Memoria CGIL alla Commissione Trasporti e alla Commissione Attività produttive della Camera su proposta di Regolamento che stabilisce regole armonizzate su Intelligenza Artificiale - COM (2021) 206 def del 21.4.2021

Lo strumento adottato dall'UE, ossia il Regolamento, ci sembra di fatto il più adeguato per garantire uniformità di applicazione ed auspichiamo dunque che, data la peculiarità della materia, siano minimizzati gli spazi di autonomia dei singoli stati in ambito applicativo.
L'approccio normativo risk based è condivisibile, nonostante sia di tipo proporzionato, perché pone in capo ai soggetti coinvolti nell'impiego dell'IA la predisposizione di un sistema di gestione dei rischi legati all'utilizzo di questi strumenti by design (cioè a partire dalla primissima fase di progettazione fino alla distribuzione e all'utilizzo) e by default (cioè per impostazione predefinita).
Ciò vale a partire dalla definizione di "sistema di intelligenza artificiale" (art. 3, punto 1) che, a nostro avviso, deve essere il meno generica possibile onde evitare che i singoli stati possano darne una interpretazione restrittiva per eludere i vincoli stabiliti dal Regolamento e, nel contempo, capace di riconoscerla come un infrastruttura in costante evoluzione.

****

Di fatto siamo dinanzi ad una tecnologia in grado di assumere decisioni ipoteticamente dannose per l'umanità per cui è opportuna una regolamentazione severa e inequivocabile di alcune pratiche.

Un esempio è la capacità di svolgere una sorveglianza di massa indiscriminata, grazie agli algoritmi di IA e all'aumento delle potenze di calcolo e di dati disponibili su di noi e sui nostri rapporti sociali ed interpersonali.
Suscita molta perplessità la previsione circa l'uso *"di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto."* Questo è in linea di principio vietato, a meno che e nella misura in cui

tale uso sia strettamente necessario per uno degli obiettivi di cui all'art. 5, par. 1, lett. d), tra cui la *" prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di un attacco terroristico"* (art 5).
Riteniamo in generale che qualsiasi forma di sorveglianza necessiti della preventiva autorizzazione dell'autorità giudiziaria, imprescindibile in caso di identificazione biometrica negli spazi aperti.
Vi è il rischio che una interpretazione larga delle eccezioni previste dall'art. 5 cit. della proposta di Regolamento, da parte di ogni singolo Stato, renda eccessivamente diffusa una pratica che confligge fortemente con il diritto alla privacy e mina i diritti fondamentali di libertà.
In tal senso concordiamo nella sostanza con il parere (Joint Opinion 5/2021) adottato dall'European Data Protection Board e dallo European Data protection Supervisor il 18 giugno 2021 ove si raccomanda "*che sia introdotto un divieto generale di qualsiasi utilizzo dell'IA a fini di riconoscimento automatico delle caratteristiche umane in spazi accessibili al pubblico, come il volto ma anche l'andatura, le impronte digitali, il DNA, la voce, le sequenze di battute su tastiera e altri segnali biometrici o comportamentali, in qualsiasi contesto.* Un altro divieto raccomandato riguarda i sistemi di IA che "*categorizzano le persone in insiemi, a partire dai dati biometrici, in base all'etnia, al genere, all'orientamento politico o sessuale oppure in base ad altri motivi di discriminazione"* ai sensi dell'articolo 21 della Carta. Inoltre, l'EDPB e il GEPD ritengono che "*l'utilizzo dell'IA per dedurre le emozioni di una persona fisica sia assolutamente inopportuno e dovrebbe essere vietato*".
Auspichiamo che si assuma che l'utilizzo dell'IA **non potrà mai** avvenire a fini repressivi e/o di controllo, in qualunque ambito, evitando così il rischio concreto di acuire asimmetrie già esistenti e di produrre situazioni pregiudizievoli e/o discriminatorie.

****

Il sistema nel complesso va integrato con altre discipline di ordine europeo, prima fra tutte ovviamente il Regolamento Ue n. 679/2016 (GDPR).
Senza privacy è infatti impossibile una qualsiasi forma di indipendenza di pensiero e di azione.

D'altra parte riteniamo inaccettabile la distinzione tra attori pubblici e privati in tema di **scoring.**
Se infatti ai primi verrà impedito l'utilizzo di sistemi di IA per valutare e classificare con un «punteggio sociale» (*social scoring*) la affidabilità delle persone sulla base del loro comportamento sociale in contesti sociali estranei a quelli in cui i dati sono stati

originariamente generati o raccolti, ai privati verrebbe mantenuta la facoltà di svolgere attività di «classifiche» (*rating)* reputazionali. Se pure questa loro facoltà è bilanciata dai principi di liceità, correttezza e trasparenza di cui all'art 5 del Gdpr, non ci sembra corretto consentire sistemi di valutazione su base algoritmica di terzi.
A nostro avviso, ad esempio, il tema si porrebbe in modo dirompente in ambito lavorativo. (vedi l'art. 6, par. 2 della proposta di Regolamento e l'Allegato III, punto 4).
Ad ogni modo, va riaffermata la vincolatività del confronto sindacale sulla scelta dei dati da sottoporre all'elaborazione dell'IA.

****

Il sistema di regole che il Regolamento appronta per garantire un utilizzo etico e non nocivo degli strumenti di IA coinvolge tutta la catena, dai fornitori agli utenti.

In tema di **garanzia di conformità** alle regole, da attuarsi in maniera costante e sistematica, riteniamo sicuramente importante la prevista certificazione di cui all'art 27 del nuovo Regolamento, ove si stabilisce che: "*prima di mettere a disposizione sul mercato un sistema di IA ad alto rischio, i distributori verificano che il sistema di IA ad alto rischio rechi la necessaria marcatura CE di conformità, che sia accompagnato dalla documentazione e dalle istruzioni per l'uso necessarie e che il fornitore e l'importatore del sistema, a seconda dei casi, abbiano rispettato gli obblighi di cui al presente regolamento*".
Ciò nonostante ci pare improprio che il tema della valutazione di conformità sia affidato in larga misura a soggetti privati, produttori o fornitori delle tecnologie in oggetto, specie in considerazione del fatto che sono poche grandi aziende private oggi ad avere la conoscenza e la materia prima (big data) necessari a sviluppare sistemi di IA.
Riteniamo sempre opportuna l'individuazione di soggetti terzi, indipendenti, con le competenze necessarie a valutare la conformità al Regolamento specie per quanto attiene i sistemi ad alto rischio.

****

Facciamo nostro il già citato parere n. 5/2021 adottato dall'*European Data Protection Board e dallo European Data Protection Supervisor* il 18 giugno 2021 nella parte in cui evidenzia la criticità dell'assenza di diritti specifici in capo ai singoli individui e l'assenza di procedure da adottare da parte degli stessi quando sottoposti a sistemi di IA.

Sostanzialmente i due organismi notano un difetto di collegamento tra il Regolamento in oggetto ed il GDPR laddove il sistema di IA utilizzasse dati personali, in particolare rispetto all'art 22 del GDPR che riconosce il diritto per un soggetto di non essere sottoposto ad una decisione completamente automatizzata.

Come è stato previsto un Comitato europeo sull'Intelligenza Artificiale, che sia responsabile dell'applicazione armonizzata del Regolamento in tutta l'area UE per le questioni di salute, sicurezza e diritti fondamentali dei cittadini e delle cittadine, cui deve esssere riconosciuto il maggior grado possibile di autonomia, parimenti è necessario capire come sarà strutturata una pari Autorità indipendente nazionale e quali saranno le sue competenze e possibilità di azione (art 59 Regolamento).

****

Altro profilo di rilievo attiene il **set di dati** con cui si istruiscono i meccanismi di IA.
A nostro avviso va riconosciuto a favore dei "portatori di interessi" il diritto all'accesso dei dati che sono alla base della specifica applicazione di IA utilizzata .

È evidente che l'utilizzo di sistemi di IA in relazione alla prestazione lavorativa apre una problematica che - riteniamo - debba essere debitamente affrontata nelle sedi opportune sia in ambito Eu che nel nostro paese, con particolare riferimento **ad un obbligo di informazione a favore dei rappresentanti di lavoratrici e lavoratori,** in merito ai sistemi adottati, ai set di dati utilizzati, alle modalità di interazione tra uomo e macchina.
Il rapporto sempre più stretto tra esseri umani e sistemi automatizzati pone il tema ulteriore della **responsabilità del datore di lavoro** e del lavoratore in presenza di processi produttivi e attività automatizzate, tema su cui sarebbe opportuno sviluppare il ragionamento già parzialemente in itinere nel Parlamento europeo. Si veda "*Risoluzione del Parlamento europeo 20*20/2014(INL) *recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale"*.

****

Parimenti sarà necessaria una discussione su una regolamentazione più dettagliata in merito alla **proprietà intellettuale o alla titolarità dei brevetti** in caso di invenzioni nate dall'interazione tra essere umano e macchina o direttamente ed autonomamente da sistemi di IA.
Si veda "*Risoluzione del Parlamento europeo su diritti di proprietà intellettuale per*

lo sviluppo di IA- 2020/2015 (INI)".

****

Rileviamo infine che non esiste alcun riferimento e dunque alcun progetto di regolazione sull'**impronta ecologica dell'IA**.
L'architettura di IA ha infatti una fortissima impronta ecologica, che andrebbe tenuta in considerazione in fase di implementazione, sia per ciò che attiene i componenti dei sistemi tech necessari per l'attività computazionale (litio, cobalto, componenti delle terre rare, ecc), sia per lo smaltimento degli stessi, sia per la sua caratteristica energivora e per l'utilizzo di acqua necessario al raffreddamento dei server.