La regolazione dell'Intelligenza Artificiale: le fasi della sua applicazione*

di Federico Marini Balestra

Sommario: 1. Regolare le diverse fasi di un sistema di IA per raggiungere l'ecosistema di fiducia: spunti comparatistici; 2. La fase di sviluppo; 3. La fase di diffusione; 4. La fase di utilizzo delle tecnologie e dei loro componenti.

1. *Regolare le diverse fasi di un sistema di IA per raggiungere l'ecosistema di fiducia: spunti comparatistici*

Come correttamente affermato nel precedente intervento (Ruffolo-Amidei), non sembra possibile immaginare di ricorrere a forme di "*one-size-fits-all solution*" in tema di regolazione dell'intelligenza artificiale ("IA").

La necessaria granularità dell'intervento regolamentare ci conduce ad affrontare una particolarità della materia di cui, *de jure condendo*, il legislatore deve tenere conto, onde evitare di indulgere, da un lato, in dannosi eccessi di regolazione e, dall'altro, nell'adozione di strumenti di controllo inadeguati.

Infatti, il funzionamento di un sistema di IA è il risultato di un ciclo di vita distinto in varie fasi di cui è complesso fornire una definizione univoca. Come affermato in letteratura, risulta difficile "*stabilire che cosa sia, esattamente, l'IA ad ogni sua fase*"[1] e, quando esattamente, essa prende "vita propria", potendo liberarsi dal controllo umano.

Quest'ultimo fattore rappresenta un significativo elemento di novità, che richiede un approccio normativo diversificato a seconda dei vari passaggi che costituiscono il ciclo di vita di un sistema di IA nella pressoché impossibilità (e anche inutilità) di individuare una regolazione univoca per ciascuna di tali fasi[2].

---

* Il presente scritto è stato elaborato nel contesto di una ricerca Astrid su Intelligenza artificiale e diritto, ed è stato pubblicato in ASTRID, "Intelligenza artificiale e diritto: una rivoluzione? Diritti fondamentali, dati personali e regolazione", a cura di Filippo Donati, Alessandro Pajno, Antonio Perrucci, vol. I, Ed. il Mulino, Bologna, 2022

[1] M. U. Scherer, *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies and Strategies*, Harvard Journal of Law and Technology, Volume 29, Number 2 Spring 2016, p. 357.

[2] *Ibidem*, p. 360.

La grande sfida legislativa/regolamentare dell'IA è, perciò, legata al fatto che, a differenza di altre tecnologie che pure hanno necessitato di interventi normativi *ad hoc*, pur essendo l'IA un prodotto umano, in quanto sviluppata, diffusa ed utilizzata da esseri umani, essa, ad un certo punto del suo sviluppo, è potenzialmente atta a sfuggire al controllo umano stesso.

Il dibattito sulla necessità e proporzionalità della regolazione dell'IA si deve necessariamente ramificare in tanti sub-livelli quanti sono gli stadi di vita di un sistema di IA, tenendo conto delle loro caratteristiche e relativi impatti sul bene giuridico tutelato.

Ogni legislatore che intenda regolamentare l'IA deve quindi definire preliminarmente le tre principali fasi dell'IA: il suo sviluppo, la sua diffusione e l'utilizzo delle relative tecnologie e dei loro componenti.

Tanto maggiore è il rischio che il prodotto o il servizio di IA possano sfuggire al controllo umano, tanto più stringente dovrà essere l'intervento umano volto ad assicurarne la regolazione in una o più fasi del suo ciclo di vita.

A livello europeo, questa esigenza di regolare ciascuna fase dell'IA è stata avvertita come un prerequisito fondamentale per poter realizzare quell'"*ecosistema di fiducia*" delineato nel Libro Bianco sull'Intelligenza Artificiale della Commissione Europea[3].

Tale ecosistema è l'asso portante di un ambizioso intervento normativo europeo volto a fissare gli standard internazionali in materia di regolazione dell'IA.

La (auspicabilmente) conseguente certezza giuridica risulta necessaria non solo per scongiurare la frammentazione del mercato interno in materia di servizi digitali, ma anche per rendere l'Unione Europea competitiva sul mercato globale grazie all'applicazione di regole chiare, robuste ma flessibili al tempo stesso[4], che si applichino a tutti i soggetti coinvolti nelle diverse fasi che caratterizzano l'IA.

L'obiettivo è realizzare un "*ecosistema di fiducia*", fondato sui valori europei e antropocentrico, che, da un lato, crei fiducia nel cittadino che utilizza il sistema di IA nella sua vita quotidiana e che, dall'altro, assicurando certezza giuridica, renda più semplice per le PMI investire nello sviluppo e nella diffusione dell'IA.

Nella prospettiva europea, per garantire tale *patto fiduciario* è necessario adottare un approccio regolatorio, che tenga conto delle specificità di ogni singolo passaggio di vita di un sistema di IA.

---

[3] Commissione Europea, *Libro Bianco sull'Intelligenza Artificiale: Un approccio europeo all'eccellenza e alla fiducia*, Bruxelles, 19.2.2020, COM(2020) 65 final, disponibile all'indirizzo: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_it.pdf.

[4] Commissione Europea, *Libro Bianco sull'Intelligenza Artificiale: Un approccio europeo all'eccellenza e alla fiducia,* (cfr. nota 3).

L'esigenza di promuovere la fiducia dei consociati nei sistemi di IA è avvertita anche al di là dell'Atlantico.

Interessante notare sin da subito le differenze di prospettiva, che poi spiegano le differenze metodologiche ipotizzate, anche con riferimento alle diverse fasi del ciclo di vita dei sistemi di IA.

In particolare, il Memorandum "*Guidance for Regulation of Artificial Intelligence Applications*" pubblicato il 17 novembre 2020 dall'*Office of Science and Technology Policy* della Casa Bianca[5], pone sì come principio cardine delle linee guida statunitensi il *public trust,* declinato però non in chiave antropocentrica, ma come prerequisito fondamentale per stimolare l'innovazione e la diffusione dell'IA, di per sé considerata benefica.

La fiducia, quindi, viene considerata come un fattore che la regolamentazione deve stimolare, dal momento che "*la continua adozione ed accettazione dell'IA dipenderà significativamente dalla fiducia pubblica*".

Il *public trust,* nella prospettiva statunitense, si fonda sulla consapevolezza degli effetti positivi che l'IA è in grado di generare, piuttosto che sulla stretta regolamentazione dei rischi ad essa collegati in ciascuna fase di sviluppo dei sistemi di IA.

In altri termini, l'approccio regolamentare europeo è più ideologico (*human-based*), mentre quello USA è più utilitaristico (*business-oriented*).

Più recentemente, nell'ottobre 2021, l'*Office of Science and Technology Policy* ("OSTP") della Casa Bianca ha richiamato l'attenzione, anche oltreoceano, sui potenziali fallimenti dell'IA, ritenendo necessario codificare "*i valori democratici che le potenti tecnologie dovrebbero essere obbligate a rispettare*".

Tale codificazione, nella strategia delineata dall'OSTP, prenderà la forma di un "*Bill of Rights for an Automated Society*" che possa fare da "guardiano" alle moderne tecnologie, garantendo che queste ultime rispettino, e rispecchino al tempo stesso, i valori e le libertà sulle quali si fonda la società statunitense.

Il primo atto di tale processo di codificazione è stato avviato il 13 ottobre 2021, con la pubblicazione, da parte dell'OSTP, di una "*Request for information*" sugli utilizzi del settore pubblico e privato delle tecnologie biometriche[6], in considerazione della loro rapida evoluzione e della loro crescente diffusione. A tale prima iniziativa, si

[5] Memorandum for the Heads of Executive Departments and Agencies of 17 November 2020, *Guidance for Regulation of Artificial Intelligence Applications*, disponibile all'indirizzo: https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf.

[6] Office of Science and Technology Policy, *Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies,* disponibile all'indirizzo: https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies.

affiancheranno una serie di eventi volti ad avviare un dibattito quanto più ampio possibile in relazione ai rischi e ai benefici che l'IA possa determinare per la vita democratica.

La necessità di introdurre un "*Bill of rights*" mirato per l'IA sembra dunque suggerire che anche un approccio maggiormente *business-oriented,* quale quello statunitense, non possa di fatto ignorare i rischi inevitabilmente associati all'utilizzo dell'IA e la necessità di fondare tale tecnologia su parametri valoriali certi e predefiniti.

L'approccio antropocentrico e di regolamentazione "per fasi", già adottato dall'Unione europea, caratterizza anche il dibattito politico sull'IA, attualmente in corso in Australia (giugno 2021).

Pur non essendo stata ancora presentata una proposta di legge vincolante, il Governo australiano ha presentato un quadro etico di riferimento per l'IA ("*Ethics Framework*")[7], che rileva l'esigenza di assicurare, in ogni fase del ciclo di vita di un sistema di IA, il rispetto di una serie di principi, quali: i diritti fondamentali, l'autonomia individuale; il benessere umano, sociale e ambientale; la trasparenza per assicurare che non vi sia discriminazione tra individui o comunità; la protezione della *privacy* e la sicurezza dei dati; l'affidabilità e la sicurezza al fine di garantire che i sistemi di IA vengano utilizzati per le finalità prefissate.

Nelle intenzioni del governo australiano, l'*Ethics Framework* costituirà una linea di orientamento volontaria per incoraggiare le imprese australiane a sviluppare sistemi di IA che siano in linea con i principi etici sopra menzionati.

La strategia australiana, ulteriormente delineata nell'*AI Action Plan* che ha fatto seguito all'*Ethics Framework*, si basa quindi su un'idea di *ethics by design*: la fiducia nell'IA si costruisce a partire da principi etici ben definiti, il cui rispetto deve essere assicurato in ogni fase del ciclo di un sistema IA.

Anche la proposta legislativa approvata in data 29 settembre 2021 dalla Camera dei Deputati brasiliana (attualmente, in discussione al Senato)[8] si inserisce nel solco dell'approccio antropocentrico e basato sul rischio tracciato dall'UE.

La normativa in esame stabilisce, infatti, che l'IA deve basarsi sul rispetto dei diritti umani e dei valori democratici, l'uguaglianza, la non discriminazione, la pluralità, la libera impresa e la *privacy* dei dati, nella convinzione che tali standard, condivisi a

[7] *Australian Government, Department of Industry, Science, Energy and Resources*, *AI Ethics Framework*, disponibile all'indirizzo: https://www.industry.gov.au/data-and-publications/building-australias-artificial-intelligence-capability/ai-ethics-framework.

[8] Camara dos Deputados, Projeto de Lei n° 21 de 2020, *Estabelece princípios, direitos e deveres para o uso de inteligência artificial no Brasil, e dá outras providências*, disponibile all'indirizzo: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1853928.

livello internazionale, costituiscano solidi punti di partenza per la regolamentazione dell'IA anche nel paese sudamericano.

Infine, pur essendo ultima in ordine di tempo per pubblicazione (agosto 2021), la proposta di Regolamento sulla gestione delle raccomandazioni algoritmiche dell'Ufficio della Commissione Centrale per gli Affari del Cyberspazio della Repubblica Popolare Cinese [9] presenta elementi di distacco rispetto ai sopracitati esperimenti regolamentari in materia di IA.

Come suggerisce la denominazione stessa del Regolamento, il primo intervento legislativo cinese in materia di IA ha come *target* principale la regolamentazione dei cosiddetti algoritmi di raccomandazione, tra cui rientrano i filtri di ricerca, gli algoritmi di raccomandazione personalizzata utilizzati dalle piattaforme *e-commerce* o dai *social media*, e gli algoritmi decisionali e di dispacciamento (sempre più presenti nei servizi di spedizione e di trasporto).

Sebbene richiami direttamente "*i principi di equità e giustizia, apertura e trasparenza, scienza e ragione, sincerità e affidabilità*" che i fornitori di servizi basati su algoritmi di raccomandazioni sono tenuti a rispettare, la proposta di Regolamento cinese non si caratterizza per la formulazione di un minimo comune denominatore valoriale sul quale fondare gli algoritmi oggetto delle nuove previsioni normative.

La bozza di Regolamento mira non tanto a creare uno standard imprescindibile di valori, quanto piuttosto a standardizzare gli algoritmi di raccomandazione, eliminandone le potenzialità di personalizzazione, con il fine ultimo di "salvaguardare la sicurezza nazionale e gli interessi pubblici sociali" e proteggere i cittadini. Si configurerebbe dunque in questo caso un'ipotesi di approccio Stato-centrico, che si differenzia dai modelli antropocentrici già analizzati.

2. *La fase di sviluppo*

Il momento di sviluppo di un sistema IA rappresenta potenzialmente la fase più rischiosa dal momento che è in questa sede che il sistema di IA prende forma, che ne vengono determinati i limiti e i livelli di autonomia *pro-futuro*. È in questo passaggio, dunque, che si determina il grado di prevedibilità delle operazioni di un sistema di IA.

A differenza di quanto avviene per altre tecnologie, lo sviluppo di un sistema basato sull'IA risulta quindi un passaggio estremamente delicato dal momento che dalle decisioni compiute dai suoi sviluppatori dipenderanno direttamente i rischi che caratterizzeranno il sistema di IA nelle fasi successive del suo ciclo vitale.

[9] Cyberspace Administration of China (CAC), *Guiding Opinions on Strengthening the Comprehensive Governance of Internet Information Service Algorithms*, disponibile all'indirizzo: http://www.cac.gov.cn/2021-09/29/c_1634507915623047.htm.

Avere controllo di questa fase, da un punto di vista regolatorio, significa anche poter tracciare a ritroso più facilmente l'intera catena di eventi che potrebbero aver determinato un evento dannoso.
Il dibattito legislativo attorno a questa prima fase si è concentrato, principalmente, su due aspetti: la gestione e la qualità dei dati, imprescindibili per la creazione di ogni sistema di IA, e la questione della responsabilità del produttore.
Con riferimento al primo aspetto, come a più riprese sottolineato dalla Commissione Europea, l'IA è "*una delle più importanti applicazioni dell'economia dei dati*"[10].
La natura e la qualità di tali dati riveste dunque un ruolo centrale nella fase di elaborazione di qualsivoglia sistema di IA, nonché un aspetto determinante per la crescita futura di questa tecnologia.
Per tale motivo, a livello europeo, la discussione sulla regolazione dell'IA è stata condotta di pari passo con l'elaborazione di una Strategia europea sui dati[11].
Nel Libro Bianco sull'IA, la Commissione Europea ha ritenuto necessario, come punto di partenza nello sviluppo dei sistemi di IA, stabilire principi generali sulla base dei quali valutare la conformità dei dati utilizzati.
Tali principi sono sintetizzati con l'acronimo di FAIR: *findable, accessible, interoperable and reusable data*[12].
Secondo la Commissione Europea, il rispetto di tali principi contribuirebbe alla "*promozione di pratiche responsabili in materia di gestione dei dati*" [13] e, di conseguenza, potrebbe facilitare il raggiungimento dell'obiettivo di creare un'"*ecosistema di fiducia*" in materia di IA.
L'utilizzo di dati facilmente rintracciabili ed accessibili, infatti, dovrebbe evitare il formarsi di "*asimmetrie informative nel processo decisionale algoritmico*" [14] che possano, a loro volta, determinare il sorgere di sistemi di IA imparziali o discriminatori che vengano dunque a minare la fiducia del singolo cittadino nei confronti di questa tecnologia sempre più diffusa.

[10] Commissione Europea, *Libro Bianco sull'Intelligenza Artificiale: Un approccio europeo all'eccellenza e alla fiducia,* (cfr. nota 3).
[11] Commissione Europea, Strategia europea in materia dei dati, disponibile all'indirizzo: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_it.
[12] Gruppo di esperti della Commissione sui dati FAIR, *Relazione finale e piano d'azione*, 2018, disponibili all'indirizzo: https://ec.europa.eu/info/sites/info/files/turning_fair_into_reality_1.pdf.
[13] Commissione Europea, *Libro Bianco sull'Intelligenza Artificiale: Un approccio europeo all'eccellenza e alla fiducia*, p. 9.
[14] *Ibidem*, p.10.

La c.d. "*etica dei dati*" risulta un punto di partenza fondamentale per ancorare lo sviluppo dell'IA ai valori europei, garantendone la trasparenza, la diversità, la non discriminazione e l'equità sin dalla sua fase embrionale.
Inoltre, la determinazione, a livello legislativo, di principi cardine chiari e certi, che regolino l'utilizzo dei dati nella progettazione del sistema di IA, risulta necessaria in virtù della rapida evoluzione delle tecnologie di IA e della relativa esigenza di stabilire un quadro normativo che sia in grado di adattarsi a tali futuri sviluppi. Si tratta, cioè, di fissare un sostrato valoriale di base che resista agli sviluppi tecnologici.
Il secondo aspetto che necessita di una revisione dell'attuale set di norme attiene al profilo della responsabilità.
Il principale intervento sotto questo profilo è rappresentato dalla Relazione del Parlamento Europeo contenente raccomandazioni per la Commissione su un regime di responsabilità civile per l'intelligenza artificiale[15].
In ragione delle peculiarità dell'IA, per cui vi è un rischio concreto che il sistema possa compiere azioni che vadano al di là delle previsioni dei suoi sviluppatori, risulta particolarmente difficile stabilire un nesso certo tra il danno causato e il soggetto a cui tale danno sia imputabile.
Il quadro normativo di riferimento, in materia di responsabilità civile, è costituito dalle Direttive sulla *Product Liability* ("PLD") e sulla *General Product Safety* ("GPSD")[16], le quali prevedono, come principio generale, una responsabilità in capo al produttore in caso di prodotto difettoso.
Secondo la citata Relazione del Parlamento Europeo, la PLD dovrà continuare ad essere applicata in riferimento alla responsabilità civile di un produttore di un sistema di IA difettoso, quando tale sistema può essere qualificato come prodotto ai sensi di tale Direttiva[17].
Questo determina però la necessità di una riqualificazione giuridica del concetto di "*produttore*", quando riferito a sistemi di IA.
Il concetto di "*produttore*" dovrà essere infatti tale da ricomprendere, al suo interno, non solo i produttori in senso stretto, ma anche sviluppatori, programmatori e fornitori di servizi di IA.

---

[15] Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL)), disponibile all'indirizzo: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_IT.html.
[16] Direttiva 85/374/CEE del Consiglio del 25 luglio 1985 relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati Membri in materia di responsabilità per danno da prodotti difettosi, disponibile all'indirizzo: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:31985L0374&from=EN.
[17] Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL)), punto 8.

In particolare, nel caso delle tecnologie basate sull'IA, sarà possibile individuare tanto un operatore di "*frontend*", quanto un operatore di "*backend*".
Mentre l'operatore di "*frontend"* dovrebbe essere definito "*come la persona fisica o giuridica che esercita un certo grado di controllo su un rischio connesso all'operatività e al funzionamento del sistema di IA e che beneficia del suo funzionamento*", l'operatore di "*backend"* coinciderebbe con "*la persona fisica o giuridica che, su base continuativa, definisce le caratteristiche della tecnologia, fornisce i dati e il servizio di supporto di* back-end *essenziale e pertanto esercita anche un elevato grado di controllo su un rischio connesso all'operatività e al funzionamento del sistema di IA*"[18].
La responsabilità viene dunque ricollegata al grado di controllo che ciascun operatore detiene sui rischi legati al sistema di IA.
In altre parole, il soggetto in grado di determinare, controllare, interferire le operazioni, e i rischi ad esse connesse, di un sistema di IA sarà considerato come responsabile per i danni che derivino dal sistema stesso.
A sua volta, la responsabilità sarà graduata in base al livello di diligenza che all'operatore si possa ragionevolmente richiedere sulla base di una serie di fattori, quali la natura del sistema di IA e l'ambito in cui lo stesso viene impiegato[19].
Ulteriori distinzioni, in materia di responsabilità, saranno da effettuarsi in riferimento al fatto che il sistema di IA di cui si tratta sia un sistema "ad alto rischio" o meno (*infra*, Capitolo 3).
La responsabilità derivante dai rischi intrinsechi alle tecnologie basate sull'IA risulta in questa fase di sviluppo maggiormente evidente, dal momento che l'operatore/produttore viene normalmente riguardato come il primario punto di contatto in riferimento ad un dato "prodotto-sistema di IA".
Tale responsabilità, però, come vedremo, incombe, in misura differente, su tutti i soggetti che entreranno a contatto con il sistema di IA, lungo l'intero arco del suo ciclo di vita, ivi compresi gli utilizzatori finali.
La necessità di stabilire i confini delle responsabilità di ciascun soggetto che partecipa, seppur in misura differente, al ciclo di vita di un sistema di IA, costituisce uno dei punti più dibattuti anche tra gli Stati membri.
Nel *Progress Report* sull'IA presentato a fine novembre 2021, la Presidenza slovena del Consiglio dell'Unione europea ha individuato tale aspetto come una delle principali questioni aperte, in virtù del fatto che "*i sistemi di IA sono sviluppati e distribuiti attraverso complesse catene di valore, dove i confini tra i diversi attori non sono sempre chiaramente delineati"* e, di conseguenza, nelle future discussioni legislative attorno

[18] *Ibidem*, punto 12.
[19] *Ibidem*, punto 18.

alla proposta legislativa, "*può essere rilevante rivalutare l'assegnazione di responsabilità e di ruoli, al fine di riflettere meglio la realtà della progettazione di un sistema di IA, metterlo sul mercato o farlo funzionare*"[20].

Un modello alternativo, elaborato dalla dottrina, di regolamentazione della responsabilità del produttore prevede invece di assegnare ad un'agenzia indipendente il compito di certificare i sistemi di IA in base al relativo grado di sicurezza.

L'agenzia avrebbe, di conseguenza, anche il potere di vietare prodotti ritenuti rischiosi o non sicuri in modo tale da creare un sistema di limitata responsabilità penale per i produttori dei sistemi certificati ed un sistema di responsabilità civile per coloro che commercializzano sistemi non soggetti a certificazione[21].

3. *La fase di diffusione*

La delicatezza di questa seconda fase risiede nel fatto che essa segna un passaggio decisivo tra chi ha progettato il sistema di IA e chi andrà ad utilizzarlo.

Gli attori coinvolti in questo passaggio di immissione nel mercato hanno dunque un duplice ruolo di valutazione/controllo nei confronti della fase a monte di sviluppo e di comunicazione rispetto alla fase a valle di utilizzo.

Il principio che quindi ispira maggiormente questa seconda fase è quello della trasparenza. Una completezza informativa fornita a monte dal produttore consentirà infatti non solo di valutare in modo più efficiente la struttura e le caratteristiche tecniche del prodotto da immettere sul mercato, ma anche di aumentare la fiducia dell'utilizzatore finale nei confronti di un sistema di IA facilmente conoscibile in tutti i suoi elementi.

In via generale, la regolazione dell'immissione di prodotti-sistemi di IA nel mercato interno dell'UE, dovrà tenere conto del quadro normativo di riferimento attualmente in vigore, e rappresentato dal Nuovo Quadro Legislativo per la Commercializzazione dei Prodotti[22].

---

[20] *Artificial Intelligence Act Progress Report*, paragrafo 26, disponibile all'indirizzo https://www.consilium.europa.eu/en/meetings/tte/2021/12/03/.

[21] M. U. SCHERER, *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies and Strategies*, Harvard Journal of Law and Technology, Volume 29, Number 2 Spring 2016, pag.393.

[22] Tale "Nuovo Quadro Legislativo" comprende: Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC and Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011.

In riferimento più specificatamente all'IA, le discussioni a livello europeo sono incentrate sulla necessità di introdurre una procedura volta ad istituire non solo un sistema di certificazione standardizzata, ma anche un sistema di controllo dei rischi.
La standardizzazione dovrà basarsi su criteri armonizzati che consentano di effettuare le necessarie verifiche in modo efficiente, ma entro tempi brevi.
Tali standard dovranno essere tali da garantire, da un lato, la certezza giuridica per gli sviluppatori e, dall'altro, un grado di flessibilità tale da adeguarsi alla rapida evoluzione della tecnologia di IA. Questo, secondo quanto previsto dalla Commissione Europea, assicurerà un approccio *fast-track* efficace anche per nuovi sistemi di IA immessi nel mercato per la prima volta.
In riferimento invece alle misure di gestione di controllo del rischio, il soggetto più idoneo a stabilirle sembra essere in definitiva lo stesso sviluppatore, essendo l'unico soggetto della catena in grado di prevedere (seppur entro certi limiti) le modalità in cui il sistema di IA si comporterà lungo l'intero arco del suo ciclo vitale.
In caso di applicazioni che continuino ad apprendere anche successivamente alla conclusione della fase di sviluppo, sarà necessario stabilire un sistema di controllo *ex post* all'immissione nel mercato stessa.
In molti casi, inoltre, dovrà prevedersi un sistema di controllo *real time*, alla luce della sensibilità degli ambiti in cui molti sistemi di IA vengono oggi impiegati (si pensi ai servizi di *e-health*, solo per citare un esempio), che richiedono un intervento immediato in caso di anomalie nel funzionamento del sistema stesso.
In tali casi si richiede dunque non solo un controllo nel momento della diffusione, ma una vera e propria "supervisione umana" lungo tutto l'arco del loro utilizzo.
Un tema ancora oggetto di dibattito riguarda l'individuazione del soggetto cui affidare tale controllo.
Anche qui, una distinzione verrà probabilmente operata sulla base del livello di rischio del sistema di IA, prevedendo verosimilmente un *self-assessment* effettuabile direttamente dallo sviluppatore per i sistemi di IA non ad alto rischio, e una procedura affidata ad un'autorità regolamentare (nazionale o europea) nel caso di sistemi di IA ad alto rischio.
Un tema che si pone in questa fase riguarda anche la questione della reciprocità con i mercati non UE. Il quadro normativo europeo si applicherà infatti a qualsiasi prodotto immesso nel mercato europeo, indipendentemente dal fatto che la società che lo ha sviluppato sia stabilita nell'UE o meno.

4. *La fase di utilizzo delle tecnologie e dei loro componenti*

Come anticipato nel trattare le prime due fasi di un sistema di IA, anche in riferimento alla terza fase di utilizzo possono individuarsi responsabilità in capo agli utenti finali, che richiedono dunque uno specifico intervento regolamentare.
Se è vero che non è possibile anticipare tutti gli usi che si possono fare di un sistema di IA, è altrettanto vero che il controllo sull'utilizzo che si fa dei sistemi di IA è, inevitabilmente, in parte affidato anche all'utilizzatore stesso.
In considerazione, infatti, della natura dei sistemi di IA e della loro potenziale capacità di sfuggire al controllo umano, è necessario che anche l'utente finale sia sottoposto ad una serie di obblighi regolamentari che disciplinino la fase di utilizzo.
Anche in questa sede assume dunque rilevanza il concetto di trasparenza già individuato in riferimento alla fase di diffusione.
Solamente se un alto livello di trasparenza è stato assicurato dallo sviluppatore, l'utilizzatore potrà essere in grado di comprendere, anche grazie al ruolo di intermediazione svolto dai soggetti cui è demandata la gestione della fase di diffusione, il sistema che sta utilizzando per poterlo controllare.
A tal proposito gli utilizzatori dovranno utilizzare i sistemi di IA conformemente alle informazioni fornite dagli sviluppatori dei sistemi stessi.
Allo stesso modo, essendo in grado di valutare il funzionamento normale del sistema di IA, sarà anche loro cura monitorare il sistema e segnalare la presenza di eventuali anomalie.
Ancora una volta, dunque, come già nel caso dello sviluppatore, la responsabilità viene ricondotta al grado di controllo che il soggetto è in grado di esercitare sul sistema di IA.
In conclusione, si può affermare che la diversità dei sistemi di IA e il diverso grado di rischi ad essi associati rende molto più complessa la regolazione dell'IA *tout court*.
Ciò sembra rendere necessario un approccio regolatorio *step-by-step* che disciplini le specificità, e le novità, che caratterizzano ogni singola fase, pur tenendo sempre presente l'inevitabile interconnessione tra le varie fasi in cui un sistema di IA si esplica e tra i vari soggetti che partecipano al suo ciclo di vita.