova, viene ribadita la necessità della loro pertinenza, sufficiente rappresentatività e integrità. Inoltre si aggiunge che i set di dati dovrebbero possedere “le proprietà statistiche appropriate, anche per quanto riguarda le persone o i gruppi di persone in relazione ai quali il sistema di IA ad alto rischio è destinato a essere usato” (Cons. 67 AI Act).

Il controllo quali/quantitativo sui dati immessi e sui dati di addestramento, guardato con la lente del diritto antidiscriminatorio, diventa allora un mezzo per prevenire le discriminazioni storiche e le stereotipizzazioni (*feedback loops* - «circuiti di feedback»: art. 15.4) e in tale contesto si giustifica

⁶⁶ “Al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e impedisca, tra l'altro, effetti discriminatori nei confronti di persone fisiche...”.

l'attenuazione di alcune garanzie tipiche della normativa *privacy*, per come le abbiamo fino ad oggi conosciute, come ad esempio il criterio della minimizzazione dei dati.

Emerge allora una sorta di adattamento (o allentamento⁶⁷) della normativa *privacy* o, meglio, l'esigenza di non discriminazione viene a plasmare l'accezione stessa di proporzionalità del trattamento, riconfigurando la portata del criterio della minimizzazione. Allo stesso tempo si incoraggiano sistemi, come l'anonimizzazione, la cifratura, la pseudonimizzazione, che aiutano a riconciliare gli obiettivi della estensione del set di dati necessari all'affidabilità del sistema e alla minimizzazione degli errori con quelli della tutela dei dati personali⁶⁸. Un approccio non dissimile, questo, da quello che ispira il DGA (v. *retro* § 2).

Per lo stesso motivo di contrasto alle discriminazioni algoritmiche, l'AI Act consente, eccezionalmente, ai fornitori di trattare categorie particolari di dati personali, in deroga alla normativa *privacy*, nella misura strettamente necessaria a garantire il rilevamento e la correzione delle distorsioni in relazione ai sistemi di IA ad alto rischio, quando si tratti di perseguire un interesse pubblico rilevante (Cons. 70).

Parallelamente, quando ciò sia dovuto a motivi medici o di sicurezza, è consentita da un lato, la deroga all'ordinaria disciplina *privacy* per il trattamento dei dati particolari e, dall'altro lato, l'esenzione dal divieto di inferenza delle emozioni tramite biometria (art. 5.1. lett. f)⁶⁹.

E' chiaro, in conclusione, che nel contesto del Regolamento europeo sulla IA, si fa strada una visione meno impermeabile e assolutizzante della normativa di protezione dei beni personali per come l'abbiamo fin qui conosciuta, e si viene a delineare uno statuto giuridico peculiare di trattamento dei dati personali nel contesto della IA, mirato a un necessario bilanciamento tra il diritto fondamentale alla protezione dei dati personali e la soddisfazione di beni/interessi pubblici di speciale rilevanza costituzionale, quali sono ad esempio quelli legati alla salute e sicurezza⁷⁰ che richiedono, a contrario, l'accrescimento della significatività dei dati e la loro circolazione.

D'altro canto la necessità di lavorare sul fronte dell'affinamento delle tecniche di trattamento e di assicurazione della qualità dei dati ad uso dei sistemi di IA ha spinto, a livello interno, la l. 132/2025 a delegare il Governo ad adottare entro 12 mesi uno o più decreti legislativi proprio "per definire una disciplina organica relativa all'utilizzo di dati, algoritmi e metodi matematici per l'addestramento di sistemi

⁶⁷ In tal senso M. CAPPAL, *Intelligenza artificiale e governance Intelligenza artificiale e protezione dei dati personali nel d.d.l. n. 1146: quale governance nazionale?*, in *Federalismi.It, Focus Lavoro persona tecnologia*, 2024, n. 30, p. 190.

⁶⁸ Analogamente all'impostazione del DGA che incoraggia il ricorso alle tecniche della pseudonimizzazione, anonimizzazione e cifratura nella circolazione dei dati.

⁶⁹ L. TEBANO, *Poteri datoriali e dati biometrici nel contesto dell'AI Act*, in *Federalismi.it, Focus Lavoro Persona Tecnologia*, 2023, n. 25, pp. 198 ss.; C. LAZZARI, P. PASCUCCHI, *Sistemi di IA, salute e sicurezza sul lavoro: una sfida al modello di prevenzione aziendale, fra responsabilità e opportunità*, in *RGL*, 2024, n. 4, pp. 587 ss.

⁷⁰ Per notazioni critiche sull'insufficiente apparato di garanzie collaterali predisposto dal Regolamento con riferimento ai sistemi di riconoscimento delle emozioni cfr. L. TEBANO, *Intelligenza artificiale e datore di lavoro: scenari e regole*, in *DML*, 2024, 3, p. 462.

di intelligenza artificiale senza obblighi ulteriori, negli ambiti soggetti al regolamento (UE) 2024/1689, rispetto a quanto già ivi stabilito” (art. 16). Inoltre la l. l. 132, in relazione a specifici interessi pubblici preminenti – in particolare la tutela della salute - apre la strada ad una specializzazione delle regole di protezione dei dati personali nell’ambito delle applicazioni di IA in campo medico e sanitario. Per fini di ricerca e sperimentazione scientifica, in ragione dell’interesse pubblico qualificato, è prevista una semplificazione dell’informativa agli interessati ed è ammesso il riuso secondario dei dati rispetto ai fini della raccolta iniziale, previa la non diretta identificazione delle persone. Così come è consentito il trattamento per fini di anonimizzazione, pseudonimizzazione e sintetizzazione dei dati personali particolari (art. 8).

Anche a livello europeo, nell’ambito degli spazi di sperimentazione normativa (*sandbox* regolative)⁷¹ di sistemi di IA per la realizzazione di servizi di interesse pubblico, l’art. 59 prevede espressamente la possibilità di derogare al limite del riutilizzo dei dati previsto di norma dal GDPR. In particolare i dati personali legalmente raccolti “per altre finalità” possono essere trattati per finalità diverse da quelle iniziali, esclusivamente ai fini dello sviluppo, dell’addestramento e delle prove di determinati sistemi di IA sviluppati per salvaguardare un interesse pubblico rilevante – come “l’efficienza e la qualità della pubblica amministrazione e dei servizi pubblici” - da parte di un’authority pubblica o di un’altra persona fisica o giuridica. L’ulteriore trattamento, in particolare, è legittimo nel rispetto di una serie di garanzie, quali: l’adozione di meccanismi di monitoraggio dell’impatto sui diritti fondamentali; la conservazione dei dati in un ambiente di trattamento funzionalmente separato, isolato e protetto; la non condivisione dei dati personali al di fuori dello spazio di sperimentazione; l’adozione di adeguate misure tecniche e organizzative e successiva cancellazione al termine della sperimentazione; la conservazione dei log del trattamento dei dati personali per la durata della partecipazione allo spazio di sperimentazione.

L’insieme dei dati normativi europei ed interni appena richiamati rende evidente il valore strategico e la relativa specificità della disciplina del trattamento dei dati personali nell’ambito di sistemi di IA, in larga parte ancora da esplorare e sviluppare. Certo è che le prime forme di adattamento hanno trovato un terreno fertile nel campo medico e sanitario, ma analoghe esigenze di bilanciamento si riscontrano, con non minore forza, in altri rilevanti campi di pubblico interesse dove sono in gioco valori di rango costituzionale, come il diritto al lavoro, il cui godimento è ormai condizionato dall’efficienza dei servizi per il lavoro e delle PAL. Anche in questo settore, allora, occorrerà trovare al più presto nuovi punti di bilanciamento tra valori giuridici fondamentali concorrenti: la protezione dei dati personali, il diritto al

⁷¹ La l. n. 132/2025 prevede in Italia un rinvio a AgID e ACN per “l’istituzione e la gestione congiunta di spazi di sperimentazione finalizzati alla realizzazione di sistemi di intelligenza artificiale conformi alla normativa nazionale e dell’Unione europea” (art. 20, c.1, lett. c) e rinvia alla decretazione delegata il coinvolgimento del sistema dell’università e ricerca nella realizzazione di “spazi di sperimentazione normativa in collaborazione con il sistema produttivo” (art. 24, c. 1, lett. l).

lavoro, la non discriminazione e le pari opportunità, l'innovazione tecnologica utile ad accrescere la qualità e l'efficacia di servizi pubblici e di interesse generale.

5. Nuove prospettive di bilanciamento degli interessi in gioco nel sistema multi-Authority della IA

La scelta politica europea di dotare l'IA di un proprio apparato di governance di riferimento è molto chiara. Si è voluta evitare l'istituzione di un'Agenzia o Autorità indipendente europea, così come si è voluta evitare la ridondanza sulla materia della IA dell'Autorità di Garanzia dei dati personali, mentre si è preferito costituire un apposito Ufficio interno alla Commissione dedicato alla IA⁷².

A livello interno questa scelta è stata replicata con la l. 132/2025 che, anziché costituire una nuova autorità indipendente ha preferito individuare le autorità nazionali dell'intelligenza artificiale in due Agenzie governative: l'AgID (Agenzia per l'Italia digitale) e l'ACN (Agenzia per la Cybersicurezza Nazionale).

La prima ha competenze - oltre che di promozione e sviluppo della IA - in materia di notifica, valutazione, accreditamento e monitoraggio dei soggetti certificatori dei sistemi di IA; la seconda ha competenze in materia di vigilanza, poteri sanzionatori e garanzia della cybersicurezza.

Il tentativo è quello di tenere l'IA sotto l'ombrello degli organismi competenti in materia di digitalizzazione del sistema Paese, cybersecurity e sicurezza nazionale e di non cedere ai tentativi del Garante della protezione dei dati personali di rivendicare a sé la competenza *naturale* sulla materia dell'IA in considerazione del suo impatto sui diritti fondamentali⁷³. La contesa di competenze era iniziata da tempo (sin dalla prima Segnalazione del Garante al Parlamento e al Governo sull'Autorità per l'IA del 25 aprile 2024 immediatamente successiva all'approvazione dell'AI ACT⁷⁴), ma alla fine la l. 132 ha fatto una scelta di campo ben precisa, pur lasciando ferme "le competenze, i compiti e i poteri del Garante per la protezione dei dati personali e dell'Autorità per le garanzie nelle comunicazioni, quale Coordinatore dei Servizi Digitali" (art. 20, c. 4) e prevedendo l'acquisizione preventiva del parere del Garante per l'emanazione della decretazione delegata.

E' indicativo di questo approccio il fatto che la l. 132 preveda la costituzione presso la Presidenza del Consiglio dei Ministri del Comitato per assicurare il coordinamento e la collaborazione ed ogni opportuno raccordo tra AgID e ACN con le pubbliche amministrazioni e le autorità indipendenti, cui sono invitati

⁷² F. BASSAN, M. RABITTI, *L'applicazione dell'AI Act in Italia e la tutela del consumatore. Il ruolo delle autorità indipendenti?*, in *Federalismi.It, Focus Lavoro Persona Tecnologia*, 2024, n. 30, pp. 250 ss.

⁷³ L. TEBANO, *Poteri datoriali e dati biometrici nel contesto dell'AI Act*, cit., p. 211; M. PERUZZI, *LA e obblighi datoriali di tutela del lavoratore: necessità e declinazioni dell'approccio riskbased*, in *Federalismi.it Lavoro Persona Tecnologia*, 2024, n. 30, pp. 225 ss.

⁷⁴ F. LAMBERTI, *La proposta di regolamento UE sull'Intelligenza Artificiale alla prova della privacy*, in *Federalismi.it Lavoro Persona Tecnologia*, paper 29 giugno 2022.

a partecipare anche CONSOB, Banca D'Italia e IVASS, ma non il Garante della protezione dei dati personali (art. 20, c. 3).

Inutile nascondere, però, che uno dei punti nodali e più critici dell'immissione della IA in qualsiasi contesto d'uso e specialmente nei luoghi di lavoro e nel mercato del lavoro, riguarda inevitabilmente la questione dell'equilibrio tra rispetto della *privacy*, spinta all'innovazione digitale e sicurezza cibernetica, laddove i sistemi di IA implicano la gestione, l'uso e il riuso di masse crescenti di dati, anche personali dei lavoratori. Il problema della intersezione tra nuclei normativi con ispirazioni differenti si sta già ponendo, del resto, con profili di particolare criticità per l'attuazione della normativa NIS II in materia di *cybersecurity*. Il rispetto dei vincoli della normativa *privacy* con riferimento al principio di minimizzazione del trattamento dei dati e la limitazione temporale di conservazione dei dati di log pone seri problemi operativi quotidiani per i datori di lavoro pubblici e privati chiamati a comprendere, banalmente, in quale misura le esigenze di sicurezza e cybersicurezza possano consentire di adattare la normativa *privacy* alle finalità specifiche di protezione del patrimonio aziendale e di sicurezza nazionale. In un contesto, è bene ricordarlo, in cui gli orientamenti del Garante *privacy* sono molto restrittivi e portano, ad esempio, a limitare la conservazione dei metadati delle e-mail aziendali per un periodo di norma non superiore ai 21 giorni⁷⁵ e a ritenere non proporzionata, anche a motivi di sicurezza informatica, la conservazione dei log di navigazione internet dei dipendenti superiore a 90 giorni⁷⁶.

In tale quadro, prima di immaginare futuribili sviluppi applicativi della IA ai contesti di lavoro e delle politiche attive, sarebbe utile affrontare questioni di base, che sono di estrema urgenza eppure, purtroppo, ancora senza risposta univoca. E' essenziale quindi che nella implementazione operativa della l. 132 possano essere sciolte questioni con cui tutti gli operatori pubblici e privati del mercato del lavoro sono chiamati oggi a confrontarsi e rispetto ai quali l'adozione di qualsiasi sistema di IA, anche il più semplice, risulta inevitabilmente foriera di molte incertezze. C'è da augurarsi, dunque, che l'Osservatorio dell'art. 12 l. 132 possa farsi carico della questione delle interferenze e del coordinamento tra normativa di protezione dei dati, normativa giuslavoristica, normativa sulla *cybersecurity* e impieghi legittimi della IA nei contesti di lavoro e nel mercato del lavoro.

Del resto la il legislatore italiano mostra di essere ben consapevole del difficile equilibrio tra *privacy*, *cybersecurity* e innovazione digitale, come testimoniano i diversi richiami incrociati al Codice *Privacy* presenti nella l. 132/2025, ora per salvaguardarne i principi, ora per tentarne un adattamento, che tuttavia avrà esiti ancora tutti da verificare e da mettere alla prova di resistenza dell'Autorità Garante per la protezione

⁷⁵ V. il Documento di indirizzo del Garante del 6 giugno 2024 in materia di programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati.

⁷⁶ V. il Provvedimento del Garante n. 243 del 29 aprile 2025 verso la regione Lombardia sull'eccessiva conservazione dei metadati di posta elettronica, dei log di navigazione internet e dei dati raccolti tramite sistemi di ticketing informatico).

dei dati personali, il cui potere, nonostante i tentativi di contingentamento della l. 132, trova fonte diretta nel GDPR e nello stesso AI Act. È a tutti nota, peraltro, la forte capacità di incidenza e condizionamento che il Garante della *privacy* ha esplicitato sull'operatività delle aziende e delle pubbliche amministrazioni negli ultimi anni. E come gli orientamenti e i provvedimenti del Garante costituiscano ormai per gli attori economici una fonte di indirizzo più incisiva della stessa autorità giudiziaria (anche per le pesanti sanzioni cui sono esposti gli operatori economici e gli enti pubblici).

Quindi il nodo che rimane aperto e che probabilmente decreterà le vere sorti della diffusione della IA in Italia e della propensione degli operatori pubblici e privati alla sperimentazione e all'investimento in sistemi di IA, è rappresentato dalla effettiva capacità del sistema di governance immaginato dalla l. 132 di trovare sintesi a monte, con norme e indirizzi chiari e univoci, in grado di infondere vere certezze al di là delle declamazioni di principio e senza rimettere al contenzioso giudiziario la formazione degli indirizzi interpretativi. Tutto dipenderà dalla capacità del Governo di farsi carico tempestivamente di quell'indispensabile coordinamento tra le molte *autorità* che ormai, a vario titolo, hanno modo di rivendicare proprie competenze e poteri in materia di IA⁷⁷.

6. Conclusioni

La cittadinanza sociale e lo stesso diritto al lavoro sono sempre più strettamente dipendenti da politiche attive del lavoro efficaci e anticipatorie dei bisogni delle persone e delle imprese. Nella società dei dati, la cittadinanza sociale è ormai anche una cittadinanza digitale, dove va preservata l'identità digitale e il diritto della persona alla corretta rappresentazione della propria identità digitale professionale.

Perché una nuova stagione di PAL possa prendere corpo è essenziale allora dare finalmente attuazione alla riforma del 2015, permettendo la *governance* e la circolazione dei dati relativi alle persone nel mercato del lavoro, la collaborazione informativa digitale, la tracciabilità, accessibilità e titolarità individuale dei dati. Oltre a resistenze politiche, istituzionali, operative, non c'è dubbio che la preoccupazione relativa al trattamento dei dati personali ha rappresentato un ostacolo alla circolazione del patrimonio informativo e alla stessa possibilità di riappropriazione da parte dell'individuo dell'accessibilità e piena disponibilità del proprio status professionale digitale.

Uno scatto di qualità nelle PAL può aversi, sulla scia del pacchetto digitale europeo e del *Data Governance Act*, a cui si deve l'affermazione del valore sociale - individuale e collettivo - della circolazione e del riutilizzo dei dati per finalità di pubblico interesse. In tale contesto il patrimonio informativo alla base delle politiche attive del lavoro dovrebbe essere trattato con uno sguardo più attento alle necessità di *data*

⁷⁷ F. BASSAN, M. RABITTI, *L'applicazione dell'AI Act in Italia e la tutela del consumatore. Il ruolo delle autorità indipendenti?*, cit.; M. CAPPAL, *Intelligenza artificiale e governance Intelligenza artificiale e protezione dei dati personali nel d.d.l. n. 1146: quale governance nazionale?*, in *Federalismi.It, Focus Lavoro persona tecnologia*, 2024, n. 30, pp. 186 ss.

governance imposte dal DGA. Si tratta quindi di ricercare nuovi punti di equilibrio tra i principi di protezione e di circolazione dei dati personali, tra GDPR e DGA, nel campo delle politiche attive del lavoro.

Contemporaneamente l'avvento dell'intelligenza artificiale e delle sue enormi potenzialità applicate al contesto delle politiche attive del lavoro richiede di trovare nuovi punti di bilanciamento tra i due plessi normativi del GDPR e dell'AI Act che, pur essendo integrati e complementari, richiedono una specializzazione delle classiche regole *privacy* per adattare al peculiare funzionamento dei sistemi di IA. E così il principio di minimizzazione del trattamento può essere cedevole rispetto all'esigenza di garantire un'adeguata rappresentatività quali/quantitativa dei dati per minimizzare gli errori e le distorsioni; i limiti al riutilizzo dei dati possono cedere il passo a sperimentazioni e innovazioni in ambienti controllati di *sandbox* normativa per il perseguimento di interessi pubblici. La *sentiment analysis* e l'inferenza delle emozioni sul luogo di lavoro sono legittime quando l'IA è indirizzata a migliorare la salute e sicurezza delle persone.

Si comprende allora come lo scambio dei dati e l'*empowerment* informazionale individuale, che dovrebbero caratterizzare un sistema di politiche attive moderne, non possono fare a meno di porsi il problema dei nuovi bilanciamenti e possibili integrazioni tra GDPR, DGA e AI Act. Solo così è possibile garantire il dinamismo dei dati nella società contemporanea, senza gerarchizzazioni preconcepite di valori. Ciò dovrebbe avvenire auspicabilmente mediante un intervento coordinato di orientamento *preventivo* da parte delle diverse autorità e agenzie governative che hanno poteri e funzioni concorrenti su queste materie (GPDP, AgId, ACN).

Tutto ciò richiede altresì di approfondire, in ottica lavoristica e di mercato del lavoro, le tecniche e i dispositivi - crittografia, anonimizzazione, pseudonimizzazione, ecc. - attraverso le quali risulta possibile soddisfare e mettere in bilanciamento i diversi principi in gioco. Ma soprattutto richiede di spostare il fuoco dell'attenzione dalla protezione dei dati, all'autodeterminazione informativa delle persone interessate che, nel mercato del lavoro, significa anche valorizzare adeguatamente l'ostensibilità della memoria professionale, la sua ricchezza storica e la sua portabilità, così come estrarre valore sociale dai dati in possesso degli attori della rete nazionale delle politiche del lavoro.

Allo stesso tempo, per favorire una maturazione dell'autodeterminazione informativa come espressione della cittadinanza sociale digitale (al di là ed oltre l'esercizio del diritto di accesso e di controllo sui dati), occorre riflettere su nuove proiezioni del *potere* della persona nel controllo della qualità dei dati di input nei sistemi di IA, come forma di tutela preventiva, onde evitare possibili errori, asimmetrie e discriminazioni algoritmiche.



E a tal riguardo appare forse ineludibile guardare con favore ad un rafforzamento di forme collettive o aggregate di tutela degli interessi, superando l'impostazione tipicamente "individualistica" che accomuna GDPR, AI Act e lo stesso sistema giuridico-fattuale delle PAL, ove la dimensione dell'interesse collettivo è ancora scarsamente sviluppata⁷⁸. Si tratta, cioè, di ragionare su possibili (nuovi) ruoli e funzioni che possono svolgere il sindacato o altre organizzazioni di rappresentanza di interessi diffusi o collettivi⁷⁹, per un rinnovamento reale del funzionamento del mercato del lavoro e delle politiche attive nei nuovi scenari digitali.

⁷⁸ N. DELEONARDIS, *L'organizzazione sindacale e il mercato del lavoro*, Adapt University Press, Bergamo, 2024.

⁷⁹ F. FAINI, *Diritto all'esistenza digitale*, in *BioLaw Journal, Rivista di BioDiritto*, 2019, n. 3, p. 107; ID., *Big data, algoritmi e diritto*, in *DPCE online*, 2019, n. 3, p. 1879; G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, *cit.*