# L'AI Act nell'ecosistema normativo europeo in tema di digitale tra continuità e discontinuità

**Antonio Iannuzzi**
*Professore ordinario di Diritto costituzionale e pubblico presso l'Università Roma Tre. Mail: antonio.iannuzzi@uniroma3.it*

## 1. Il Regolamento (UE) 2024/1689 nel contesto della regolazione della società digitale

Il Reg. (UE) 2024/1689 che stabilisce regole armonizzate sull'intelligenza artificiale (c.d. AI Act), non è assolutamente un atto isolato nell'ecosistema normativo digitale. La rivendicazione della sovranità digitale condivisa a livello europeo ha avuto come effetto, negli ultimi anni, un'accentuata produzione di regolamenti per la disciplina di diversi ambiti lambiti dalle applicazioni delle tecnologie digitali. Oltre all'intelligenza artificiale che richiede una regolazione specifica, in ragione delle sue straordinarie attese circa gli utilizzi positivi che si combinano ai rischi per i diritti umani ed i processi democratici, l'ecosistema normativo impone di considerare anche altri tre ambiti settoriali, vale a dire la regolazione dei dati, personali e non, delle piattaforme digitali e della cybersicurezza. I tanti regolamenti e le direttive che intervengono per disciplinare gli oggetti della società digitale fanno sistema fra loro, implicando che l'AI Act non può essere interpretato isolatamente.

## 2. Incentivare la circolazione lecita dei dati come precondizione per la diffusione ed il buon funzionamento dei sistemi di intelligenza artificiale

Se l'AI Act, in una metafora cinematografica, rappresenta il colossal della produzione dell'UE, il suo "prequel" sono altri tre atti normativi: il DGA, il Data Act, l'EHDS, nei termini in cui si dirà subito appresso.
L'ordinamento dell'UE ha cercato di arrivare preparato al momento della prepotente diffusione dei sistemi di AI nel mercato digitale. Poiché la circolazione dei dati, in una cornice di liceità, è un'esigenza primaria del floridissimo mercato digitale, l'UE ha avvertito che, come primo passo, fosse necessario favorire la ricerca di un più equilibrato bilanciamento fra protezione e circolazione dei dati personali. Ad avviso di molti, il Reg. (UE) 2016/679, Regolamento generale sulla protezione dei dati personali (GDPR), ha prodotto effetti maggiori sul piano della protezione, mentre ha, oltre il suo portato normativo, conseguito risultati meno apprezzabili per favorire la circolazione. Per conseguire quest'obiettivo, è stato adottato il Reg. (UE) n. 2022/868, relativo alla *governance* europea dei dati (c.d. Data Governance Act – DGA), che istituisce una rete per la condivisione di dati, pubblici e privati. Con la finalità di muoversi in parallelo con il DGA, il 27 novembre del 2023. A questo atto ha fatto seguito, poi, il Reg. (UE) 2023/2854 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (c.d. Data Act). Ancora, come prima applicazione settoriale delle norme orizzontali del DGA, è stato, ancora, adottato il Reg. (UE) 2025/327, che istituisce lo spazio europeo dei dati sanitari (EHDS).

## 3. L'AI ACT fra obiettivi condivisi e limitazioni di intervento derivanti dalla base giuridica

In questo quadro si inserisce l'approvazione dell'AI Act, che condivide con i regolamenti della

società digitale le medesime finalità e la ricerca degli stessi bilanciamenti.

In primo luogo, l'adozione di un Regolamento generale sull'AI parte dal presupposto di sviluppare un mercato unico dei dati e dell'Intelligenza Artificiale. Coerente con quest'affermazione è la sua base giuridica: l'art. 114 TFUE che attribuisce all'UE la competenza a adottare le misure relative al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri che hanno per oggetto l'instaurazione ed il funzionamento del mercato interno. Il Regolamento mira a trovare un equilibrio fra mercato e diritti in nome del perseguimento di un «umanesimo digitale», che metta al centro dello sviluppo delle tecnologie digitali emergenti i diritti fondamentali della persona. Il problema è che il perseguimento di questa finalità esorbita dall'ampiezza della base giuridica[1].

## 4. L'osmosi a livello di principi fra l'AI Act e le altre componenti normative in materia di tecnologie digitali

Anche dal punto di vista del contenuto normativo l'AI Act si pone in continuità con le altre componenti normative che regolano le tecnologie digitali.

L'AI Act si inserisce nel quadro normativo europeo già consolidato dal GDPR, che è la pietra d'angolo della disciplina europea sui dati e le tecnologie digitali incentrata sulla persona, nonché la bussola per l'impiego della tecnologia nel contesto della duplice transizione, ecologica e digitale, che caratterizza la definizione delle politiche dell'Ue. In questo senso, si condivide la tesi secondo cui il GDPR costituisce la prima vera regolazione europea dell'AI[2].

L'ecosistema normativo digitale europeo è animato dalla necessità di individuare principi condivisi capaci di orientare trasversalmente il settore dei dati, delle piattaforme, dell'intelligenza artificiale e della sicurezza cibernetica.

In comune vi è l'approccio basato sul rischio, che pervade il complesso della normativa dal GDPR, fino all'AI Act, con il suo impianto articolato sulla c.d. piramide del rischio, passando per il Reg. 2022/2065, c.d. Digital Service Act (DSA), e per i tanti atti normativi che disciplinano la cybersecurity. Il carattere diffuso di questo approccio ha spinto a qualificare l'attività normativa europea in materia in termini di *risk regulation*[3]. In definitiva, è emerso il concetto di «rischio digitale» che, com'è stato ben detto, «è una specificazione del più generale "rischio tecnologico"»[4]. L'approccio *risk-based* conosce ora un'applicazione più decisa nella regolazione dell'intelligenza artificiale, per via della classificazione ivi operata, che distingue tra sistemi vietati, sistemi ad alto rischio e sistemi a rischio minimo (*risk approach*). Sulla gestione del rischio, tuttavia, l'UE mostra di avere una variabilità di accentuazioni, risultando ad esempio ben più evidente il suo impatto sulla configurazione di divieti nell'AI Act

[1] M.D. Cole, C. Etteldorf, *Future Regulation of Cross-border Audiovisual Content Dissemi-nation: A Critical Analysis of the Current Regulatory Framework for Law Enforcement Under the EU Audiovisual Media Services Directive and the Proposal for a European Media Freedom Act*, Nomos, 2023; O. Pollicino, *Regolazione e innovazione tecnologica nell'"ordinamento della rete"*, in *Rivista AIC*, 2025, 128 ss.; E. Longo, *Il fondamento della libertà dei media nell'UE: la base giuridica dell'EMF*, in *Rivista italiana di informatica del diritto*, 2025, 1 ss.

[2] P. Nemitz, *Constitutional democracy and technology in the age of artificial intelligence*, *in Philosophical transactions of the Royal Society*, 2018 (376).

[3] A. Alemanno, *The Past, Present and Future of Risk Regulation*, in *European Journal of Risk Regulation*, 2017, 1 ss.

[4] E. Longo, *La disciplina del "rischio digitale"*, in F. Pizzetti, S. Calzolaio, A. Iannuzzi, E. Longo, M. Orofino, *La disciplina europea della società digitale*, cit., 58.

rispetto a quanto lo sia invece negli altri atti normativi.

Sul piano dell'individuazione di principi fondamentali i regolamenti europei stanno conseguendo effetti importanti.

In primo luogo, si è affermato e rafforzato il principio «*one continent, one law*», che è una sorta di *ius commune* in materia di *privacy*, che le Istituzioni europee hanno scelto di disciplinare con lo strumento normativo più efficace per portare ad unità le diverse

legislazioni nazionali: il Regolamento.

In secondo luogo, è stato introdotto il principio di responsabilizzazione (*accountability*), di matrice europea, che nell'ordinamento giuridico italiano ha determinato una rivoluzione copernicana nell'approccio degli operatori alla *compliance*, comportando il superamento della concezione autorizzatorio/concessoria dell'amministrazione, in favore del riconoscimento di una libertà immediata di agire salva la vigilanza da parte dell'autorità pubblica, con la possibilità di effettuare controlli successivi ed eventualmente di comminare sanzioni.

In terzo luogo, si è diffuso l'approccio *by design* e *by default*, che è forse una tecnica regolatoria ancora più innovativa rispetto all'*accountability*, perché impone di considerare la protezione dei dati personali, l'etica, la cybersicurezza e le altre misure sin dalla progettazione e per impostazione predefinita. Questa tecnica regolatoria consente «typically involving the design of products or places, or the automation of processes . . . [which] seeks to *exclude* (i) the possibility of certain actions which, in the absence of this strategy, might be subject only to rule regulation [and/] or (ii) human agents who otherwise would be implicated in the regulated activities»[5].

Ancora trasversale è l'applicazione del principio di neutralità tecnologica, in applicazione del quale si stabilisce un regime di indifferenza, o di imparzialità, verso il mezzo utilizzato, nel caso del GDPR per il trattamento dei dati, rispetto alla protezione della persona: «al fine di evitare l'insorgere di gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate» (Considerando 15). La neutralità tecnologica «significa che la legislazione deve definire gli obiettivi da perseguire e non deve imporre né favorire l'uso di un particolare tipo di tecnologia per conseguirli»[6]. In questo senso, il principio si applica anche ai sistemi di AI.

Una speciale declinazione di questo principio sul piano meta-normativo è rappresentata dalla «neutralità tecnologica della legge», vale a dire dall'assunzione dell'idea che sia compito delle fonti giuridiche individuare e definire gli obiettivi e i valori da tutelare, a prescindere dalla singola tecnologia impiegata per perseguirli.

## 5. L'inestricabile intreccio fra l'art. 22 del GDPR e l'art. 14 dell'AI Act

Ancora dal GDPR possono essere filtrati principi che orientano anche la disciplina dell'AI.

Viene in riferimento, intanto, il diritto alla trasparenza algoritmica (art. 22 GDPR). Detto diritto ha un'applicazione molto difficile in rapporto ai sistemi di *machine learning*, che sono delle complesse *black box* che non consentono di tenere traccia e di dare conto dei processi decisionali.

[5] R. Brownsword, *In the Year 2061: From Law to Technological Management*, in *Law, Innovation and Technology*, 2015 (7), 18.

[6] Commissione Europea, *Comunicazione del 10 novembre 1999, Verso un nuovo quadro per l'infrastruttura delle comunicazioni elettroniche*, COM (1999) 539 definitivo, 13.

Complementare alla trasparenza è il riconoscimento del diritto alla spiegabilità algoritmica. In proposito, come ha affermato in Italia il Consiglio di Stato, «"il meccanismo con cui si concretizza la decisione robotizzata" dev'essere "conoscibile, secondo una declinazione rafforzata del principio di trasparenza, che implica anche quello della piena conoscibilità di una regola espressa in un linguaggio differente da quello giuridico», nonché che la logica dell'algoritmo deve essere «non solo conoscibile in sé, ma anche soggetta alla piena cognizione, e al pieno sindacato, del giudice amministrativo»[7].

Ancora dall'art. 22 del GDPR emerge l'affermazione della non esclusività algoritmica[8], che sembra assurgere a principio costitutivo del rapporto fra uomo e macchina, tanto da far trasparire con decisione i contorni di un sicuro tono costituzionale. Esso afferma il diritto a non essere sottoposti a trattamenti totalmente automatizzati e specularmente il diritto ad essere informati rispetto all'eventuale sottoposizione a trattamenti interamente automatizzati. Dal riconoscimento di questa situazione giuridica soggettiva è agevole enucleare un diritto all'intervento umano (*human in the loop*), che è ora affermato nell'AI Act. L'art. 22 del GDPR recita al paragrafo 1 che «L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona».

Al par. 3 dello stesso articolo si introduce il diritto di ottenere l'intervento umano da parte del titolare del trattamento: nei casi previsti dal GDPR in cui non si applica il paragrafo 1, il titolare del trattamento deve attuare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, fra di essi deve assicurare «almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione». In ogni caso, le ipotesi in cui non si applica il paragrafo 1, non riguardano le decisioni che concernono le «categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato».

Detto diritto dovrebbe auspicabilmente essere esteso ad ogni aspetto della relazione fra uomo e macchina ed assumere carattere universale, in un'epoca che è stata definita come «Novacene» (J. Lovelock), un'età, vale a dire, che va a caratterizzarsi per coesistenza degli umani con dispositivi dotati di superintelligenza. Per effetto di questa estensione si inizierebbe effettivamente ad avviare quell'operazione di individuazione delle attività che devono restare prerogativa dell'uomo ed essere protette dai rischi di ingerenza delle tecnologie intelligenti, contribuendo a delineare la concettualizzazione di uno spazio intangibile riservato all'uomo.

Muovendosi nella stessa direzione normativa, l'AI Act presenta un forte riconoscimento del diritto all'intervento umano, nella parte in cui dispone che i sistemi ad alto rischio debbano essere programmati e sviluppati in modo da garantire la necessaria supervisione umana (art. 14). Tale attività di supervisione deve essere orientata a prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali, che possono emergere quando un sistema di IA ad alto rischio è utilizzato conformemente alla sua

[7] Cons. Stato, Sez. IV, 8 aprile 2019, n. 2770.

[8] Fondamentale in tema è A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, 2019, 69: Nella giurisprudenza amministrativa v. ancora Cons. St., sez. IV, 8 aprile 2019, n. 2270

finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile, in particolare quando tali rischi persistono nonostante l'applicazione delle misure introdotte dallo stesso Regolamento.

Ad integrazione, la norma tecnica internazionale di riferimento, la ISO/IEC 22989 (*Information technology - Artificial intelligence - Artificial intelligence concepts and terminology*), definisce la controllabilità la proprietà di un sistema di intelligenza artificiale che consente ad un agente esterno di intervenire nel suo funzionamento. La controllabilità, aggiunge, può essere ottenuta fornendo meccanismi affidabili con cui un agente può assumere il controllo del sistema di AI. Precisa, infine, che un aspetto basilare della controllabilità è la determinazione di quale agente (o quali agenti) possa controllare quali componenti del sistema di AI, citando come a titolo esemplificativo il fornitore di servizi o di prodotti, il fornitore dell'AI costituente, l'utente piuttosto che un'autorità di regolamentazione.

Una prima importante applicazione giurisprudenziale del diritto in parola si è registrata con la Sentenza C-634/21della Corte di Giustizia (Prima Sezione) del 7 dicembre 2023, nella quale è stato stabilito che l'art. 22, par. 1, del GDPR deve essere interpretato nel senso che «il calcolo automatizzato, da parte di una società che fornisce informazioni commerciali, di un tasso di probabilità basato su dati personali relativi a una persona e riguardanti la capacità di quest'ultima di onorare in futuro gli impegni di pagamento costituisce un «processo decisionale automatizzato relativo alle persone fisiche», ai sensi di tale disposizione, qualora da tale tasso di probabilità dipenda in modo decisivo la stipula, l'esecuzione o la cessazione di un rapporto contrattuale con tale persona da parte di un terzo, al quale è comunicato tale tasso di probabilità»[9].

In definitiva, il diritto all'intervento umano rappresenta la prima concretizzazione dell'umanesimo digitale che propugna l'Ue. Nell'ordinamento costituzionale italiano la sua affermazione appare pienamente in linea con l'impianto assiologico della Carta, con riferimento, in primo luogo, alla centralità dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità (art. 2 Cost.), alla solidarietà e all'uguaglianza (art. 3 Cost.). Una conferma istituzionale fondamentale è arrivata dal Presidente della Repubblica, Sergio Mattarella, che nel messaggio di fine anno (2023), ha affermato che «La tecnologia ha sempre cambiato gli assetti economici e sociali. Adesso, con l'intelligenza artificiale che si autoalimenta, sta generando un progresso inarrestabile. Destinato a modificare profondamente le nostre abitudini professionali, sociali, relazionali. Ci troviamo nel mezzo di quello che verrà ricordato come il grande balzo storico dell'inizio del terzo millennio. Dobbiamo fare in modo che la rivoluzione che stiamo vivendo resti umana. Cioè, iscritta dentro quella tradizione di civiltà che vede, nella persona - e nella sua dignità - il pilastro irrinunziabile. Viviamo, quindi, un passaggio epocale. Possiamo dare tutti qualcosa alla nostra Italia. Qualcosa di importante. Con i nostri valori. Con la solidarietà di cui siamo capaci»[10].

## 6. I due principali nodi critici dell'AI Act

Il rapporto fra l'AI Act e gli altri atti normativi europei che intervengono a disciplinare la società

[9] Corte di Giustizia, causa C-634/21, *Oq vs. Land Hessen, con l'intervento di SCHUFA Holding AG*, 7 dicembre 2023.

[10] *Messaggio di Fine Anno del Presidente della Repubblica Sergio Mattarella*, 31 dicembre 2023, disponibile al seguente link: https://www.quirinale.it/elementi/103914.

digitale non è sempre lineare, anzi in taluni casi emergono evidenti segnali di discontinuità che pongono le principali incognite nell'applicazione effettiva del Regolamento.

In questo senso, i principali nodi critici sembrano essere due.

Il primo è relativo al non chiaro rapporto fra le regole previste dall'art. 6 del GDPR per la liceità del trattamento dei dati personali in rapporto, invece, all'esigenze peculiari del trattamento dei dati per l'addestramento degli algoritmi. Nessuna delle basi giuridiche previste dal GDPR appare utile per coprire il massiccio utilizzo dei dati da parte dell'AI. Di conseguenza, viene da chiedersi fino a quanto sarà possibile stiracchiare l'interesse legittimo senza stravolgerne la *ratio* normativa, rendendolo un *passepartout* buono per giustificare ogni forma di trattamento? È stato osservato condivisibilmente in proposito che «un'interpretazione debole o eccessivamente elastica delle basi giuridiche potrebbe minare, infatti, l'intera architettura della protezione dei diritti ai sensi del GDPR»[11]. Vista la mole delle informazioni trattate non sembra pensabile fare ricorso al consenso informato. Altri problemi sorgono in relazione al difficile rapporto tra la finalità del trattamento e l'attività di addestramento ad ampio spettro degli algoritmi. Se i dati devono essere raccolti solo per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità (art. 5, par. 1, lett. b), GDPR) come si possono utilizzare questi dati in modo tendenzialmente non predefinito o limitato a fini di efficientare il lavoro e i risultati dell'AI?

Il secondo problema attiene alla *governance* dell'AI. Il Regolamento ha previsto un complesso sistema articolato in tre sistemi diversi: *i)* per i sistemi ad alto rischio; *ii)* per i modelli a finalità generali; *iii)* per i prodotti *post-market*. Laddove la *governance* non sia demandata alla Commissione europea, nella specie per i sistemi ad alto rischio, la scelta dell'autorità nazionale competente è rimessa alla determinazione statale (art. 70 AI Act). È noto che in Italia siano state individuate come autorità competenti l'Agenzia per l'Italia Digitale (AGID) e l'Agenzia per la Cibersicurezza Nazionale (ACN). In considerazione della circostanza che entrambe sono Agenzie del Governo e non Autorità amministrative indipendenti, la scelta appare condivisibile in termini di tutela del mercato, nella misura in cui il Governo voglia guidare l'innovazione digitale e darle impulso, anche se forse in tal senso si poteva immaginare un coinvolgimento del Ministero dello Sviluppo economico. La decisione appare comprensibile se si considera che il posizionamento in tema di AI influenza le dinamiche politiche e di potere del mondo contemporaneo. Affatto coerente con tutto l'impianto dell'ecosistema normativo digitale europeo, invece, è la mancata istituzione di un'Autorità *ad hoc* o la *mancata* estensione dei poteri di una o più *Authorities* già competenti in materia di dati e di tecnologie digitali con riferimento alla tutela dei diritti nel ciberspazio. La tutela dei diritti nell'ecosistema dell'intelligenza artificiale e la difesa dei valori fondamentali dell'UE non possono essere affidate ad una o più autorità di governo nazionali che difettano del requisito dell'indipendenza, che rappresenta il presupposto indefettibile «che consente di indagare su potenti piattaforme globali» e che «garantisce che i diritti non vengano subordinati alle valutazioni di opportunità»[12].

[11] G. Cerrina Feroni, *Chi vigila sull'IA? Le Autorità privacy tra controllo e innovazione*, in *Agenda digitale*, 2025.

[12] G. Cerrina Feroni, *Chi vigila sull'IA?,* cit.

## 7. Il futuro dell'AI Act. Il tempo e le sfide

Se la scorsa legislatura europea si è caratterizzata, come si è mostrato, per l'affermazione della volontà politica di regolare e limitare le tecnologie digitali ed il loro potere, realizzando un'operazione di riaccentramento delle fonti del diritto, nel momento attuale di inizio legislatura l'attenzione è rivolta a cercare di capire se si continuerà a procedere nella stessa direzione oppure se si svolterà in direzione opposta. Se si sceglierà la strada della continuità, occorrerà lavorare per dare attuazione a principi e diritti che reclamano effettività, a fronte di una loro non semplice affermazione concreta. Servirebbe anche una razionalizzazione che possa orientare l'interpretazione del reticolo normativo, che talvolta risulta complesso perché troppo dettagliato, nonché una semplificazione che agevoli l'attività di *compliance* integrata alle diverse normative europee.

In questa prospettiva si è mossa la prima proposta di revisione del GDPR[13], che è parte integrante del quarto pacchetto «semplificazione Omnibus», pubblicato il 21 maggio dalla Commissione Europea. Obiettivo della proposta, che presenta a dire il vero ancora un articolato minimo perciò non pienamente adeguato allo scopo, è quello di diversificare gli adempimenti fra grandi aziende e PMI, in particolare riducendo i costi amministrativi e i procedimenti per l'adeguamento alla normativa in materia di protezione dei dati personali primariamente nei confronti di piccole e medie imprese (PMI) e di imprese a media capitalizzazione di piccole dimensioni, pur mantenendo standard elevati di privacy e sicurezza.

Si avverte che la proposta si muove sulla scia di due rapporti recentemente presentati da importanti esponenti italiani. Si richiama espressamente, infatti, nella proposta la relazione su «Il futuro della competitività europea», di Mario Draghi, nella parte in cui sostiene che la regolamentazione dell'UE impone irrazionalmente oneri proporzionalmente maggiori alle PMI e alle piccole imprese a media capitalizzazione, rispetto alle imprese più grandi. Secondo la relazione «Molto più di un mercato» presentata da Enrico Letta, anch'essa puntualmente citata, la distinzione tra *mid-cap* e grandi imprese, oggi non presente nei regolamenti dell'UE, consentirà di dettare regole più adeguate, favorendo la loro crescita e la loro equa partecipazione al mercato unico, soprattutto durante le crisi.

Non si tratta di una novità, perché anche il DGA si è mosso nella direzione di intervenire all'interno del mercato digitale favorendo le PMI, attraversi l'imposizione di regole specifiche e particolarmente indicate, con la motivazione che esse rappresentano la specificità europea nel mercato delle ICT, e non solo, e che rischiano di rimanere schiacciate, nella contesa globale, dal potere dei giganti della tecnologia.

Per rispondere ai rilievi emersi nei rapporti citati e per conseguire gli obiettivi dichiarati, ora la proposta inserisce all'interno delle definizioni di cui all'art. 4 la nozione di «microimprese, piccole e medie imprese» e «imprese a media capitalizzazione di piccole dimensioni». Di conseguenza, viene aggiunto un riferimento ad entrambe all'art. 40, par. 1 (Codici di condotta) e all'art. 42, par. 1 (Certificazioni).

L'UE potrebbe anche decidere, invece, di invertire la rotta. Si fanno sentire con forza i condizionamenti derivanti dal difficile contesto

[13] COM(2025)501 - Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2016/1036, (EU) 2016/1037, (EU) 2017/1129, (EU) 2023/1542 and (EU) 2024/573.

geopolitico e dai rapporti internazionali ora più tesi con gli Stati Uniti d'America, che lamentano l'eccessiva rigidità della regolazione europea della società digitale che si riverberebbe negativamente – a loro dire – sulle Big Tech americane in termini di maggiori costi amministrativi.

Queste rivendicazioni fanno leva su posizioni diametralmente opposte rispetto alle conclusioni dei due citati rapporti di Mario Draghi e di Enrico Letta, mostrando come dietro i modelli regolatori si celano interessi di mercato ben definiti.

Due richieste formali di "*Stop the Clock*" dell'AI Act sono state presentata da alcune decine di *top manager* e da un altro buon numero di *startupper,* che lamentano l'eccessiva burocratizzazione e la difficoltà di *compliance* agli adempimenti previsti dall'AI Act a fronte di interpretazioni conflittuali[14].

Se prevarrà l'ipotesi di procedere in questa direzione, occorrerà, invece, verificare, nella discontinuità, dove andrà a ricadere l'individuazione di un nuovo punto di equilibrio tra la tutela dei diritti fondamentali e le ragioni del mercato.

Alla luce di queste conclusioni, appare allora ancora più evidente come lo studio del costituzionalismo digitale stia offrendo un osservatorio privilegiato per mettere a fuoco - e forse direi anche anticipare - alcune questioni che condizionano gli attuali scenari geopolitici e le relazioni internazionali. In un contesto di politica internazionale fortemente instabile, l'UE, similmente a quanto si osserva nell'ecosistema digitale, rischia purtroppo di recitare la parte del vaso di coccio in mezzo ai vasi di ferro, ruolo che, invece, ancora parimenti a quanto si osserva nella partita del mercato digitale, è interpretato dai soggetti che animano il conflitto triadico[15]: Stati Uniti, Cina e Big tech, con tutti i loro oscillanti satelliti a muoversi intorno.

[14] È possibile leggere le due lettere al seguente link: https://www.wired.it/article/ai-act-pausa-startup-europa-commissione-codice-buone-pratiche-standard/#lettera.

[15] Su questo aspetto v. D. Rodrik, *La globalizzazione intelligente*, Roma-Bari, 2011, spec. 263 ss.