# DIVERSE STRADE PER REGOLARE L'IA. ANALISI COMPARATA DELL'AI ACT EUROPEO, DELLE MISURE PROVVISORIE CINESI SULL'IA GENERATIVA E DEL COLORADO AI ACT

Dario De Lorenzo*

SOMMARIO: 1.- La regolamentazione dei sistemi di IA ai sensi dell'AI Act Europeo; 2.- L'AI Act e la nuova frontiera della regolamentazione dei modelli "General purpose"; 3.- La regolamentazione cinese dell'IA. In particolare, analisi delle Misure provvisorie per la gestione dei servizi di intelligenza artificiale generativa; 4.- Il Colorado AI Act: un modello "statale" per la regolamentazione dell'IA predittiva.

## 1.- **La regolamentazione dei sistemi di IA ai sensi dell'AI Act Europeo.**

L'impegno dell'Unione Europea nel regolamentare l'intelligenza artificiale tramite il Regolamento sull'IA (AI Act) rappresenta il primo tentativo complessivo di stabilire regole giuridiche armonizzate per lo sviluppo, la commercializzazione, l'implementazione e l'uso di sistemi di IA nell'Unione. Strutturalmente, il regolamento si presenta come un atto di regolazione del mercato interno[1], seguendo da un lato l'approccio del "new legislative framework"[2], dall'altro lato, prevedendone l'applicazione in modo congiunto rispetto a una serie di normative settoriali. In questa prospettiva, il legislatore europeo ha operato una riconduzione dell'IA alla categoria dei prodotti, strutturando il regolamento attorno al concetto di sistema di IA, allineandosi alla definizione offerta dall'OCSE[3]. Il regolamento presenta un ambito di applicazione extraterritoriale, estendendosi a tutti gli operatori[4] che introducono sistemi sul mercato dell'UE o il cui "output" venga impiegato nell'Unione salvo specifiche eccezioni[5], tra cui l'uso dei sistemi per scopi militari, difesa o sicurezza nazionale[6]. Quanto ai razionali, il regolamento adotta un approccio precauzionale riconoscendo la natura ambivalente delle tecnologie basate sull'IA, le quali, se da un lato generano benefici trasversali, dall'altro presentano potenziali criticità in termini di tutela dei diritti fondamentali e salvaguardia dell'interesse pubblico. Pertanto, obiettivo dichiarato del regolamento è quello di introdurre un insieme

* Addetto all'ufficio per il processo presso il Tribunale di Novara.

[1] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13/06/2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i Regolamenti (CE) 2008/300, (UE) 2013/167, (UE) 2013/168, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le Direttive (UE) 2014/90, (UE) 2016/797 e (UE) 2020/1828, (Regolamento sull'intelligenza artificiale). Il Regolamento segue la tendenza della Commissione europea ad utilizzare come base giuridica l'art. 114 del TFUE che riguarda il ravvicinamento delle legislazioni per migliorare il funzionamento del mercato interno, M. Carta, *Il regolamento UE sull'intelligenza artificiale: alcune questioni aperte*, in *Eurojus* 3 (2024) 192ss.

[2] L'UE adotta un paradigma normativo consolidato, integrando la regolamentazione dell'IA nel "framework" della sicurezza dei prodotti, capitalizzando su decenni di esperienza legislativa. In questo contesto l'AI Act definisce norme specifiche per l'IA, allineandosi al NLF per assicurare elevati standard di sicurezza e conformità dei prodotti AI sul mercato europeo.

[3] OECD, *Explanatory memorandum on the updated OECD definition of an AI system*, in *OECD Artificial Intelligence papers* 8 (2024).

[4] Art. 3, punto 8.

[5] L'art. 2 dell'AI Act prevede diverse esenzioni: il par. 6 esclude i sistemi sviluppati esclusivamente per ricerca e sviluppo scientifico; il par. 10 esenta i deployer che usano l'IA per fini personali e non professionali; il par. 12 esclude i sistemi open source, salvo che siano classificati come ad alto rischio o rientrino negli ambiti degli artt. 5 o 50.

[6] Art. 2, par. 3 e considerando 24. In ottica critica si veda F. Palmiotto, *The AI Act roller coaster: the evolution of fundamental rights protection in the legislative process and the future of the regulation*, in *European journal of risk regulation* (2025) 20.

proporzionato ed efficace di norme vincolanti per i sistemi di IA che, seguendo un approccio basato sul rischio[7], ne determina il regime di regolamentazione[8]. In base a tale approccio, i sistemi di IA sono classificati in tre categorie di rischio (inaccettabile, alto e minimo) con regole ad hoc per ciascuna, nonché obblighi di trasparenza per determinati sistemi di IA[9]. Al vertice della "piramide del rischio", il regolamento colloca una serie di pratiche di IA vietate, elencate nell'art. 5. Tra queste rientrano, ad esempio, la manipolazione tramite tecniche subliminali[10] (art. 5, par., lett. a) e lo sfruttamento di vulnerabilità[11] per condizionare il comportamento delle persone (art. 5, par. 1, lett. b), l'uso di sistemi di "social scoring"[12], utilizzati per «valutare o classificare persone fisiche o gruppi di persone per un certo periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note, dedotte o previste"» (art. 5, par., lett. c), nonché l'impiego di sistemi di identificazione biometrica remota "in tempo reale" negli spazi accessibili al pubblico a meno che non sia strettamente necessario per determinati obiettivi (art. 5, par., lett. h). L'elencazione dei sistemi vietati ai sensi dell'art. 5, pur qualificando l'identificazione biometrica in tempo reale come rischio inaccettabile, ha suscitato forti controversie per le ampie deroghe previste, generando un compromesso normativo ritenuto insoddisfacente da chi auspicava maggiori tutele per i diritti fondamentali[13]. Il capo III della proposta di regolamento stabilisce un regime normativo con requisiti obbligatori per i sistemi di IA ad alto rischio, definiti come quei sistemi di IA che presentano un impatto nocivo significativo per la salute, la sicurezza o i diritti fondamentali delle persone nell'UE (considerando 46). Questo regime normativo si applica a due sottocategorie di sistemi di IA ad alto rischio[14]: i sistemi di IA destinati a essere utilizzati come componente di sicurezza di un prodotto o il sistema di IA è esso stesso un prodotto (allegato I) per i quali è prevista una valutazione di conformità da parte di terzi ai fini dell'immissione o messa in servizio; i sistemi di IA elencati in uno dei settori indicati nell'allegato III. In via del tutto eccezionale, l'art. 6 prevede che i sistemi ad alto rischio non saranno considerati come tali, nonostante rientrino in una delle otto aree di cui all'allegato III, in

[7] Il concetto di rischio, ai sensi dell'art. 3, par. 2, è definito come «la combinazione della probabilità del verificarsi di un danno e la gravità del danno stesso». Il danno è valutato principalmente in relazione al suo «impatto sulla salute, sulla sicurezza e sui diritti fondamentali delle persone nell'Unione» (considerando 46), includendo altresì effetti sulla «democrazia, Stato di diritto e la protezione dell'ambiente» (considerando 2). Tale nozione comprende danni di natura materiale e immateriale, che possono manifestarsi in forma fisica, psicologica, sociale o economica (considerando 5).

[8] Sul concetto di regolamentazione basata sul rischio si veda M. E. Kaminski, *Regulating the risks of AI*, in *Boston university law review* (2023) 1403 ss.; M. Ebers, *Truly risk-based regulation of artificial intelligence. How to implement the EU's AI Act*, in *European journal of risk regulation* (2024) 6ss.

[9] In merito alla classificazione di sistemi di IA ai sensi dell'AI Act, si vedano M. Kop, *EU artificial intelligence act: The european approach to AI*, in *Transatlantic antitrust and IPR developments* 2 (2021) 8ss.; A. Gikay, P. Lau, C. Sengul, A. Miron, B. Malin, *High risk artificial intelligence systems under the european union's artificial intelligence act: systemic flaws and practical challenges*, in *Social science research network* (2023) 6.; L. A. Bygrave, R. Schmidt, *Regulating Non-High-Risk AI Systems under the EU's Artificial Intelligence Act, with Special Focus on the Role of Soft Law,* in *Research Paper* 10 (2024) 9.

[10] Sul concetto di manipolazione subliminale nel contesto nell'AI Act si veda J. R. Neuwirth, *The EU artificial intelligence Act: regulating subliminal AI systems*, I ed., London 2022, 40ss.

[11] Sul concetto di vulnerabilità nel contesto dell'IA si veda C. Novelli, F. Galli, *The many meanings of vulnerability in the AI Act and the one missing*, in *BioLaw Journal* 1s (2024) 53ss.

[12] Il concetto di "social scoring" è ampiamente riconosciuto grazie a sperimentazioni condotte prevalentemente in Cina e, in misura minore, in India. Si veda sul punto R. Schroeder, *Aadhaar and the social credit system: personal data governance in India and China*, in *International journal of communication* 16 (2022) 2370ss.

[13] Si veda S. Wachter, *Limitations and loopholes in the EU AI Act and AI liability directives: what this means for the European Union, the United States, and beyond*, in *Yale journal of law & technology* 26 (2024) 680.

[14] Art. 6 par. 1 e par. 2.

quanto non «presentano un rischio significativo di danno alla salute, alla sicurezza o ai diritti fondamentali delle persone fisiche, anche nel senso di non influenzare materialmente il risultato del processo decisionale»[15]. In questi casi, i fornitori saranno semplicemente tenuti a documentare la propria valutazione trasmettendola su richiesta all'autorità competente oltre che registrare il loro sistema in una banca dati accessibile al pubblico, ai sensi dell'art. 49 par. 2[16]. La Commissione europea ha il potere di modificare l'allegato III[17] attraverso atti delegati, aggiungendo o modificando settori o casi d'uso, previa consultazione del Parlamento e del Consiglio[18]. Inoltre, è previsto un riesame annuale dell'elenco per tenerlo aggiornato in base agli sviluppi tecnologici[19] con il coinvolgimento dell'ufficio per l'IA[20]. Sebbene nella proposta originaria la Commissione stimasse che la categoria dei sistemi di IA ad alto rischio avrebbe interessato una percentuale compresa tra il 5% e il 15% del totale[21], la maggior parte del testo dell'AI Act si concentra sulla regolamentazione dei sistemi di IA ad alto rischio, e sulla definizione dei requisiti legali di questi sistemi[22]. Ciononostante, l'AI Act muove dal presupposto che ciò non basterà a ridurre tutti i rischi a un livello accettabile: anche se i fornitori di sistemi di IA ad alto rischio rispettano i suddetti requisiti, alcuni rischi possono residuare. Da questo punto di vista, va sottolineata la centralità dell'art. 9 che prevede l'istituzione, l'attuazione, la documentazione e il mantenimento di un sistema di gestione del rischio come processo iterativo per tutto il ciclo di vita del sistema di IA ad alto rischio[23]. È importante notare che il regolamento va oltre il semplice requisito della documentazione di gestione del rischio, richiedendo che i sistemi siano testati in modo tale da individuare le misure di gestione del rischio necessarie per garantire la conformità ai vari requisiti[24]. Inoltre, mentre il processo di gestione del rischio ricade principalmente sul fornitore, quest'ultimo deve prevedere le conoscenze, l'esperienza, l'istruzione e la formazione che ci si può aspettare dal "deployer", nonché l'ambiente in cui il sistema è destinato a essere utilizzato[25]. In larga misura, gli oneri normativi ricadono sul fornitore, il quale deve attenersi agli obblighi specificati nella sezione III prima di immettere sul mercato o mettere in

[15] L'art. 6, par. 3 stabilisce i criteri che esentano dalla designazione ad alto rischio i sistemi che, non eseguendo la profilazione di persone fisiche, soddisfano uno o più dei seguenti quattro criteri: i) svolgono un compito procedurale limitato; ii) migliorano il risultato di un'attività umana precedentemente completata; iii) rilevano anomalie; iv) svolgono un lavoro preparatorio. Inoltre, ai sensi dell'art. 6, par. 5, un'ulteriore elencazione avverrà a tempo debito, poiché la Commissione è tenuta a fornire linee guida che definiscano, tra l'altro, «un elenco esaustivo di esempi pratici di casi d'uso di sistemi di IA ad alto rischio e non ad alto rischio» ai sensi dell'art. 96.

[16] Art. 6, par 4. Se l'autorità competente ha "motivi sufficienti" per ritenere che un fornitore abbia erroneamente classificato il proprio sistema come "non ad alto rischio", potrà successivamente rivedere la valutazione e richiedere al fornitore di conformarsi ai requisiti previsti per i sistemi ad alto rischio (art. 80, par. 2). La mancata conformità può comportare l'irrogazione di una multa ai sensi dell'art. 99 (art. 80, par. 7).

[17] Art. 7.

[18] Art. 112, par. 1.

[19] Art. 112, par. 10.

[20] Per una disamina dell'ambito operativo dell'ufficio per l'IA si veda C. Novelli, P. Hacker, J. Morley, J. Trondal, L. Floridi, *A robust governance for the AI Act: AI office, AI board, scientific panel, and national authorities*, in *European journal of risk regulation* (2024) 10ss.

[21] M. Almada, N. Petit, *The EU AI Act: between the rock of product safety and the hard place of fundamental rights*, in *Common market law review* 62 (2025) 91.

[22] Artt. 10-15.

[23] Per un'analisi dell'art. 9, si veda J. Schuett, *Risk management in the Artificial Intelligence Act*, in European *journal of risk regulation* 15 (2024) 367ss.

[24] Art. 9. par. 6,7 e 8.

[25] Art. 9. par. 5.

servizio un sistema ad alto rischio[26]. In subordine, i "deployer" hanno obblighi limitati, che includono la supervisione umana, la conservazione dei "log" generati automaticamente dal sistema, doveri di monitoraggio sulla base delle istruzioni fornite dal fornitore e il dovere di segnalare eventuali incidenti[27]. Per alcune applicazioni di cui all'allegato III, i "deployer" devono condurre una valutazione d'impatto sui diritti fondamentali[28] e sono soggetti a doveri di registrazione presso la banca dati di cui all'art. 71[29]. Sebbene il regolamento attribuisca la maggior parte di queste responsabilità al fornitore e ai "deployer", il corpus normativo presenta talune situazioni in cui anche altri attori sono soggetti a tali obblighi[30]. Il regolamento prescrive che i sistemi di IA ad alto rischio non devono essere immessi sul mercato o messi in servizio se non viene effettuata una valutazione *ex ante* di conformità. Le disposizioni generali in materia sono delineate nell'art. 43, il quale impone al fornitore l'obbligo di dimostrare la conformità ai requisiti stabiliti nel Titolo III, sez. 2. A tal fine, il fornitore può scegliere tra due opzioni: eseguire una valutazione di conformità interna basata sul sistema di controllo specificato nell'allegato VI[31] oppure avvalersi della verifica da parte di organismi notificati esterni, secondo le disposizioni dell'allegato VII[32]. Inoltre, i sistemi di IA richiederanno una valutazione della conformità che si baserà su norme armonizzate[33] e specifiche tecniche redatte da organizzazioni europee di normazione[34], ai quali il legislatore ha conferito notevoli poteri normativi[35], come la generazione di una presunzione di conformità[36]. Questa procedura porterà quindi alla marcatura di conformità europea (CE)[37]. Infine, il regolamento prevede un meccanismo di monitoraggio post vendita a cura dei fornitori[38] e delle autorità di vigilanza del mercato[39], chiamate a controllare la conformità del sistema dopo la sua immissione sul mercato. Nel complesso, il sistema di monitoraggio post vendita è complementare allo strumento di valutazione della conformità *ex ante* necessario per i sistemi di IA ad alto rischio, in quanto, a differenza della valutazione *ex ante*, che si limita a verificare la conformità tecnica, questo strumento permette di valutare l'impatto effettivo del sistema nel contesto reale di utilizzo[40].

[26] Artt. 16-21.
[27] Art. 26.
[28] Art. 27.
[29] Art. 49, par. 3.
[30] Artt. 22-25.
[31] Art. 46, par. 1, lett. a.
[32] Art. 46, par. 1, lett. b.
[33] Art. 40.
[34] Art. 41.
[35] L'affidamento di tali compiti a enti di diritto privato, sprovvisti di un'investitura democratica diretta, solleva significative perplessità. Si veda M. Gornet, W. Maxwell, *The European approach to regulating AI through technical standards*, in *Internet policy review* 13 (2024) 16ss.
[36] Art. 40 par. 1 e art. 41 par. 3.
[37] Art. 48.
[38] Art. 72.
[39] Artt. 74-76.
[40] Si veda sul punto J. Mokander, M. Axente, F. Casolari, L. Floridi, *Conformity assessments and post-market monitoring: a guide to the role of auditing in the proposed european AI regulation*, in *Minds and Machines* 31 (2021) 9ss.

## 2.- **L'AI Act e la nuova frontiera della regolamentazione dei modelli "General purpose".**

Sebbene la proposta originaria della Commissione europea[41] sia stata valutata come un passo importante nella direzione di un quadro normativo armonizzato per l'IA in Europa, è fondamentale notare che la sua pubblicazione è avvenuta prima dell'ampia adozione dell'IA generativa. Di conseguenza, la proposta della Commissione non fornisce una definizione chiara di IA generativa, né affronta in modo specifico i rischi associati[42]. Il cambiamento di paradigma si è avuto con il Consiglio dell'UE, che nel dicembre 2022 ha adottato il suo approccio generale all'AI Act, includendo il termine GPAI[43]. Il Consiglio ha riconosciuto i rischi associati a tali sistemi e ha aggiunto un titolo separato, introducendo norme specifiche[44]. Tuttavia, così facendo, il Consiglio ha di fatto equiparato le GPAI ai sistemi di IA ad alto rischio, con tutti gli oneri che ciò comporta[45]. Il lento avanzamento dell'*iter* legislativo in seno al Parlamento europeo ha offerto l'opportunità di considerare attentamente i nuovi progressi dell'IA generativa. La versione emendata del testo[46], invece di riconoscere tutti i modelli GPAI come ad alto rischio per impostazione predefinita, ha posto l'attenzione sulla definizione dei "foundation models"[47] e sull'imposizione di obblighi specifici per i fornitori di tali modelli. A differenza delle versioni del Consiglio e del Parlamento, che si sono concentrate sulla dicotomia GPAIS/foundation models generando non poche incertezze interpretative[48], la versione finale dell'AI Act propone ora una struttura a più livelli, prevedendo nuovi obblighi per tutti i modelli GPAI e obblighi aggiuntivi per i modelli GPAI che comportano rischi sistemici, aggiungendo così una nuova categoria di rischio alle categorie esistenti. Un modello GPAI[49] è considerato con "rischio

[41] Proposta di regolamento del parlamento europeo e del consiglio che stabilisce regole armonizzate sull'Intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione, COM/2021/206 final del 21 aprile 2021.

[42] La proposta di regolamento della Commissione si focalizza sul concetto di «finalità prevista del sistema di intelligenza artificiale». Mentre molti sistemi di IA sono definiti da uno scopo fisso, permettendone la categorizzazione in base al rischio, i sistemi di IA per scopi generali (GPAIS), come definiti dall'UE, sfidano questa premessa, potendo essere utilizzati per un'ampia varietà di scopi a valle, spesso imprevedibili in anticipo. Si veda sul punto, C. I. Gutierrez, A. Aguirre, R. Uuk, C. C. Boine, M. Franklin, *A proposal for a definition of general purpose artificial intelligence systems*, in *Digital society* 2 (2023) 3ss.

[43] Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain Union legislative acts -General approach, 14954/22, art. 3, punto 1b.

[44] Il Titolo Ia introduce obblighi specifici per i fornitori di GPAIS, prevedendo che i sistemi potenzialmente impiegabili in contesti ad alto rischio rispettino i requisiti del Titolo III, Capo 2, tra cui gestione del rischio, governance dei dati, documentazione tecnica, trasparenza, accuratezza, robustezza e cibersicurezza, al fine di garantire una equa ripartizione delle responsabilità lungo la catena del valore dell'IA.

[45] P. Hacker, A. Engel, M. Mauer, *Regulating ChatGPT and other large generative AI models*, in *proceedings of the 2023 ACM conference on fairness, accountability and transparency* (2023) 1114.

[46] Amendments adopted by the European Parliament on 14 June 2023 on the Proposal for a Regulation of the European Parliament and of the Council on Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (COM (2021)0206 – C9-0146/2021 – 2021/0106(COD)).

[47] Il termine "foundation model" è stato introdotto dallo Stanford institute for human centered artificial intelligence nell'agosto 2021. Tale concetto si riferisce a un nuovo paradigma di apprendimento automatico in cui un modello di grandi dimensioni viene pre addestrato su un'enorme quantità di dati e può essere utilizzato per molte attività e applicazioni a valle.

[48] Per una rassegna dei concetti di sistema di IA per scopi generali, foundation model e IA generativa nelle diverse versioni del testo della Commissione, del Parlamento e del Consiglio si veda D. F. Llorca, E. Gómez, I. Sánchez, G. Mazzini, *An interdisciplinary account of the terminological choices by EU policymakers ahead of the final agreement on the AI Act: AI system, general purpose AI system, foundation model, and generative AI*, in *Artificial intelligence and law* (2024) 5ss.

[49] Art. 3, punto 63.

sistemico"[50] qualora presenti "capacità di impatto elevato" oppure qualora sia identificato come tale dalla Commissione[51]. Si presume che un modello GPAI abbia capacità ad alto impatto qualora la quantità di potenza di calcolo, misurata in operazioni in virgola mobile sia maggiore di 10^25[52]. Sebbene la Commissione preveda di adeguare queste soglie classificatorie in risposta all'evoluzione tecnologica[53], sono già emerse preoccupazioni riguardo alla fissazione della soglia di 10^25 FLOPs per la categorizzazione predefinita dei modelli a rischio sistemico[54]. I fornitori, il cui modello soddisfa tale condizione, devono notificarlo alla Commissione entro due settimane dal raggiungimento della soglia, o prima, dal momento in cui ne prendono conoscenza[55]. Questi fornitori possono, tuttavia, scegliere di presentare argomentazioni alla Commissione per spiegare perché la loro GPAI non presenta un rischio sistemico[56]. Se la Commissione designa un modello GPAI come modello a rischio sistemico, può tuttavia, su richiesta del fornitore, rivalutare siffatta designazione[57]. La Commissione dovrà garantire che un elenco di GPAI con rischi sistemici sia pubblicato e aggiornato, a condizione che il materiale pubblicato non violi i diritti di proprietà intellettuale o riveli informazioni commerciali riservate o segreti commerciali[58]. Tutti i fornitori di GPAI, indipendentemente dal rischio che rappresentano, sono soggetti ad alcuni obblighi minimi[59]. Per i modelli GPAI con rischi sistemici, l'AI Act prevede regole più stringenti, tra cui valutazioni del modello, gestione dei rischi sistemici, test avversari, gestione degli incidenti e misure correttive[60]. In questa fase transitoria, al fine di attestare l'adempimento degli obblighi inerenti ai fornitori di modelli GPAI a rischio sistemico, sarà consentito l'utilizzo di codici di condotta fino all'adozione di "standard" armonizzati che, anche in questo caso, determinerà una presunzione di conformità[61].

## 3.- **La regolamentazione cinese dell'IA. In particolare, analisi delle Misure provvisorie per la gestione dei servizi di intelligenza artificiale generativa.**

Se da un lato, il vantaggio della prima mossa in termini di regolamentazione tecnologica è significativo, dall'altro, l'UE non è sola in questo caso. Anche la Cina ha compiuto sforzi significativi, confermando così le proprie ambizioni in questo campo[62]. Sebbene entrambe abbiano sviluppato strategie di sviluppo dell'IA in tempi analoghi, i loro approcci alla "governance" dell'IA divergono in modo significativo. L'approccio europeo, delineato nell'AI Act, si basa su un modello regolatorio *omnibus*[63], adottando un quadro normativo che affronta in modo sistematico le implicazioni dell'IA,

[50] Art. 3, punto 65. Il considerando 110 fornisce esempi di modelli di IA che potrebbero comportare rischi sistemici.
[51] Art. 51 par. 1.
[52] Art. 51 par. 2.
[53] Art. 51 par. 3.
[54] In particolare, si vedano Almada, Petit, *The EU*, cit. 102ss.; Wachter, *Limitations*, cit. 715ss.; Novelli, Casolari, Hacker, Spedicato, Floridi, *Generative* cit. 3.
[55] Art. 52, par. 1.
[56] Art. 52, par. 2.
[57] Art. 52, par. 5.
[58] Art. 52, par. 6.
[59] Art. 53.
[60] Art. 55, par.1.
[61] Art. 55, par. 2.
[62] Per una panoramica si veda H. Roberts, J. Cowls, J. Morley, M. Taddeo, V. Wang, L. Floridi, *The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation*, in *AI & Society* 36 (2021) 60ss.
[63] M. Sloane, E. Wüllhorst, *A systematic review of regulatory strategies and transparency mandates in AI regulation in Europe, the United States, and Canada*, in *Data & policy 7* (2025) 11.

applicandosi trasversalmente a tutti i settori e tipologie di IA. Al contrario, la "governance" cinese adotta un modello prevalentemente "verticale", caratterizzato da regolamentazioni settoriali mirate e da un approccio "iterativo", con aggiornamenti continui volti a colmare lacune ed estendere l'ambito di applicazione delle disposizioni esistenti[64]. Inoltre, mentre l'Europa ha incentrato il dibattito politico sulla necessità di mitigare i rischi derivanti dall'adozione diffusa dell'IA, la Cina ha inizialmente privilegiato lo sfruttamento del suo potenziale innovativo, orientandosi verso una visione più espansiva e mirata alla crescita tecnologica[65]. Tuttavia, questa distinzione si sta gradualmente attenuando: il governo cinese, infatti, ha iniziato a dimostrare una crescente cautela, adottando un approccio più equilibrato che integra considerazioni sui possibili danni. Un esempio tangibile di questo paradigma regolatorio è rappresentato dalle "Interim Measures for the Management of Generative Artificial Intelligence Services"[66] (Misure provvisorie), che introducono una serie di obblighi per i fornitori di servizi di IA generativa, spaziando dalla moderazione dei contenuti alla gestione dei dati di addestramento e alla protezione degli utenti. Analizzando le disposizioni pertinenti l'ambito territoriale, si può notare che le Misure provvisorie operano una distinzione tra tecnologia di IA generativa "orientata al pubblico" e "non orientata al pubblico"[67]. Le Misure sono state concepite principalmente per i servizi di IA generativa offerti al pubblico cinese per la generazione di contenuti quali testi, immagini, audio o video[68], mentre settori come la ricerca scientifica e le applicazioni industriali sono esentati dalla normativa, sottolineando l'impegno del paese nel promuovere la ricerca e l'innovazione sull'IA generativa[69]. Inoltre, le Misure provvisorie mirano a disciplinare l'uso di servizi di IA generativa in Cina, indipendentemente dal fatto che siano offerti da organizzazioni nazionali o internazionali. Pertanto, i fornitori di servizi di IA generativa, che siano nazionali o meno, purché forniscano direttamente servizi al pubblico cinese o indirettamente tramite API, rientrano nell'ambito di applicazione della normativa[70]. Per quanto concerne la protezione dei dati, poiché i dati utilizzati per l'addestramento influenzano direttamente i risultati prodotti, diventano naturalmente un elemento centrale di regolamentazione[71]. Pertanto, i fornitori devono assicurare la

[64] Come sottolineato da M. Sheehan*, China's AI regulations and how they get made* (2023) 16, «se il governo ritiene che un regolamento che ha emanato sia viziato o insufficiente, ne rilascerà semplicemente uno nuovo che colmerà i buchi o amplierà la portata, come ha fatto con il progetto di regolamento sull'intelligenza artificiale generativa che espande le misure di sintesi profonda». Si veda sul punto https://carnegieendowment.org/2023/07/10/china-s-ai-regulations-and-how-they-get-made-pub-90117.

[65] H. Roberts, J. Cowls, E. Hine, J. Morley, V. Wang, M. Taddeo, L. Floridi, *Governing artificial intelligence in China and the European Union: Comparing aims and promoting ethical outcomes*, in *The Information Society 39* (2022) 82ss.

[66] Interim Measures for the Management of Generative Artificial Intelligence Services (2023), disponibile al seguente indirizzo https://www.chinalawtranslate.com/en/generative-ai-interim/.

[67] Art. 2.

[68] Art. 22, par. 1.

[69] Art. 2 par. 3. Questa ampia esclusione è estremamente importante anche perché nell'ambito dei servizi di IA rivolti al pubblico, le misure provvisorie prevedono l'obbligo di licenza per quei soli servizi che hanno il potenziale di influenzare l'opinione pubblica (art. 17).

[70] Come sottolineato da G. Abiri, Y. Huang, *A red flag? China's generative AI dilemma*, in *Harvard journal of law & technology* 37 (2023) 13, tale l'approccio sembra avere due obiettivi principali. In primo luogo, una politica protezionistica per ridurre la dipendenza della Cina dalle piattaforme straniere di IA e, in secondo luogo, garantire una fornitura stabile di servizi di IA da parte di fornitori internazionali per evitare interruzioni nei processi di produzione e distribuzione.

[71] Le Misure provvisorie sono strettamente connesse alla legge sulla sicurezza dei dati. Come chiarito all'art. 1, esse si basano sulla legge sulla sicurezza dei dati, sulla legge sulla protezione delle informazioni personali e su altri regolamenti amministrativi. L'art. 7, impone ai fornitori il rispetto di tali normative e dei requisiti stabiliti dalle autorità competenti, mentre l'art. 21 prevede sanzioni per le violazioni delle disposizioni in materia.

legittimità delle fonti dei dati, il rispetto dei diritti di proprietà intellettuale, il consenso degli interessati in caso di trattamento di dati personali (art. 7), adottare procedure rigorose per l'etichettatura dei dati e la formazione del personale (art. 8). Il capitolo III delle Misure provvisorie introduce ulteriori obblighi per i fornitori di servizi di IA generativa. Nella fornitura di servizi, la prima responsabilità del fornitore è quella di agire come produttore di contenuti informativi online e di adempiere agli obblighi di sicurezza delle informazioni online[72]. Nel caso in cui siano coinvolte informazioni personali, i fornitori dovranno attenersi agli obblighi di protezione delle informazioni personali[73]. Tra il fornitore di servizi e gli utenti che si registrano ai suoi servizi deve essere stipulato un contratto di servizio[74]. L'art. 10 delle misure introduce una serie di previsioni "anti dipendenza" stabilendo che fornitori di servizi devono dichiarare chiaramente la popolazione target e lo scopo del loro servizio nonché attuare misure efficaci per evitare che gli utenti minorenni diventino dipendenti da tali servizi. L'art. 12 impone ai fornitori di etichettare i contenuti generati, comprese immagini e video, per garantire la trasparenza e consentire agli utenti di riconoscere e filtrare i contenuti prodotti dall'IA, mentre l'art. 14 richiede un intervento tempestivo in presenza di contenuti illegali, mediante la loro rimozione, l'adeguamento dei modelli e la notifica alle autorità competenti. Infine, i fornitori devono istituire un meccanismo per ricevere e gestire i reclami degli utenti[75] e devono collaborare con le autorità competenti che effettuano ispezioni di supervisione, fornendo informazioni su come funzionano i loro sistemi, spiegando in particolare la provenienza dei dati utilizzati, tipi di dati utilizzati, modelli utilizzati e regole di etichettatura impiegate[76].

## 4.- **Il Colorado AI Act: un modello "statale" per la regolamentazione dell'IA predittiva.**

Nonostante il peso globale della nazione e la crescente pervasività dell'IA nel settore sia privato che pubblico, gli Stati Uniti hanno finora evitato interventi regolatori in stile UE[77], riponendo fiducia nella capacità delle aziende di autoregolarsi[78]. Se il governo federale ha adottato un approccio ampiamente non interventista, le legislature statali hanno iniziato a implementare leggi che riguardano l'innovazione dell'IA e la tutela dei consumatori. Il Colorado Act concerning consumer

[72] Art. 9. In base alle «Provisions on the governance of the online information content ecosystem", per "produttori di contenuti informativi online» si intendono organizzazioni o individui che realizzano, riproducono o pubblicano contenuti informativi online. L'art. 6 vieta loro di creare, riprodurre o pubblicare informazioni illegali, mentre l'art. 7 impone ai produttori di contenuti informativi online di adottare misure per prevenire e contrastare la creazione, la riproduzione o la pubblicazione di informazioni dannose.

[73] Le Misure provvisorie pongono particolare attenzione alla protezione delle informazioni personali, imponendo ai fornitori l'obbligo di ottenere il consenso dell'interessato (art. 7, par. 3), proteggere i dati inseriti dagli utenti e i relativi record di utilizzo, evitare raccolte non necessarie, archiviazioni illecite e condivisioni non autorizzate (art. 11, par. 1), e di gestire tempestivamente le richieste di accesso, modifica o cancellazione dei dati (art. 11, par. 2).

[74] Art. 9, par. 2.

[75] Art. 15. Si veda sul punto anche l'art. 18.

[76] Art. 19.

[77] Alcuni autori interpretano la prolungata assenza di un quadro normativo per l'IA negli Stati Uniti come una perdita dell'opportunità di generare un "Washington effect", che avrebbe potuto influenzare positivamente l'ecosistema digitale globale, considerando il potere economico e l'influenza del Paese nel settore dell'IA. Si veda sul punto J. Mökander, P. Juneja, D.S. Watson, L. Floridi, *The US Algorithmic Accountability Act of 2022 vs. The EU Artificial Intelligence Act: what can they learn from each other*, in *Minds & machines* 32 (2022) 755.

[78] Gli Stati Uniti adottano infatti un approccio "market driven" alla regolamentazione del digitale, delegando la definizione di regole e restrizioni tecnologiche all'industria anziché allo Stato, convinti che tale strategia sia la più efficace per non ostacolare l'innovazione. Si veda sul punto A. Bradford, *Digital empires: The global battle to regulate technology*, New York 2023, 33ss.

protections in interactions with artificial intelligence systems (CAIA), introduce tutele per i consumatori nell'uso dei sistemi di IA e, sebbene presenti analogie con l'AI Act europeo, risulta meno rigoroso e più circoscritto nei suoi ambiti di applicazione. Mentre il regolamento europeo adotta un approccio più ampio, con un quadro dettagliato basato sul rischio applicabile a più settori e giurisdizioni, il CAIA regola specificamente gli sviluppatori e i "deployer" di "sistemi di IA ad alto rischio", che operano commercialmente all'interno dello stato del Colorado, definiti come «qualsiasi sistema di intelligenza artificiale che, una volta implementato, prende, o è un fattore sostanziale nel prendere, una decisione consequenziale»[79]. Il CAIA pone l'accento sulla prevenzione della "discriminazione algoritmica" ossia ogni impatto o trattamento differenziale illecito derivante dall'uso di sistemi di IA che svantaggi individui o gruppi in base all'appartenenza effettiva o percepita a classi protette (es. etnia, sesso, disabilità)[80]. Sia gli sviluppatori che i "deployer" di sistemi di IA ad alto rischio devono adottare una "cura ragionevole" per proteggere i consumatori da «qualsiasi rischio noto o ragionevolmente prevedibile di discriminazione algoritmica derivante dagli usi previsti e contrattualizzati» del sistema di IA ad alto rischio[81]. Gli sviluppatori devono rispettare diversi requisiti di trasparenza, come stabilito nella sez. 6-1-1702. In particolare, devono fornire ai "deployer" una dichiarazione generale che descrive gli usi previsti e i rischi noti del sistema, insieme ad una documentazione dettagliata che include informazioni per la conformità, valutazioni delle prestazioni e ulteriori documenti ragionevolmente necessari affinché l'utilizzatore comprenda gli "output" del sistema e ne monitori le prestazioni per rischi. Inoltre, devono pubblicare sul proprio sito web una dichiarazione pubblica che riassume i sistemi di IA ad alto rischio offerti e le strategie di gestione dei rischi. Un obbligo cruciale è la notifica di discriminazione algoritmica: entro 90 giorni dalla scoperta di rischi di discriminazione, gli sviluppatori devono comunicare tali rischi al Procuratore Generale e a tutti gli utilizzatori noti. Gli utilizzatori, da parte loro, devono adottare politiche e programmi di gestione del rischio per governare l'uso dei sistemi di IA ad alto rischio, come previsto dalla Sezione 6-1-1703. In particolare, il CAIA richiede agli utilizzatori di IA ad alto rischio di adottare programmi aggiornati per identificare e mitigare la discriminazione algoritmica, condurre valutazioni di impatto annuali e dopo modifiche sostanziali al sistema, pubblicare una sintesi dei sistemi utilizzati e notificare eventuali discriminazioni al Procuratore Generale entro 90 giorni. Inoltre, impone obblighi di trasparenza verso gli individui coinvolti in decisioni consequenziali, garantendo diritto all'informazione, alla rettifica dei dati, al ricorso e, se tecnicamente possibile, a una revisione umana della decisione.

**Abstract.-** Il presente articolo offre un'analisi comparata di tre principali modelli di regolamentazione dell'IA. In primo luogo, viene analizzato l'AI Act europeo, che mira a creare un ambiente normativo completo per l'IA all'interno dell'UE, stabilendo un punto di riferimento globale. Successivamente, l'indagine si focalizza sulla risposta normativa cinese all'IA generativa, anche alla luce delle sue differenze rispetto all'IA ACT. L'analisi si conclude con l'esame del Colorado AI Act, quale prima legislazione statale completa sull'IA predittiva negli Stati Uniti, con il potenziale di

[79] Sez. 6-1-1701(9a).
[80] Sez. 6-1-1701(1)
[81] Sez. 6-1-1702 e sez. 6-1-1703.

fungere da modello per normative analoghe in altri Stati e di favorire l'elaborazione di un quadro normativo nazionale sull'IA.

This article provides a comparative analysis of three major AI regulatory models. First, it examines the European AI Act, which aims to create a comprehensive regulatory framework for AI within the EU, establishing a global benchmark. Next, the study focuses on China's regulatory response to generative AI, highlighting its differences compared to the AI Act. The analysis concludes with a review of the Colorado AI Act, the first comprehensive state legislation on predictive AI in the United States, with the potential to serve as a model for similar regulations in other states and to support the development of a national AI regulatory framework.