
IA GENERATIVA E IL FUTURO DEL LAVORO: SFIDE TECNOLOGICHE E IMPLICAZIONI DI DIRITTO DEL LAVORO

SILVIA CIUCCIOVINO, ALESSANDRO TOSCANO
Università degli Studi Roma Tre, LabChain

19 febbraio 2025
Intelligenza artificiale e lavoro

IA GENERATIVA E IL FUTURO DEL LAVORO: IMPLICAZIONI DI DIRITTO DEL LAVORO

SILVIA CIUCCIOVINO

**Università degli Studi Roma Tre, LabChain
Dipartimento di Economia**

19 febbraio 2025

Intelligenza artificiale e lavoro

SOMMARIO

- Classificazione dei sistemi di IA e finalità d'uso
- Le fonti multilivello: AI ACT e sistema normativo nazionale
- Le applicazioni vietate e i sistemi ad alto rischio in ambito lavoristico
- Gli obblighi del datore di lavoro-deployer dei sistemi di IA
 - La formazione/alfabetizzazione
 - La trasparenza
 - I dati di input
 - I diritti di informazione sindacale
- I codici di condotta

Classificazione dei sistemi di IA e finalità d'uso

QUALI USI DELLA IA

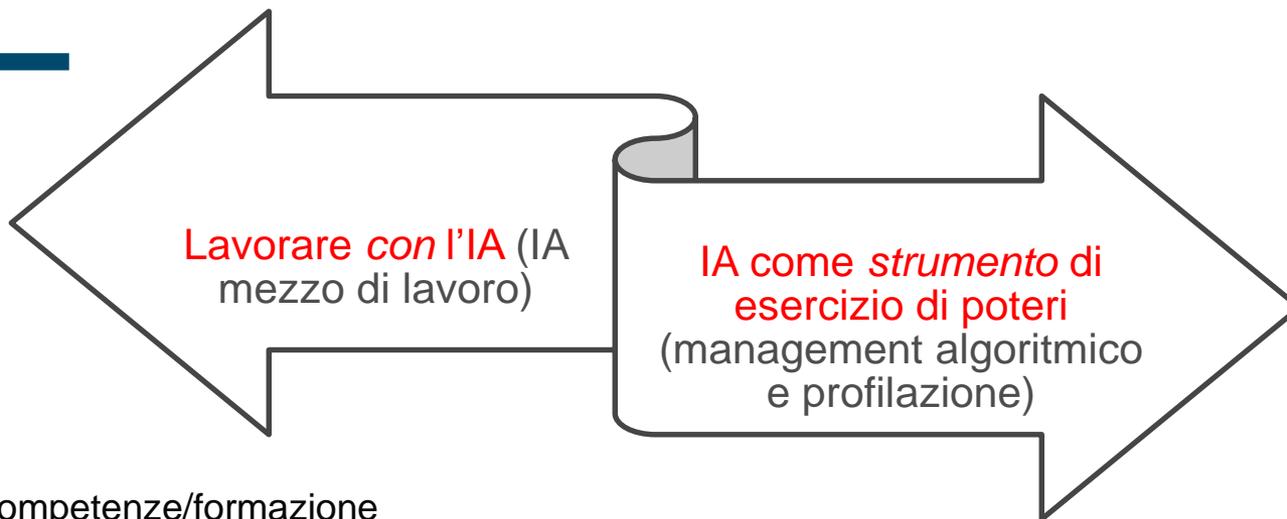
Lavorare con l'IA
(IA mezzo di lavoro)

- Strumenti digitali intelligenti per l'esecuzione della prestazione
- Co-robot (robot che lavorano in stretta prossimità degli umani)
- Applicazioni intelligenti per gestione del ciclo produttivo o fasi di lavorazione o manutenzione
- Applicazioni e dispositivi per la sicurezza sul lavoro
- DPI intelligenti

IA come strumento di esercizio di poteri
(management algoritmico)

- Strumenti per gestire turni, team, squadre di lavoro
- Per gestire le carriere
- Per valutare performance
- Per controllare il processo produttivo
- Per gestire lo sviluppo professionale e formativo
- Per politiche retributive e di incentivazione
- People analytics e smistamento carichi lavoro

QUESTIONI DI DIRITTO DEL LAVORO IN BASE AGLI USI DELLA IA



Competenze/formazione

Mansioni

Diligenza

Collaborazione

Obbedienza

Salute e sicurezza

2087 c.c.

Responsabilità civile vs terzi

Controllo tecnologico

Dati personali

Trasparenza di interazione

Limiti al potere direttivo e di controllo

Arbitrarietà /razionalità decisioni

Procedimentalizzazione poteri

Discriminazione algoritmica

Trasparenza delle decisioni e di funzionamento

Protezione dignità, personalità morale

Controllo tecnologico

Spiegabilità/contestazione/revisione umana decisione algoritmica

Dati personali

SISTEMI AUTOMATIZZATI VS INTELLIGENZA ARTIFICIALE

automatismo *della decisione*
datoriale

vs

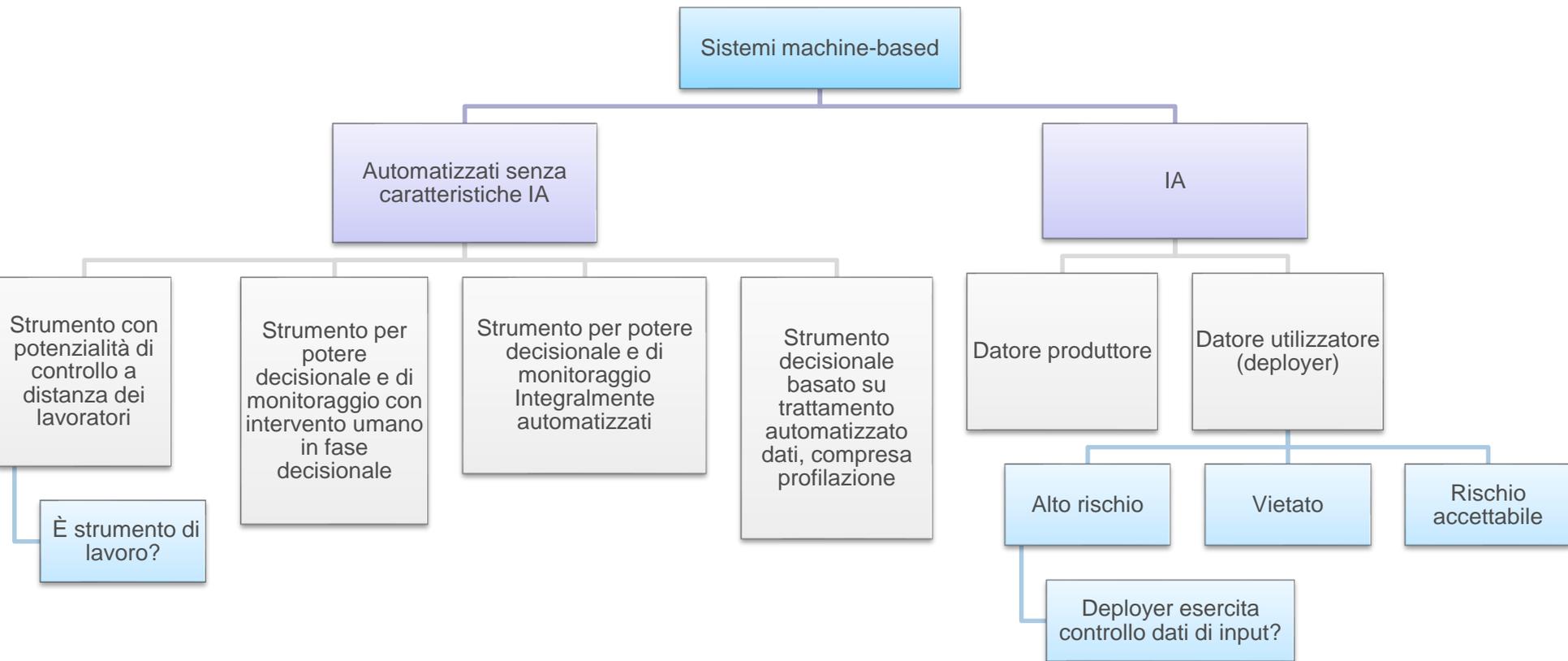
automatismo *del sistema* algoritmico

**Sistemi decisionali e di
monitoraggio integralmente
automatizzati** (Art. 1 bis D.
Lgs 152/1997)

Intelligenza artificiale
(Reg. UE 2024/1689)

capacità inferenziale
autoapprendimento
adattività senza intervento
umano

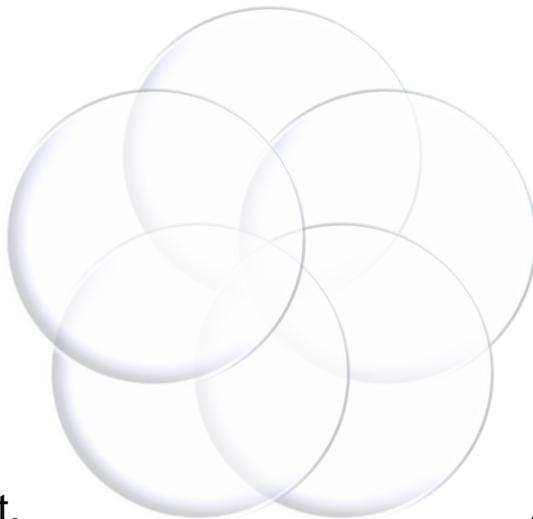
ORIENTARSI TRA I SISTEMI MACHINE-BASED (FATTISPECIE)



Le fonti multilivello: AI ACT e sistema normativo nazionale

IA E NORMATIVA MULTILIVELLO

AI ACT (Reg. UE
2024/1689)



Normativa
antidiscriminatoria e salute e
sicurezza

Controllo
tecnologico (art.
4 l. 300/70)

GDPR (Reg UE
2016/679)

Decreto
Trasparenza
(art. 1bis d. lgs.
152/1997)

Fonti che

a) **Limitano poteri:**

- organizzativi/manageriali,
- direttivi
- controllo
- trattamento dati personali

b) Impongono obblighi di **trasparenza individuale**

c) Procedimentalizzano **sindacalmente**
(informazione,
consultazione)

l'AI ACT **pone obblighi nuovi**
al datore di lavoro rispetto alla
normativa lavoristica già
applicabile?

IA E NORMATIVA MULTILIVELLO

Il Regolamento (UE) 2024/1689 fa sistema con altre fonti:

- Il GDPR
- Le norme dei Trattati
- La Carta dei diritti fondamentali dell'Unione, con cui deve integrarsi
- Il Diritto del lavoro nazionale
- Il Regolamento **rinvia alle condizioni più favorevoli** ai lavoratori che l'UE o i **singoli Stati membri** possono adottare per via legislativa, amministrativa o contrattuale collettiva (articolo 2, § 11)

ENTRATA IN VIGORE REGOLAMENTO UE

Dal 2 agosto 2024 codici di condotta volontari

Dal **2 febbraio 2025**:

- **divieti** relativi a pratiche inaccettabili (riconoscimento emozioni sul luogo di lavoro)
- obbligo di **alfabetizzazione** in materia di IA (anche per datori di lavoro)

Dal **2 agosto 2025**:

- Stati membri individuano autorità competenti, organismi notifica della conformità, certificazione
- Requisiti sistemi per finalità generali
- Governance europea
- **Sanzioni**

Dal **2 agosto 2026**:

- Entrata in **vigore generalizzata**, tranne che per **sistemi ad alto rischio** per i quali entrata in vigore decorre dal **2 agosto 2027**

SANZIONI VIOLAZIONE REG. IA (DA PREVEDE A LIVELLO NAZIONALE)

35 mil € o 7% fatturato globale:
Violazione divieti

15 mil € o 3% fatturato globale:
Violazione obblighi dei deployer (art. 26)
Violazione obblighi di trasparenza per fornitori e deployers (art.50)

BASE GIURIDICA DEL REG. UE 2024/1689 PRODUTTORI E DEPLOYERS

- IA trattata come «prodotto» (art. 16 e 114 UE), non riguarda «diritti ed interessi dei lavoratori dipendenti»
- Focalizzato sui requisiti dei sistemi di IA: obblighi sui produttori
- Deployer datori di lavoro, in quanto utilizzatori, interessati in via secondaria

La **FRIA** (*fundamental rights impact assessment*) è effettuata dal produttore. E' richiesta per il deployer soltanto per alcuni sistemi ad alto rischio da parte della PA o enti privati che erogano servizi pubblici

n.b. l'art. 1 bis prevede a carico del datore una valutazione di impatto e un sistema di gestione della qualità dei sistemi automatizzati

DEPLOYER - DATORE DI LAVORO

- ❑ Il **deployer deve sempre valutare la finalità d'uso** dell'IA, contestualizzando ai casi d'uso le istruzioni ricevute dai fornitori al fine di:
 - **classificarla correttamente** (rispetto alla classificazione del produttore), anche tenendo conto di come l'output si incorpora nei processi decisionali
 - verificare l'area di esenzione del divieti qualora si tratti di sistemi finalizzati alla **tutela della salute e sicurezza**

Verifica preliminare posizione del datore di lavoro rispetto ai sistemi di IA:

- ***Il datore di lavoro è solo deployer?***
- ***Il datore di lavoro esercita il controllo sui dati di input?***

OBBLIGHI DEL DEPLOYER NELLA VALUTAZIONE DI IMPATTO

□ Nei soli sistemi ad alto rischio, il deployer deve:

- **Monitorare il funzionamento** del sistema sulla base delle istruzioni per l'uso e informare i fornitori di eventuali anomalie
- Valutare la **qualità dei dati** eventualmente immessi: rappresentatività e pertinenza (quindi il potenziale discriminatorio diretto o indiretto dei dati)
- Segnalare al fornitore **eventuali rischi per la salute o la sicurezza o per i diritti fondamentali** delle persone che dovesse rilevare in fase di utilizzazione del sistema e sospenderne l'uso
- Per i dati personali: **deve integrare la DPIA** (*data protection impact assessment*) - valutazione di impatto sui dati personali ex art. 35 GDPR - facendo uso delle informazioni fornite dal fornitore aggiornamento/integrazione trattamento dati ai sensi della normativa privacy

Le applicazioni vietate e i sistemi ad alto rischio in ambito lavoristico

L'IA APPLICATA ALLE RISORSE UMANE NELL'AI ACT



APPLICAZIONI VIETATE DI RILIEVO LAVORISTICO

19 febbraio 2025
Intelligenza artificiale e lavoro

DIVIETO UTILIZZO AI PER RICONOSCIMENTO EMOZIONI SUL LUOGO DI LAVORO

Riconoscimento delle emozioni sul luogo di lavoro, **salvo che per motivi medici o di sicurezza**

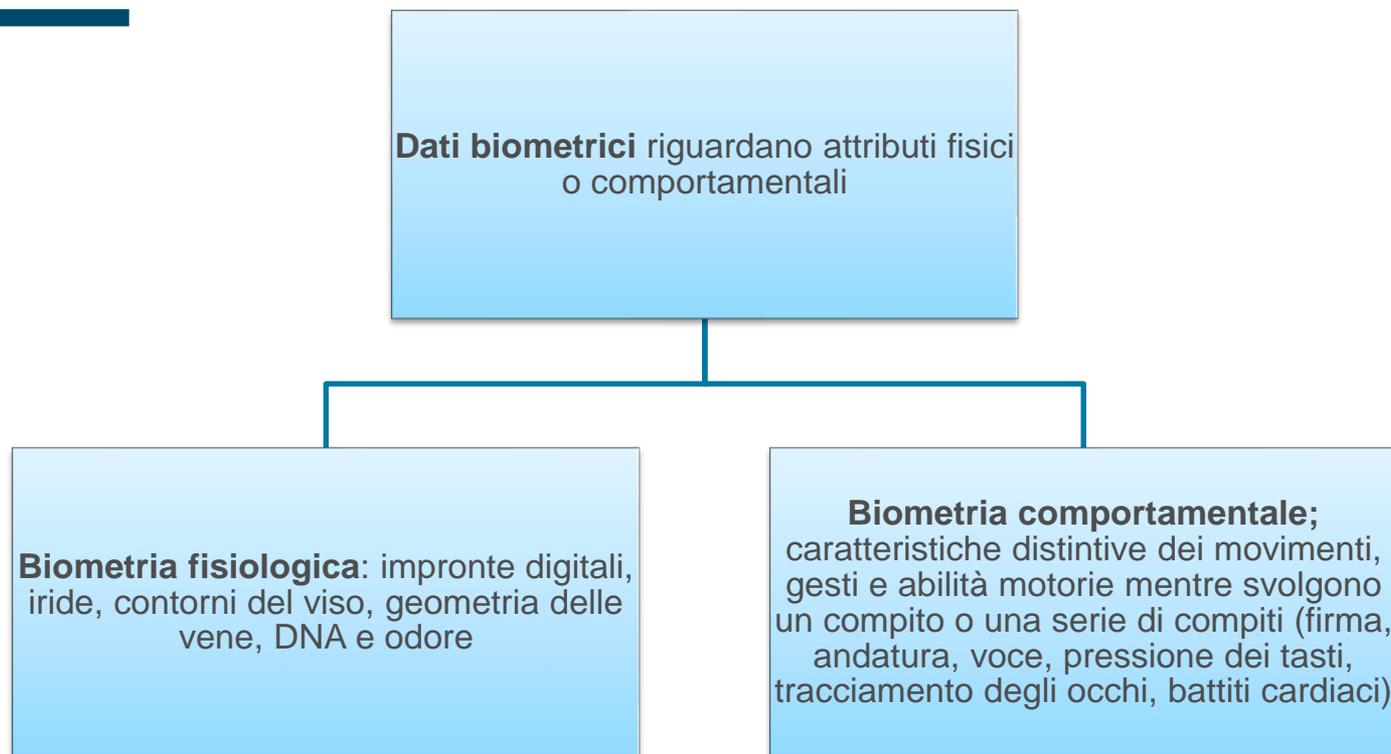
Riguarda soltanto sistemi basati su rilevazione **dati biometrici**

La nozione si riferisce a emozioni o intenzioni quali **felicità, tristezza, rabbia, sorpresa, disgusto, imbarazzo, eccitazione, vergogna, disprezzo, soddisfazione e divertimento**

Non comprende stati fisici, quali dolore o affaticamento; ad es. per prevenire gli incidenti

Non comprende semplice individuazione di espressioni, gesti o movimenti, a meno che non siano utilizzati per inferire emozioni (es. espressioni facciali aggrottamento delle sopracciglia sorriso, movimento mani, braccia testa, caratteristiche della voce)

DIVIETO UTILIZZO AI PER RICONOSCIMENTO EMOZIONI SUL LUOGO DI LAVORO



Es. Un sistema di intelligenza artificiale che deduce emozioni dalla pressione dei tasti, espressioni facciali, posture o movimenti del corpo si basa su dati biometrici e rientra nell'ambito del divieto

DIVIETO UTILIZZO AI PER RICONOSCIMENTO EMOZIONI SUL LUOGO DI LAVORO

Esempi vietati:

- L'utilizzo di webcam e sistemi di riconoscimento vocale da parte di un call center per tracciare le emozioni dei propri dipendenti, come la rabbia
- Un sistema di IA che deduce che un dipendente è infelice, triste o arrabbiato con i clienti (ad esempio dai gesti del corpo, da un'espressione accigliata o dalla mancanza di un sorriso)

Esempi consentiti:

- I sistemi di riconoscimento vocale da parte di un call center per monitorare le emozioni dei clienti, come la rabbia o l'impazienza (ad esempio per aiutare i dipendenti a gestire alcuni clienti arrabbiati)
- I sistemi di riconoscimento delle emozioni sono consentiti solo a scopo di formazione personale, se i risultati non sono condivisi con i responsabili delle risorse umane e purchè non abbia alcun impatto sul rapporto di lavoro (non possono influire sulla valutazione, sulla promozione ecc. della persona formata)

SISTEMI AD ALTO RISCHIO DI RILIEVO LAVORISTICO

19 febbraio 2025
Intelligenza artificiale e lavoro

SISTEMI AD ALTO RISCHIO NEL CAMPO RISORSE UMANE

ALLEGATO III



La classificazione di rischio spetta al produttore ma dipende anche dal ruolo della IA nel processo decisionale del deployer

SISTEMI AD ALTO RISCHIO NEL CAMPO RISORSE UMANE

ALLEGATO III

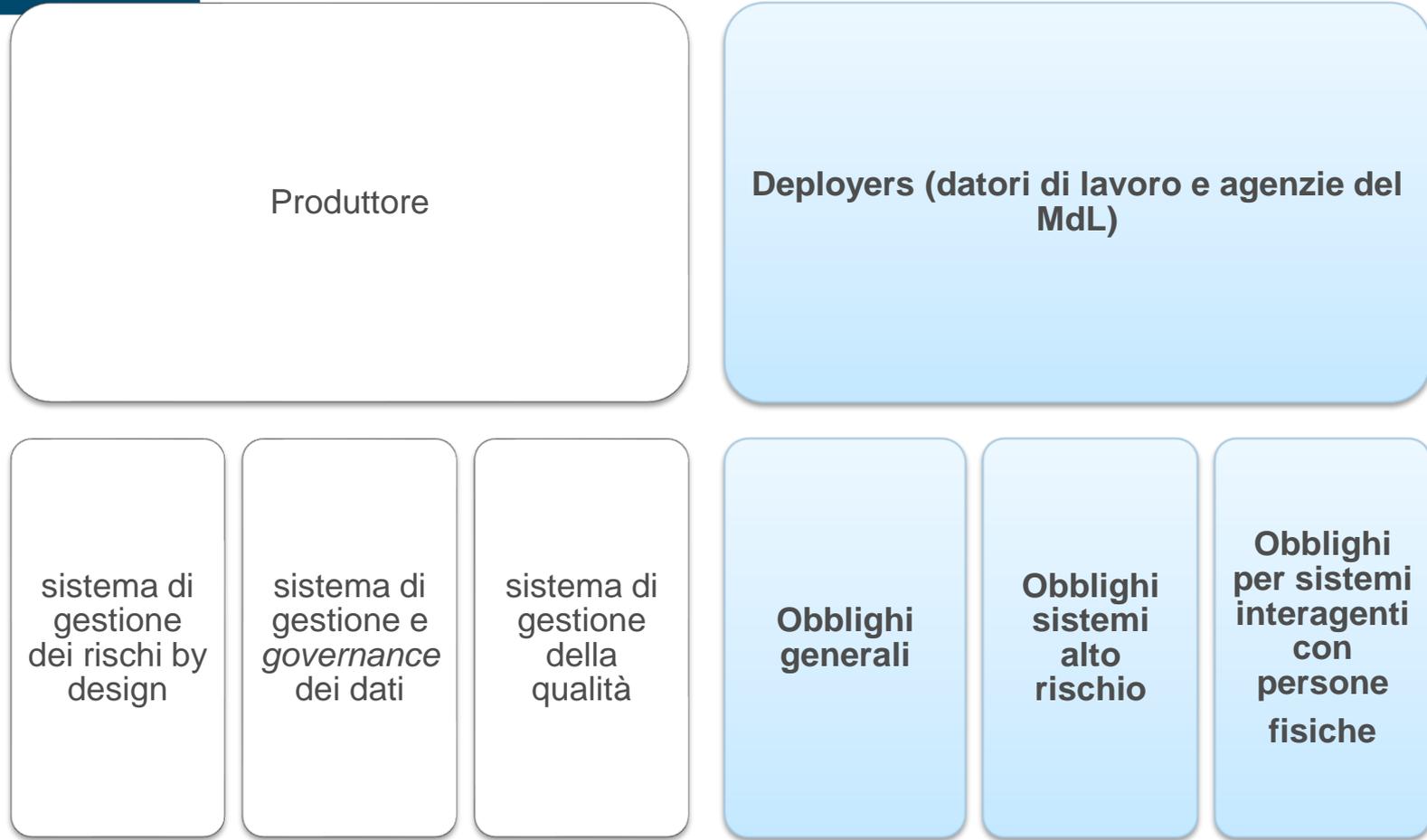
Deroga alla classificazione come ad alto rischio se il ruolo della IA nel processo decisionale del deployer è limitato:



- a) esegue un compito procedurale limitato
- b) migliora il risultato di un'attività umana precedentemente completata
- c) verifica schemi decisionali precedenti, ma non li modifica senza revisione umana
- d) esegue un compito preparatorio per una valutazione pertinente ai casi dell'All. III

Gli obblighi del datore di lavoro-deployer dei sistemi di IA

IA IN AMBITO LAVORATIVO: OBBLIGHI PER PRODUTTORE E PER DEPLOYER



OBBLIGHI PER DEPLOYER

Obblighi generali

alfabetizzazione
formazione personale
(art. 4), formazione
personalizzata per
consapevolezza e
corretto
funzionamento

Obblighi sistemi ad alto rischio

preventiva informazione
sindacale (art. 26, § 7)

informativa individuale
(articolo 26, § 11)

controllo sui dati di
input (art. 26, § 4)

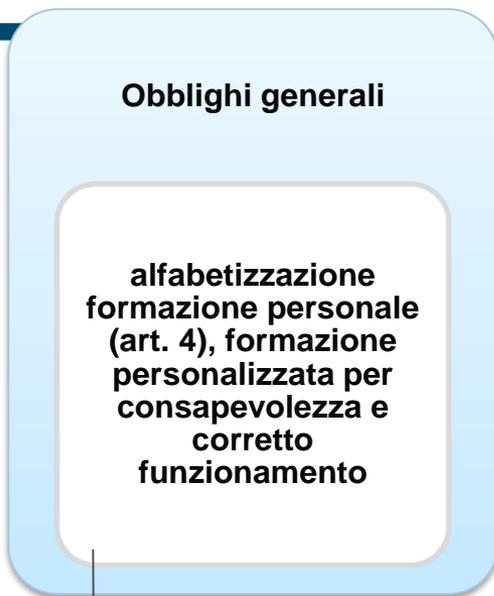
sorveglianza umana
(art. 14)

spiegabilità dei
processi decisionali
(art. 86)

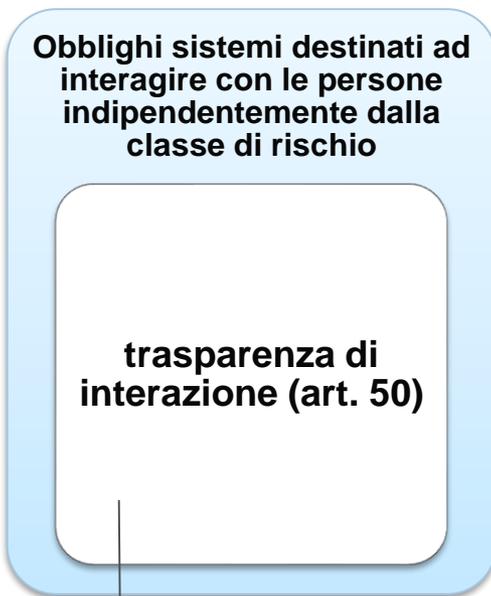
Obblighi per sistemi che interagiscono con le persone indipendentemente dalla classe di rischio

trasparenza di
interazione (art. 50)

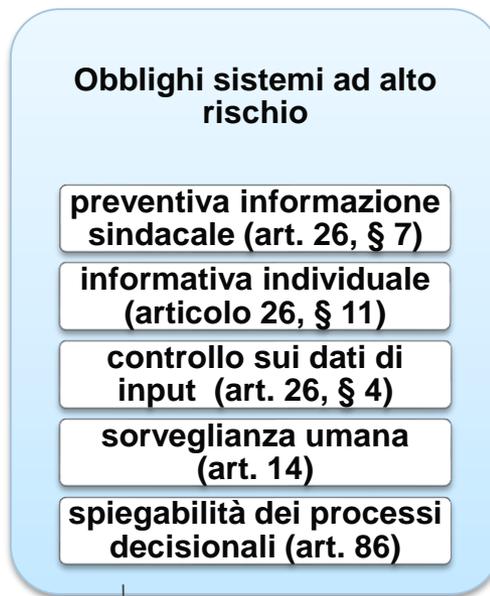
QUID PLURIS RISPETTO AGLI OBBLIGHI GIÀ PREVISTI DAL DIRITTO NAZIONALE?



Art. 2103 c.c.
Art. 2104 c.c.
Art. 2087 c.c.
Buona fede e
correttezza



Art. 1 bis
Art. 4 l. 300/1970



Art. 1 bis
D. Lgs. 25/2007
GDPR
Art. 4 l. 300/1970
Norme
antidiscriminatorie

QUID PLURIS RISPETTO AGLI OBBLIGHI GIÀ PREVISTI DAL DIRITTO NAZIONALE?

1. La formazione/alfabetizzazione
2. La trasparenza
3. I dati di input
4. I diritti di informazione sindacale

La formazione/alfabetizzazione

Obbligo generale di alfabetizzazione/formazione per tutti i sistemi IA a carico del deployer verso tutti gli utilizzatori finali, dipendenti e non

Dal 2 febbraio 2025

OBBLIGO DI ALFABETIZZAZIONE IN MATERIA DI IA

Articolo 4

I fornitori e i deployer dei sistemi di IA adottano misure per garantire nella misura del possibile un **livello sufficiente di alfabetizzazione** in materia di IA del **loro personale** nonché di **qualsiasi altra persona che si occupa del funzionamento e dell'utilizzo dei sistemi** di IA per loro conto, prendendo in considerazione **le loro conoscenze** tecniche, la loro esperienza, istruzione e formazione, nonché il **contesto** in cui i sistemi di IA devono essere utilizzati, e tenendo conto delle persone o dei gruppi di persone su cui i sistemi di IA devono essere utilizzati.

OBBLIGO DI ALFABETIZZAZIONE IN MATERIA DI IA

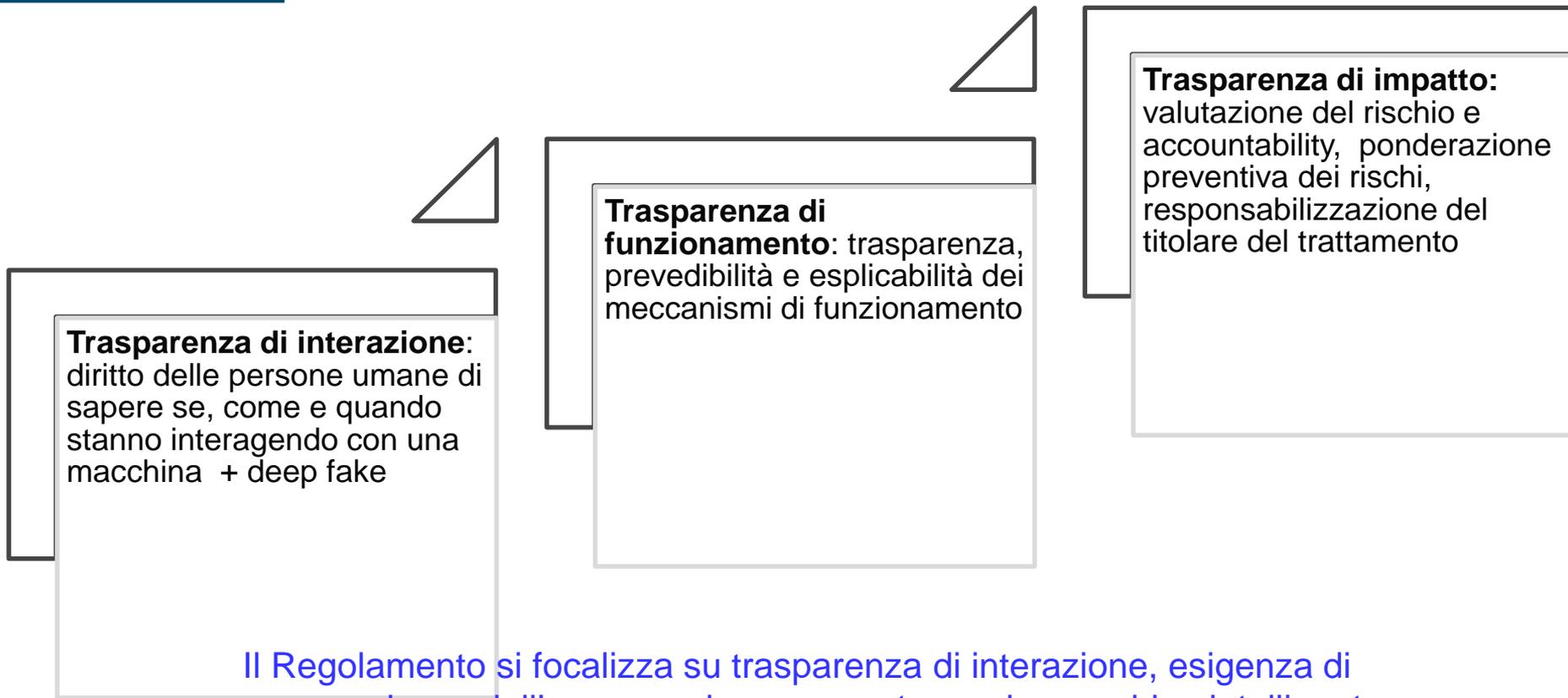
L'obbligo di formazione rappresenta una delle previsioni più significative dell'AI ACT:

- Formazione **personalizzata**: si deve tener conto caratteristiche individuali, istruzione, conoscenze, ruolo
- Formazione **contestualizzata**: deve tener conto delle finalità e del contesto
- Formazione **generalizzata**: tutti coloro che si occupano di funzionamento o utilizzo
- Formazione **sufficiente** a un uso consapevole

- In orario di lavoro?
- Cooperazione creditoria, il lavoratore deve collaborare, rientra negli obblighi di diligenza
- Attestazioni e tracciabilità
- Conseguenze mancata formazione? Esigibilità mansioni?

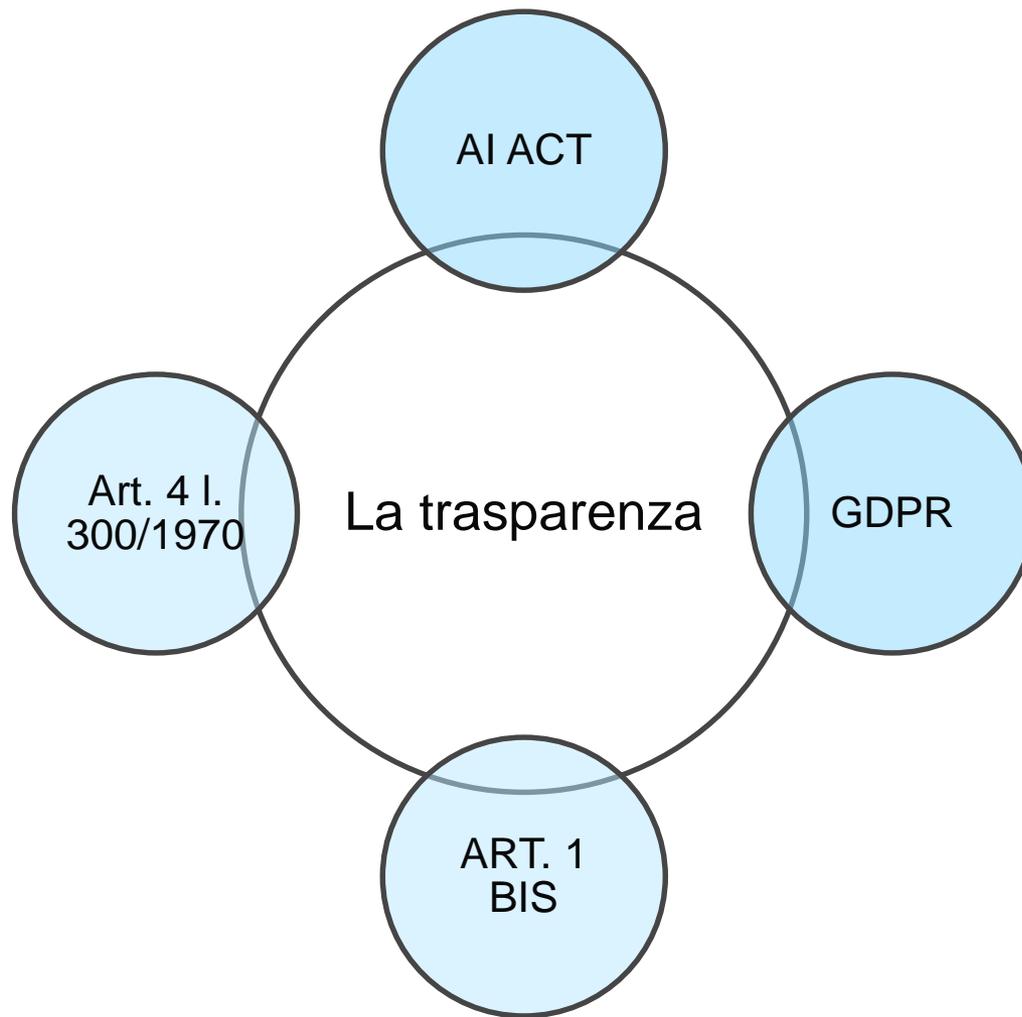
La trasparenza

GLI OBBLIGHI DI TRASPARENZA: QUALI ACCEZIONI?



Il Regolamento si focalizza su trasparenza di interazione, esigenza di consapevolezza dell'umano nel suo rapporto con la macchina intelligente (principi della dignità e dell'autonomia individuale)

GLI OBBLIGHI DI TRASPARENZA: QUALI FONTI?



GLI OBBLIGHI DI TRASPARENZA NELL'AI ACT

Trasparenza di funzionamento della IA del **produttore verso il deployer**:

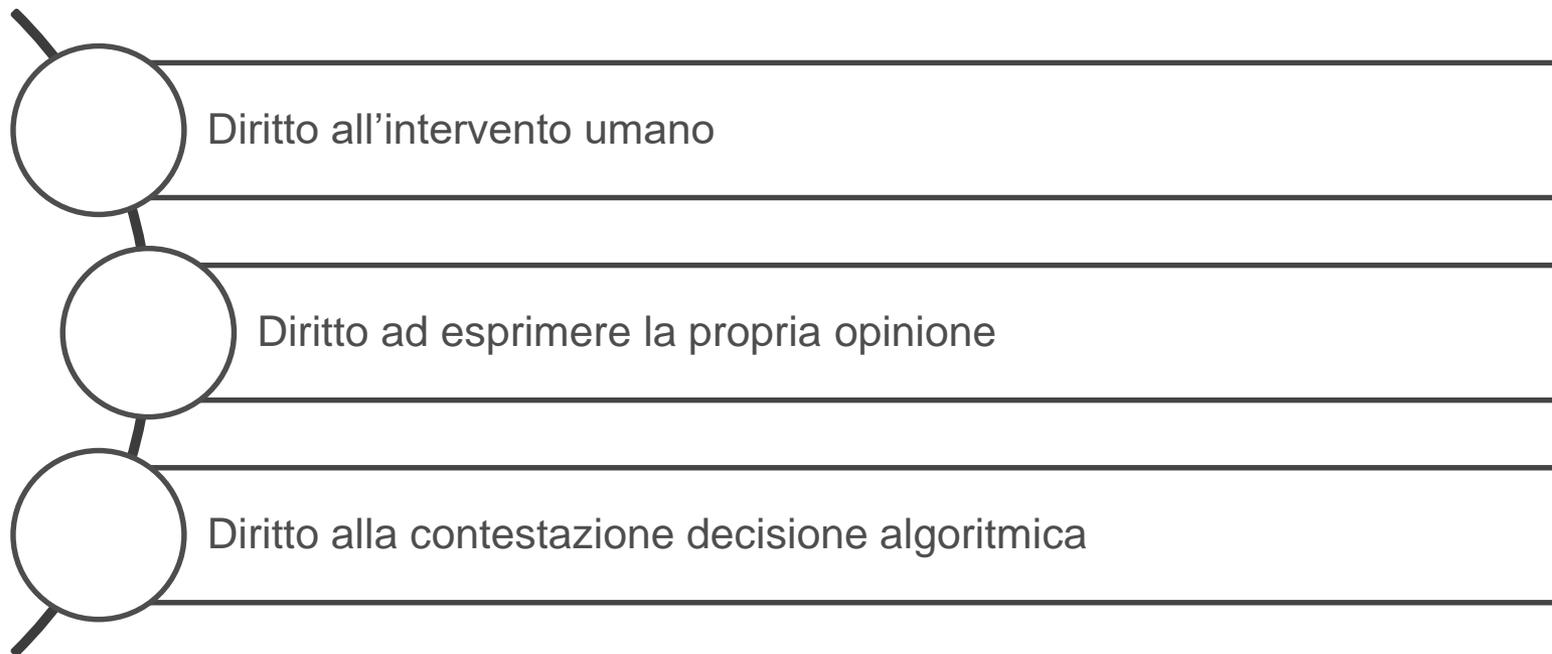
- “istruzioni d’uso” fornite dal produttore all’utente **trasparenza tecnica** (art. 13)
- il deployer deve essere messo in grado di interpretare gli output

Obblighi di trasparenza del **deployer vs utilizzatori finali**

- trasparenza di **interazione** per i sistemi destinati ad **interagire con le persone fisiche** (art. 50)
- trasparenza sul **funzionamento** del sistema nel caso di **categorizzazione biometrica** o riconoscimento emozioni (art. 50)
- trasparenza **deep fake** (art. 50)
- **spiegabilità nel caso lesione** diritto (sezione IV mezzi di ricorso) «diritto ad ottenere dal deployer spiegazioni chiare e significative sul ruolo del sistema di IA nella procedura decisionale e sui principali elementi della decisione adottata nel caso di diritti lesi da sistemi ad alto rischio» (art. 86)
- rinvio alle legislazioni nazionali e altre fonti europee applicabili-**GDPR**

GLI OBBLIGHI DI TRASPARENZA NEL GDPR

(Per i sistemi decisionali automatizzati, inclusa profilazione)



GLI OBBLIGHI DI TRASPARENZA NELL'ART. 4, L. 300/1970 (strumenti tecnologici per esigenze produttive o organizzative da cui derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori)

Accordo sindacale o autorizzazione INL, salvo che per «strumenti di lavoro» e registrazioni accessi/presenze

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

GLI OBBLIGHI DI TRASPARENZA NELL'ART. 1 BIS (sistemi integralmente automatizzati)



Diritto informazione individuale/collettiva- diritto alla spiegabilità

Obbligo di informazione preventiva prima dell'inizio (individuale e collettiva rsa/rsu o in mancanza territoriali di quelle nazionali)

Diritto di accesso

- Diritto accesso ai dati e a ulteriori informazioni (individuale, anche *per tramite* rsa o territoriali)

Accountability, analisi dei rischi e valutazione di impatto

- Diritto informativa cybersicurezza e trattamento dati
- Istruzioni sulla sicurezza dei dati e aggiornamento del registro dei trattamenti

Diritto all'aggiornamento

- Informazione scritta (individuale+ collettiva) delle modifiche entro 24 ore se incide su condizioni di svolgimento rapporto

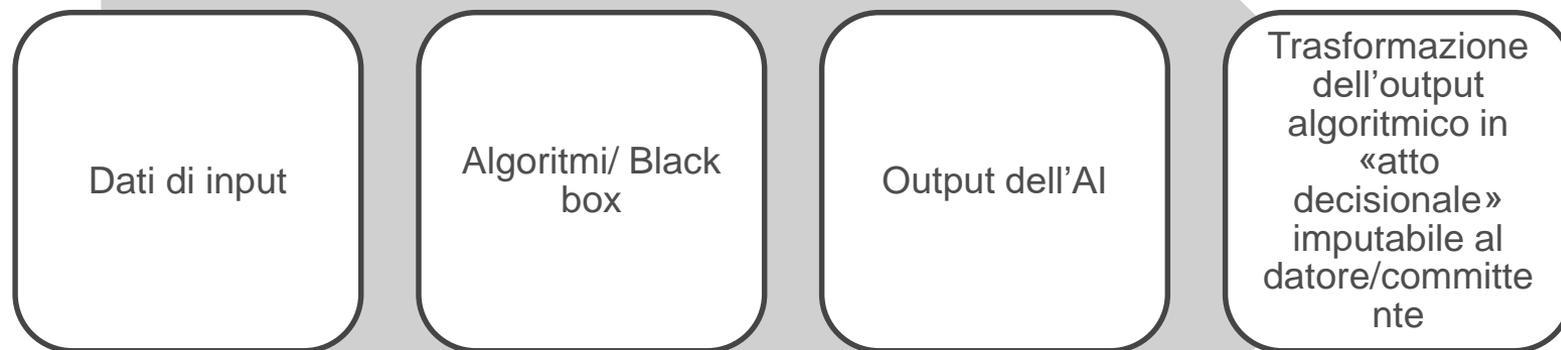
GLI OBBLIGHI DI TRASPARENZA NELL'ART. 1 BIS (sistemi integralmente automatizzati)

Oggetto informativa vs singoli lavoratori e loro rappresentanze sindacali:

- utilizzo
- incidenza
- categorie di dati
- parametri
- logica e parametri principali per programmare e addestrare
- misure di controllo
- processi di correzione e responsabile del sistema di gestione della qualità
- livello di accuratezza, robustezza e cybersicurezza
- metriche utilizzate per misurare tali parametri
- impatti potenzialmente discriminatori delle metriche stesse

Informativa preventiva e iterativa

GLI OBBLIGHI DI TRASPARENZA NELL'ART. 1 BIS (sistemi integralmente automatizzati)



Dilemma: controllo sui criteri di funzionamento della AI «*come fa*» o piuttosto sugli impatti su «*cosa fa*»

Informazione collettiva vs informazione individuale

«Rappresentanza tecnica» vs rappresentanza sindacale

I dati di input

I DATI DI INPUT: AI ACT E GDPR

- Valutazione di impatto della protezione dei dati
- Rinvio al GDPR
- Dati di input devono essere pertinenti e sufficientemente rappresentativi
- Conservazione dei log (per 6 mesi) nei sistemi ad alto rischio

Art. **35 Gdpr** valutazione d'impatto **DPIA** nel caso di trattamento con l'uso di nuove tecnologie che può presentare un rischio elevato per i diritti e le libertà delle persone fisiche

una **valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato**, compresa la profilazione, e sulla quale si **fondano decisioni** che hanno effetti giuridici o incidono su dette persone fisiche

misure di gestione del rischio: sorveglianza umana; *governance* interna e meccanismi di reclamo

L'AI PUÒ DISCRIMINARE?

i dati di input, i parametri, i pesi, le correlazioni

- La **discriminazione storica** (l'algoritmo di reclutamento dei software developer di Amazon)
- La **proxy discrimination** e pattern di correlazione (la correlazione ingegneri-fumetti manga)
- L'**algoritmo cieco** (gli algoritmi di profilazione e di ranking di Deliveroo e di Foodinho)
- I **bias di progettazione** (Google translator e annunci di lavoro STEM mostrati più a uomini che a donne da Facebook e Instagram)

Servono norme ad hoc o sono sufficienti le norme antidiscriminatorie?

I diritti di informazione sindacale

OBBLIGO DI PREVENTIVA INFORMAZIONE PER SISTEMI AD ALTO RISCHIO (INDIVIDUALE/COLLETTIVO)

Articolo 26

Obblighi dei deployer dei sistemi di IA ad alto rischio

7. Prima di mettere in servizio o utilizzare un sistema di IA ad alto rischio sul luogo di lavoro, i deployer che sono datori di lavoro **informano i rappresentanti dei lavoratori e i lavoratori interessati** che saranno soggetti all'uso del sistema di IA ad alto rischio. Tali informazioni sono fornite, se del caso, conformemente alle norme e alle procedure stabilite dal diritto e dalle prassi dell'Unione e nazionali in materia di informazione dei lavoratori e dei loro rappresentanti.

OBBLIGO DI PREVENTIVA INFORMAZIONE PER SISTEMI AUTOMATIZZATI ART. 1 BIS



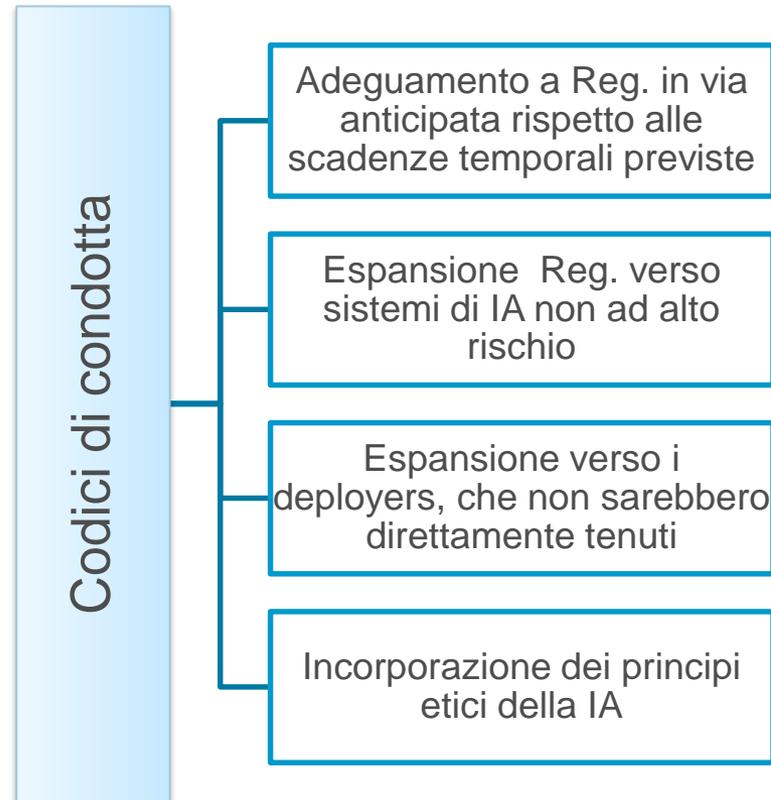
I codici di condotta e le prospettive regolative

I Codici di condotta (art. 95)

I codici di condotta possono essere elaborati da singoli fornitori o deployer di sistemi di IA o da organizzazioni che li rappresentano o da entrambi, anche con la partecipazione di qualsiasi portatore di interessi e delle sue organizzazioni rappresentative, comprese le organizzazioni della società civile e il mondo accademico.

- Attuare orientamenti etici dell'Unione per un'IA affidabile
- Valutare e ridurre l'impatto dei sistemi di IA sulla sostenibilità ambientale
- Promuovere l'alfabetizzazione in materia di IA, in particolare quella delle persone che si occupano dello sviluppo, del funzionamento e dell'uso dell'IA
- Facilitare la progettazione inclusiva e promuovere la partecipazione dei portatori di interessi a tale processo
- Valutare e prevenire l'impatto negativo sulle persone vulnerabili o sui gruppi di persone vulnerabili, (disabilità, parità di genere)

Codici di condotta (art. 95)



DE IURE CONDENDO

DDL (S. 1146) «Disposizioni e delega al Governo in materia di intelligenza artificiale»

Art. 10 Disposizioni sull'uso dell'intelligenza artificiale in materia di lavoro

1. L'intelligenza artificiale è impiegata per migliorare le condizioni di lavoro, tutelare l'integrità psico-fisica dei lavoratori, accrescere la qualità delle prestazioni lavorative e la produttività delle persone in conformità al diritto dell'Unione europea.
2. L'utilizzo dell'intelligenza artificiale in ambito lavorativo deve essere sicuro, affidabile, trasparente e non può svolgersi in contrasto con la dignità umana né violare la riservatezza dei dati personali. Il datore di lavoro o il committente è tenuto a **informare il lavoratore dell'utilizzo** dell'intelligenza artificiale nei casi e con le modalità di cui all'articolo 1-bis del decreto legislativo 26 maggio 1997, n. 152.
3. L'intelligenza artificiale nell'organizzazione e nella gestione del rapporto di lavoro garantisce l'osservanza dei diritti inviolabili del **lavoratore senza discriminazioni** in funzione del sesso, dell'età, delle origini etniche, del credo religioso, dell'orientamento sessuale, delle opinioni politiche e delle **condizioni personali, sociali ed economiche**, in conformità con il diritto dell'Unione europea.

19 febbraio 2025

Intelligenza artificiale e lavoro

CONCLUSIONI

Gran parte degli obblighi posti dall'AI ACT sono stati anticipati dal nostro legislatore con il decreto trasparenza

L'AI ACT ha un forte impatto sugli adempimenti privacy

Occorre verificare con attenzione la tipologia e la qualità di dati utilizzati sotto il controllo del datore

I sistemi di IA aumentano il potenziale di controllo del datore (associato al potere direttivo) con impatto su art. 4 l. 300 1970

La formazione al personale è obbligatoria e va curata adeguatamente e tracciata

L'AI ACT ha un impatto sindacale: obblighi di preventiva informazione sindacale in relazione all'introduzione di sistemi di IA ad alto rischio

L'AI ACT prevede un complesso sistema di governance con autorità di riferimento e di vigilanza a livello nazionale ed europeo. Ciò determinerà un sistema di fonti complesso (analogo a quello che abbiamo verificato con privacy)