Anitec-Assinform

Position Paper

Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale e modifica alcuni atti legislativi dell'Unione

a cura del Tavolo di lavoro Intelligenza Artificiale – Gruppo di lavoro Cloud & New Technologies di Anitec-Assinform

Gennaio 2022

ANITEC-ASSINFORM
Associazione Italiana per l'Information and Communication Technology

Sede e uffici di Milano:
Via San Maurilio 21, 20123 Milano

Uffici di Roma:
Via Barberini 11 00187 Roma

segreteria@anitec-assinform.it www.anitec-assinform.it Aderisce a CONFINDUSTRIA CONFINDUSTRIA DIGITALE

Anitec-Assinform

Sommario

PREMESSA

Anitec-Assinform valuta positivamente l'adozione di una proposta di regolamento europeo sull'Intelligenza artificiale che sia *human-centered* e *trustworthy,* con l'obiettivo di assicurare la massima fiducia dei consumatori verso gli impieghi di questa tecnologia. Parimenti, si ritiene fondamentale che qualsivoglia intervento di regolazione dell'IA garantisca certezza giuridica, non ostacoli l'innovazione e non comporti oneri regolatori eccessivi per PMI e Start-up, specialmente in mancanza di standard condivisi o *best pra*ctices di riferimento. Alla regolazione dell'IA dovrebbe poi accompagnarsi, da un lato, un robusto investimento parallelo sulle infrastrutture abilitanti dello sviluppo di IA come *data spaces* e *high performance computers*, dall'altro un piano di formazione altrettanto solido per avere più competenze utili nel mondo del lavoro e maggiore *digital literacy* nei cittadini.

EXECUTIVE SUMMARY

- Anitec-Assinform valuta positivamente l'adozione di una proposta di regolamento europeo sull'Intelligenza artificiale, purché si garantisca un quadro regolatorio di supporto e stimolo all'innovazione, soprattutto nell'ottica di non gravare PMI e Start-up di eccessivi oneri e costi per la sua attuazione.

- Alla regolazione dell'IA dovrebbero affiancarsi:

    - investimenti su infrastrutture abilitanti dello sviluppo di IA (es. *data spaces* e *high performance computing*);

    - piano di formazione solido per avere competenze utili nel mondo del lavoro e maggiore *digital literacy* nei cittadini.

- È fondamentale che il Regolamento sia in armonia con la legislazione rilevante a livello europeo. Ad esempio, le disposizioni riguardanti il trattamento dei dati devono concordare con quanto previsto dal GDPR.

- Condividiamo la scelta della Commissione di regolare in modo stringente l'utilizzo dell'identificazione biometrica remota. In linea generale, apprezziamo che siano vietate alcune pratiche di IBR rischiose per la protezione dei diritti fondamentali e non la tecnologia in sé (sistemi di IBR possono essere sviluppati come IA ad alto rischio). Il testo necessita di maggiori chiarimenti in riferimento alle pratiche vietate (art. 5).

- Apprezziamo l'approccio della "regolazione basata sul rischio", ma riteniamo che sia fondamentale prendere in considerazione, nel definire i livelli di rischio, non solo l'effettivo danno potenziale associato ai sistemi di IA, ma anche la probabilità che un evento avverso accada nonché i benefici che il sistema di IA potrebbe apportare alla società (es. impatto positivo dell'IA su ambiente e sostenibilità).

- La definizione di "sistema di intelligenza artificiale" di cui all'articolo 3 risulta essere eccessivamente ampia, con l'effetto di rendere incerto il perimetro attuativo del regolamento per le imprese.

- Per garantire la massima certezza del diritto, le materie di cui all'art 5 (pratiche di Intelligenza Artificiale vietate) richiedono una maggiore specificazione.

- È importante che i requisiti richiesti ai sistemi di intelligenza artificiale (ad alto rischio) siano realistici. Riteniamo eccessivi gli standard richiesti dagli articoli 10 (dati e governace dei dati) e 14 (supervisione umana).

- L'allocazione delle responsabilità nei confronti dei sistemi di IA tra fornitori e utenti risulta essere troppo sbilanciata verso i primi (art. 16 e art. 28). Molto spesso – si pensi agli *smart objec*t – il sistema continua a raccogliere dati e ad adattare il proprio comportamento senza essere sotto il controllo del fornitore che l'ha prodotto. Un discorso analogo può essere fatto per i cd. strumenti "*off-the-shelf*". Proponiamo di prevedere degli strumenti contrattuali che possano definire caso per caso e a priori il riparto degli obblighi tra produttori, utenti e altre parti terze. Lo stesso discorso vale anche per gli obblighi di "post-market monitoring" di cui all'articolo 61.

- I costi per la messa in atto di un *Quality Management System* (QMS) in regola con i requisiti imposti dall'art. 17 sono eccessivi e rischiano di fare uscire dal mercato molte Start-up e PMI. Sempre per quanto riguarda i costi di compliance per PMI e Start-up, riteniamo che anche la procedura per ottenere la certificazione CE per i sistemi di IA (ad alto rischio) sia eccessivamente complessa e costosa (art. 43, valutazione della conformità).

- Giudichiamo positivamente la previsione di misure ad hoc per "fornitori di piccole dimensioni" come l'accesso facilitato a spazi di sperimentazione normativa (sandbox ex. Art. 53). In generale, preme sottolineare come sia necessario un investimento in infrastrutture parallelo alla regolazione e in grado di valorizzare le realtà più piccole che sono molto diffuse nell'ecosistema di questa tecnologia.

- La condivisione di dataset e codici sorgente è una materia estremamente delicata. L'articolo 64 prevede che le autorità di vigilanza del mercato possano accedere a queste risorse. Riteniamo che una simile pratica debba essere considerata solo come *extrema ratio* dopo aver utilizzato altri metodi di auditing meno invasivi.

1. TITOLO I – DISPOSIZIONI GENERALI

1.1.1 Articolo 3 – Definizioni

Contenuto dell'articolo: *l'art. 3 riporta le definizioni che si applicano ai fini del Regolamento. In particolare, quella di sistema di IA è la seguente: "un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono. In tutto l'articolo riporta 44 definizioni, tra le altre anche quelle di "produttore", "produttore di piccole dimensioni"; "utente".*

L'articolo 3 della Proposta di Regolamento propone – tra le altre – una definizione di "sistema di Intelligenza Artificiale". Siamo consapevoli della difficoltà in cui si incorre nel definire questa tecnologia, in quanto si rischia di allontanarsi delle caratteristiche tecnologiche vere e proprie per spostarsi su campi più astratti. Da questo punto di vista, apprezziamo lo sforzo della Commissione di dare una definizione di sistema di IA incentrata su elementi concreti come gli algoritmi utilizzati per svilupparla. Ciò nondimeno, riscontriamo come alcune delle tecniche cui si fa riferimento nell'Allegato I della Proposta siano proprie di *software* che spesso non vengono definiti come IA, ad esempio il punto c) "approcci statistici, stima bayesiana, metodi di ricerca e ottimizzazione". Di conseguenza, la definizione proposta presenta un rischio di incertezza giuridica a carico dei fornitori che potrebbero non essere consci di sviluppare *software* che potrebbero essere considerati come IA. Inoltre, riscontriamo che l'espressione "obiettivi definiti dall'uomo" potrebbe rivelarsi inadeguata in quanto sistemi di IA simbiotici arriverebbero a definire i loro *input* e obiettivi a seguito di una collaborazione uomo-macchina.

In generale, riteniamo che sarebbe opportuno valutare l'adozione di una definizione diversa[1] e possibilmente riconsiderare il rapporto costi/benefici riequilibrando l'impegno a introdurre nuove forme di tutela e l'esigenza di limitare le categorie di operatori su cui graverebbero i costi di *compliance*.

[1] Definizioni globalmente accettate, e che sono già utilizzate dall'industria, potrebbero essere più appropriate: un esempio è la definizione offerta dall'Expert Group sull'intelligenza artificiale dell'OECD, che cattura la distinzione tra sistempi complessi di IA e logid-based algorithms: "An AI system is a machine-based system that is capable of influencing the Environment by making recommendations, predictions or decisions for a given set of objectives. It does so by utilising machine and/or human-based inputs/data to: i) perceive real and/or virtual environments; ii) abstract such perceptions into models manually or automatically; and iii) use model interpretations to formulate options for outcomes."

https://oecd.ai/en/ai-principles

1.1.2 Articolo 4 – Modifiche all'allegato I

Contenuto dell'articolo: *l'articolo stabilisce che la Commissione ha il potere di adottare atti delegati (secondo una procedura prevista all'art. 73 del presente Regolamento al fine di modificare l'elenco delle tecniche e approcci di cui all'allegato I*.

Condividiamo l'accento posto dalla Commissione Europea sulla necessità di dare una definizione di sistema di IA "a prova di futuro". L'articolo 4 affida alla Commissione Europea il potere di modificare l'allegato I, nel quale sono riportati gli algoritmi che connoterebbero lo sviluppo di un sistema di IA. Riteniamo sia dubbio che – per quanto immediato possa essere l'intervento del regolatore – si riesca ad aggiornare l'Allegato I parallelamente all'avanzare della tecnologia, sia perché spesso impatti, caratteristiche ed eventuali rischi si avvertono e si comprendono anche molto tempo dopo l'utilizzo di una tecnologia, sia perché il tempo della regolazione è necessariamente più lento e, per questo, eventuali soluzioni a problemi emersi potrebbero essere inadeguate rischiando, in questo modo, di alimentare disaffezioni e sfiducia (o contenziosi) verso l'IA da parte dei cittadini. Si ritiene pertanto necessario modificare la definizione di sistema di IA eliminando i richiami puntuali agli algoritmi o, in alternativa, adottare un sistema solido di monitoraggio del progresso tecnologico che consente di aggiornare il testo dell'allegato.

2. TITOLO II – PRATICHE DI INTELLIGENZA ARTIFICIALE VIETATE

2.1.1 Articolo 5 – Pratiche di intelligenza artificiale vietate

Contenuto dell'articolo: *sono vietate:*

- *l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA che utilizzano tecniche subliminali al fine di distorcere il comportamento di una persona inconsapevole in un modo che possa provocare all'utilizzatore o a un'altra persona un danno fisico o psicologico.*

- *L'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA che sfruttano le vulnerabilità di un gruppo di persone (es. età, disabilità etc..) al fine di distorcere il comportamento e in un modo tale da provocare danni fisici o psicologici all'utilizzatore o a terzi.*

- *L'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA finalizzati a pratiche di "social scoring" da parte di autorità pubbliche.*

- *L'uso di sistemi di identificazione biometrica remota per attività di contrasto (law enforcement) "In tempo reale" in spazi accessibili al pubblico (con alcune eccezioni).*

Riteniamo che sia positivo che il regolatore vieti taluni utilizzi dell'Intelligenza Artificiale piuttosto che i sistemi di IA veri e propri. Questo permette, almeno in parte, di continuare a fare ricerca e sviluppare applicazioni nonostante alcune tecnologie siano impiegate in pratiche che verrebbero vietate. A nostro avviso, sono comunque necessari interventi volti a definire più accuratamente le pratiche che andrebbero proibite. Sempre nell'ottica di garantire la massima certezza del diritto, la Commissione dovrebbe fornire maggiori dettagli su espressioni come "danno psicologico" e "tecniche subliminali".

Il tema dell'identificazione biometrica remota (IBR) merita un approfondimento. Per costruire un ecosistema europeo dell'IA *human-centric* e *trustworthy*, una pratica come l'IBR, problematica dal punto di vista della privacy e della protezione dei diritti fondamentali dei cittadini, va trattata dal regolatore con un'attenzione speciale al fine di prevenirne l'abuso ma continuandone a garantire i benefici per l'intera società, come ad esempio l'efficientamento dell'assistenza sanitaria, o il supporto alle persone con disabilità. Nel testo l'utilizzo dell'IBR è vietato solo se "in tempo reale", in spazi pubblici e per attività di contrasto (law enforcement). Non vengono trattati gli utilizzi dell'identificazione biometrica remota in tempo reale e da parte di autorità pubbliche al di fuori delle forze dell'ordine, il che costituisce un potenziale rischio per il rispetto dei diritti fondamentali dei cittadini. Per migliorare la chiarezza giuridica del testo e assicurare una migliore

protezione dei diritti fondamentali raccomandiamo di riformulare il testo con disposizioni più precise.

.

3. TITOLO III – SISTEMI DI IA AD ALTO RISCHIO

3.1 Capo 1 – Classificazione dei sistemi di IA come "ad alto rischio"

3.1.1 Articolo 6 – Regole di classificazione per i sistemi di IA ad alto rischio

Contenuto dell'articolo: *un sistema di IA è considerato "ad alto rischio" se sono soddisfatte due condizioni:*

- *è destinato a essere utilizzato in un prodotto o è esso stesso un prodotto disciplinato dalla normativa di armonizzazione di cui all'allegato II;*
- *il prodotto di cui il componente di sicurezza è il sistema di IA, o il sistema di IA stesso in quanto prodotto, è soggetto a valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato e ai sensi della normativa di cui all'allegato II.*

Oppure se:

2. *appartiene ai sistemi di IA di cui all'allegato III*[2] *(cd stand-alone high risk ai systems).*

In linea generale, apprezziamo l'approccio della "regolazione basata sul rischio" che l'AI ACT peraltro condivide anche con altra legislazione europea (es. GDPR). Riteniamo che sia fondamentale prendere in considerazione, nel definire i livelli di rischio, non solo l'effettivo danno potenziale associato ai sistemi di IA, ma anche la probabilità che un evento avverso accada nonché i benefici che il sistema di IA potrebbe apportare alla società (es. impatto positivo dell'IA su ambiente e sostenibilità).

[2] Di seguito i settori nei quali operano i sistemi ad alto rischio "*stand alone*":

- Identificazione e categorizzazione biometrica delle persone fisiche.
- Gestione e funzionamento delle infrastrutture critiche.
- Istruzione e formazione professionale.
- Occupazione, gestione dei lavori e accesso al lavoro autonomo.
- Accesso a prestazioni e servizi pubblici e a servizi privati essenziali e fruizione degli stessi.
- Attività di contrasto (*law enforcement*).
- Gestione della migrazione, dell'asilo e del controllo delle frontiere.
- Amministrazione della giustizia e processi democratici.

Per quanto riguarda i sistemi di IA ad alto rischio che rientrano nella categoria dei componenti di sicurezza dei prodotti o sono essi stessi prodotti soggetti alla normativa Europea sulla sicurezza dei prodotti, è fondamentale che si evitino sovrapposizioni con la normativa già esistente.

È anzi condivisibile un approccio in cui sono interessate dal Regolamento solamente le applicazioni di IA ad alto rischio "*stand alone*", ossia quelle utilizzate nei campi applicativi indicati nell'allegato III alla proposta di Regolamento. Tuttavia, l'ecosistema è incredibilmente variegato e i sistemi di IA possono essere sviluppati in molti modi e secondo processi molto diversi tra loro. Riteniamo che nella versione corrente l'elenco sia eccessivamente generico: è vero che le aree indicate necessitano di tutele speciali dal punto di vista del diritto ma, all'interno di esse, andrebbero raffinate ancora meglio le applicazioni di IA intese come ad alto rischio.

3.1.2 Articolo 7 – Modifiche dell'allegato III

Contenuto dell'articolo: *la Commissione ha il potere di adottare atti delegati (secondo una procedura prevista all'art. 73 del presente Regolamento al fine di modificare l'allegato III.*

Analogamente a quanto affermato per l'art. 4, è necessario che la Commissione modifichi con cautela l'allegato III. Da un lato, esiste il rischio che il regolatore inserisca nell'elenco nuove aree inibendo il livello di ricerca e sviluppo di soluzioni di IA nei settori in questione; dall'altro, si rileva il rischio che non vengano riconosciuti miglioramenti della maturità tecnologica in certe aree che giustificherebbero una diminuzione del livello di rischio da "alto" a "limitato":

3.2 Capo 2 – Requisiti per i sistemi di IA ad alto rischio

3.2.1 Articolo 9 – Sistema di gestione dei rischi (Risk management system)

Contenuto dell'articolo: *i sistemi di IA ad alto rischio devono essere dotati di un sistema di gestione dei rischi; si tratta di un processo eseguito nel corso di tutto il ciclo di vita del sistema di IA che comprende le seguenti fasi: identificazione e analisi dei rischi noti e prevedibili, valutazione dei rischi che possono emergere quando il sistema è usato conformemente alle sue finalità e in condizioni di uso improprio ragionevolmente prevedibile, valutazione di altri rischi derivanti dall'analisi dei dati raccolti nel monitoraggio successivo all'immissione sul mercato e adozione di misure di gestione dei rischi adeguate.*

I sistemi di IA ad alto rischio sono sottoposti a prova per individuare le misure di gestione dei rischi più appropriate.

L'articolo 9 necessita di maggiori specificazioni. In primo luogo, manca una definizione di "rischio". In secondo luogo, l'articolo non esplicita quali siano rischi a cui si fa riferimento (per quanto i considerando 1, 13, 27 e 43 affermino che lo scopo del Regolamento è quello di mitigare i rischi per i diritti fondamentali, la salute, e la sicurezza dei cittadini).

3.2.2 Articolo 10 – Dati e governance dei dati

Contenuto dell'articolo: *l'art. 10 indica i criteri di qualità per i dataset di addestramento, convalida e prova utilizzati dai sistemi di IA ad alto rischio.*

È giusto richiedere per i sistemi "ad alto rischio" un certo standard di qualità dei dati utilizzati nel *training* delle IA, ma è necessario che tali requisiti siano realistici. I fornitori di sistemi di intelligenza artificiale lavorano spesso con quantità di dati elevatissime che possono provenire da fonti diverse. Riteniamo che il requisito di *dataset* "rappresentativi, esenti da errori e completi" sia irrealistico da soddisfare,

Più nel dettaglio, si può affermare che i requisiti presentati dal Regolamento causano tre ordini di problemi:

a. I bias non sono conseguenza esclusiva dei data set, ma devono essere considerati durante l'intero ciclo di vita del prodotto.

b. Standard quali "completezza" e "esenzione da errori" non sono tecnicamente raggiungibili, per una moltitudine di motivi. Ad esempio, la completezza confligge con la necessità di compiere delle scelte nella creazione di data sets che riflettono un certo timeframe, geografie, dimensione di un certo campione. Spesso, la completezza di un data set mina l'equità dei risultati se il data set riflette bias sociali o strutturali. Infine, la completezza del data sets può frustrare principi fondamentali di protezione dei dati, come quello di minimizzazione.

c. I requisiti rendono più difficile il rispetto della privacy e l'applicazione di *fairness-enhancing technologies*: gli standard possono limitare l'utilizzo di tecnologie privacy come i cosiddetti "synthetic data", creati artificialmente per educare modelli di IA.

È preferibile la formula utilizzata nel considerando n. 44: "I set di dati di addestramento, convalida e prova dovrebbero essere **sufficientemente** pertinenti, rappresentativi e privi di errori, nonché completi alla luce della finalità prevista del sistema".

3.2.3 Articolo 14 – Sorveglianza umana (Human oversight)

Contenuto dell'articolo: *i sistemi di IA ad alto rischio devono prevedere strumenti di interfaccia uomo-macchina adeguati in modo da esser efficacemente supervisionati da persone fisiche. La sorveglianza umana è garantita da:*

a. *misure individuate e integrate nel sistema dal fornitore;*

b. *misure individuate dal fornitore adatte a essere attuate dall'utente.*

Il comma 4 dell'articolo tratta nel dettaglio le azioni consentite a chi svolge la supervisione.

Un discorso analogo a quello fatto per l'art. 10 vale anche per l'art. 14. In linea generale, riteniamo che il requisito della sorveglianza umana sia condivisibile per i sistemi "ad alto rischio", tuttavia è opportuno sottolineare che il requisito secondo cui il personale atto alla sorveglianza del sistema di IA debba "comprendere appieno le capacità e i limiti del sistema di IA" sia irrealistico, in quanto è molto complesso avere una comprensione completa della capacità e dei limiti dei sistemi. Per questo, suggeriamo di utilizzare l'espressione: "comprendere sufficientemente le capacità e i limiti del sistema di IA".

3.3 Capo 3 – Obblighi dei fornitori e degli utenti dei sistemi di IA ad alto rischio e di altre parti

3.3.1 Articolo 16 – Obblighi dei fornitori dei sistemi di IA ad alto rischio

Contenuto dell'articolo: *l'articolo elenca gli obblighi dei fornitori di sistemi di IA ad alto rischio*[3]

- garantire la conformità ai requisiti al capo 2, titolo III del Regolamento,
- disporre di un sistema di gestione della qualità ex. Art. 17 del Regolamento;
- redigere la documentazione tecnica del sistema di IA ad alto rischio;
- quando sono sotto il loro controllo, conservano i log dei sistemi di IA ad alto rischio
- garantiscono che il sistema di IA sia sottoposto alla procedura di valutazione della conformità prima dell'immissione sul mercato;
- rispettano gli obblighi di registrazione;
- adottano le misure correttive necessarie se il sistema non è conforme ai requisiti del capo 2 titolo III e informano le autorità competenti sulla non conformità e sulle misure correttive adottate;

Riteniamo che una delle criticità principali della proposta di Regolamento riguardi l'allocazione delle responsabilità tra fornitori e utenti dei sistemi di IA. L'articolo 16, alla lettera (a)[4], indica tra gli obblighi dei produttori attività di controllo sui sistemi di IA quali la gestione dei dati (data governance – art. 10) e la supervisione umana (art.14).

Per quanto riguarda il primo punto, evidenziamo che lo sviluppo di sistemi di Intelligenza Artificiale avviene spesso in *value chain* complesse nelle quali i fornitori non hanno sempre il controllo totale delle evoluzioni che possono interessare l'IA da loro "prodotta". Ad esempio, non è raro che - una volta immesso sul mercato – un sistema di IA continui a raccogliere dati per migliorare le proprie prestazioni sebbene di fatto non sia più sotto il controllo dei fornitori. Questo può essere il caso di campi di applicazione emergenti come quello degli *smart objects*.

In merito invece alla supervisione umana sui sistemi di IA ad alto rischio, consideriamo inadeguato che la proposta di Regolamento la ponga in capo ai fornitori piuttosto che agli utenti business. Nella proposta di regolamento, infatti, questi ultimi, infatti, sono responsabili esclusivamente di seguire le istruzioni tecniche fornite dai produttori[5].

3.3.2 Articolo 17 – Sistema di gestione della qualità (Quality Management System)

Contenuto dell'articolo: *i fornitori di sistemi di IA ad alto rischio devono istituire un sistema di gestione della qualità. Il sistema deve essere documentato in modo sistematico e ordinato sotto forma di politiche procedure e istruzioni scritte[6].*

Nell'analisi d'impatto sulla proposta di Regolamento condotta dal CEPS[7] viene stimato un costo compreso tra 190.000 e 330.000 euro per la creazione *ex-novo* di un *Quality Management System* a cui si andrebbero ad aggiungere oltre 70.000 euro di costi manutenzione annuale. Reputiamo i requisiti richiesti per il

- appongono la marcatura CE per indicare la conformità al regolamento;
- su richiesta di un'autorità nazionale competente, dimostrano la conformità del sistema di IA ai requisiti di cui al capo 2 titolo III del Regolamento.

[4] "I fornitori dei sistemi di IA ad alto rischio garantiscono che i loro sistemi di IA ad alto rischio siano conformi ai requisiti di cui al capo 2 del presente titolo".

[5] Michael Veale and Frederik Zuiderveen Borgesius, Demystifying the Draft EU Artificial Intelligence Act

QMS eccessivi: i costi previsti sarebbero infatti tali da escludere dal mercato un grande numero di piccoli sviluppatori.

3.3.3 Articolo 28 – Obblighi di distributori, importatori, utenti e altri terzi (tema della distribuzione di obblighi tra provider e user)

Contenuto dell'articolo: *l'articolo 28 stabilisce che qualsiasi distributore, importatore, utente o terzo è considerato un fornitore se:*

a. *immette sul mercato o mette in servizio un sistema di IA ad alto rischio con il proprio nome o marchio;*
b. *modifica la finalità prevista di un sistema di IA ad alto rischio già immesso sul mercato;*
c. *apporta una modifica sostanziale al sistema di IA ad alto rischio.*

Se si verificano le circostanze dei punti b o c il fornitore che ha messo inizialmente sul mercato il sistema non è più considerato tale ai fini del Regolamento.

L'articolo 28 fa riferimento ai casi in cui utenti, distributori, importatori o qualsiasi altra parte terza modifichino i sistemi di IA ad alto rischio. Riteniamo che sia apprezzabile che la Commissione Europea sia cosciente di questa possibilità (vedi Par. 3.3.1. del presente position paper), tuttavia – visto l'elevato livello di complessità delle interazioni tra i molti attori dell'ecosistema dell'IA[8] – riteniamo che una misura "rigida" di spostamento della responsabilità da fornitori alle terze parti possa non essere efficiente. Proponiamo di prevedere invece degli strumenti contrattuali che possano definire caso per caso e a priori il riparto degli obblighi tra produttori, utenti e altre parti terze, e in generale la riorganizzazione dei soggetti dell'ecosistema secondo una tassonomia più sfumata, che identifichi la rilevanza dei partecipanti nei sistemi di IA e allochi appropriate responsabilità ed obblighi a ciascuno.

3.4 Capo 5 – Norme (*standards*), valutazione della conformità, certificati, registrazione

3.4.1 Articolo 43 – Valutazione della conformità

Contenuto dell'articolo: *prima di essere immessi sul mercato o messi in servizio, i sistemi di IA ad alto rischio devono superare una procedura di valutazione della conformità. Se il sistema di IA ad alto rischio è "stand-alone"*

[8] I sistemi di IA sono il risultato di un lavoro stratificato di una moltitudine di organizzazioni, e possono svilupparsi costruendo su librerie open-source, strumenti e framework creati da altrettanti partecipanti, che offrono parti di codice secondo diverse modalità. Questi possono, successivamente, essere combinati con ulteriori data set, costruiti sulla base di altre contribuzioni. In un ecosistema così complesso è difficile identificare chi ha effettivamente sviluppato il sistema di IA.

(esclusa l'identificazione biometrica) i fornitori utilizzano la procedura di controllo interno di cui all'allegato VI del regolamento.
Per i sistemi di identificazione remota la procedura cambia a seconda dell'esistenza di norme armonizzate ex. Art. 40 (o se non disponibili, almeno specifiche comuni ex. Art. 41), se le norme armonizzate esistono si possono scegliere sia la procedura di cui all'allegato VI che quella di cui all'allegato VII (certificazione esterna a opera di un organismo notificato). Se gli standard non esistono si deve utilizzare la procedura di cui all'allegato VII.
Per i sistemi di IA ad alto rischio di cui all'allegato II del Regolamento (quelli interessati dalla normativa di armonizzazione dell'UE) si deve applicare la procedura di conformità prevista dalla normativa già esistente nei vari settori di riferimento e, in aggiunta, i punti 4.3, 4.4 e 4.5 e il quinto paragrafo dell'allegato VII al Regolamento[9]*.*

La procedura prevista per la valutazione della conformità e apposizione della marcatura CE potrebbe rivelarsi molto complessa e gravosa in termini di costi regolatori per gli attori più piccoli dell'ecosistema dell'IA (start-up, PMI, laboratori, centri di ricerca ecc…), i quali potrebbero avere poche risorse organizzative per gestire la *compliance* a regole con cui hanno poca familiarità. A nostro avviso, esiste un rischio concreto che tali obblighi frenino rilevante all'innovazione.

Non va sottovalutato neanche il tema dell'accesso ai dataset da parte degli organismi notificati (art. 4.3 Allegato VII), in generale infatti garantire l'accesso di terzi ai dati potrebbe danneggiare la privacy (per esempio in casi in cui non verrebbero cancellati alcuni dati), oltre che avere implicazioni relative a temi di diritto d'autore (es. casi in cui la "non-violazione" dipende sull'uso esclusivamente temporaneo delle copie).

[9] Tali punti e il quinto paragrafo riguardano: esame da parte dell'organismo notificato della documentazione tecnica e accesso di quest'ultimo ai dataset, richiesta di elementi probatori supplementari, accesso al codice sorgente, notifica della decisione al fornitore, vigilanza del sistema di gestione della qualità approvato.

4. TITOLO IV – OBBLIGHI DI TRASPARENZA

4.1.1 Articolo 52 – Obblighi di trasparenza per determinati sistemi di IA

Contenuto dell'articolo: *I fornitori di sistemi di IA che interagiscono con persone devono essere progettarli e svilupparli in modo tale da informare chi li utilizza, del fatto che stanno interagendo con un sistema di IA.*
Gli utenti di sistemi emotion recognition o categorizzazione biometrica devono informare le persone fisiche che sono esposte all'applicazione del sistema (con le eccezioni di sistemi categorizzazione biometrica autorizzati dalla legge per accertare prevenire e indagare reati.).
Gli utenti di sistemi che manipolano audio e generano immagini (es. deep fake), devono rendere noto che i contenuti sono generati artificialmente.

Riteniamo che costruire un clima di fiducia tra produttori, utenti e utenti finali sia fondamentale per lo sviluppo e il successo dell'ecosistema dell'IA europeo. Per questo motivo, accogliamo con favore la proposta di obblighi di trasparenza per determinati sistemi di IA. Notificare la natura "artificiale" di sistemi che hanno il compito di interfacciarsi con il pubblico presenta, da un lato, bassi costi di attuazione e, dall'altro, un grande ritorno in termini di chiarezza e fiducia tra produttori e consumatori.

5. TITOLO V – MISURE A SUPPORTO DELL'INNOVAZIONE

5.1.1 Articolo 53 – Spazi di sperimentazione normativa per l'IA/Sandboxes regolatorie:

Contenuto dell'articolo: *l'articolo dispone che una o più autorità competenti degli Stati membri o il Garante europeo della protezione dei dati possono istituire sandboxes (spazi di sperimentazione normativa), vale a dire ambienti controllati che facilitano lo sviluppo, le prove e la convalida di sistemi di IA innovativi per un periodo di tempo limitato prima della loro immissione sul mercato o della loro messa in servizio conformemente a un piano specifico.*

Valutiamo positivamente la previsione di *Sandboxes* o spazi di sperimentazione normativa per lo sviluppo e la sperimentazione "in ambienti controllati" di sistemi di IA. Allo stesso tempo, bisogna constatare, in primo luogo, che l'istituzione di questi strumenti è lasciata alla volontarietà degli stati membri; per questo motivo, evidenziamo il rischio di un generico depotenziamento dell'iniziativa, nonché di frammentazione del mercato unico per quanto riguarda l'IA, sarebbe invece auspicabile prevedere l'obbligo di istituzione delle *sandbox* a livello dei singoli stati membri. In secondo luogo, le misure riguardanti le *sandbox* nel Regolamento non sembrano sufficientemente dettagliate: andrebbero indicati chiaramente i vantaggi di cui beneficiano le aziende partecipanti e offerti livelli di protezione in termini di responsabilità rispetto ai risultati della sperimentazione. Infine, sottolineiamo come sia prioritario affiancare agli spazi di sperimentazione normativa anche investimento in infrastrutture abilitanti per lo sviluppo di IA, prime fra tutte i *data space*.

5.1.2 Articolo 55 – Misure per fornitori di piccole dimensioni e utenti

Contenuto dell'articolo: *L'articolo dispone che gli Stati membri forniscono ai fornitori di piccoli dimensioni un accesso prioritario alle sandboxes per l'IA. Gli stati membri organizzano inoltre attività di sensibilizzazione sull'applicazione del presente regolamento adattate alle esigenze dei fornitori di piccole dimensioni e degli utenti e istituiscono, ove opportuno, un canale dedicato per la comunicazione con i fornitori di piccole dimensioni, gli utenti e altri innovatori, al fine di dare indicazioni e rispondere alle domande sull'attuazione del Regolamento.*

Riteniamo che sia positiva la previsione di misure mirate alla riduzione dei costi regolatori per i fornitori di piccole dimensioni e, in particolare, misure come l'accesso agevolato alle *sandboxes* e la riduzione delle tariffe per la valutazione della conformità a norma dell'art. 43 vanno nella direzione di controbilanciare gli elevati costi di conformità imposti nelle altre sezioni della proposta di Regolamento.

Allo stesso tempo, tuttavia, vale la pena rimarcare che le *sandboxes* sono istituite dagli Stati membri in via *volontaria*, per cui trarrebbero beneficio dall'accesso agevolato solo gli *small-scale providers* di certi Stati.

In generale, riteniamo che la regolazione dell'IA possa rappresentare un'opportunità anche per gli attori più piccoli dell'ecosistema solo se inserita in un disegno strategico più ampio che ricomprenda anche misure a favore dell'accesso ai dati per il *training* dei sistemi e investimenti in infrastrutture abilitanti. Ad esempio, prevedere spazi di dati in condivisione e con accesso agevolato per realtà di dimensioni più contenute, potrebbe valorizzare notevolmente gli ecosistemi IA del nostro paese e più in generale dell'UE.

6. TITOLO VIII – MONITORAGGIO SUCCESSIVO ALL'IMMISSIONE SUL MERCATO, CONDIVISIONE DELLE INFORMAZIONI, VIGILANZA DEL MERCATO

6.1.1 Articolo 61 – Monitoraggio successivo all'immissione sul mercato effettuato dai fornitori e piano di monitoraggio successivo all'immissione sul mercato per i sistemi di IA ad alto rischio

Contenuto dell'articolo: *I fornitori istituiscono e documentano un sistema di monitoraggio successivo all'immissione sul mercato proporzionato alla natura delle tecnologie di intelligenza artificiale e ai rischi del sistema di IA ad alto rischio. Il sistema di monitoraggio successivo all'immissione sul mercato raccoglie, documenta e analizza attivamente e sistematicamente i dati pertinenti forniti dagli utenti o raccolti tramite altre fonti sulle prestazioni dei sistemi di IA ad alto rischio per tutta la durata del loro ciclo di vita e consente al fornitore di valutare la conformità dei sistemi di IA ai requisiti di cui al titolo III, capo 2.*

Come rilevato anche per gli articoli 16 e 28, riteniamo gli obblighi di monitoraggio "post market" debbano essere ripartiti in modo più equo tra fornitori e utenti. Idealmente tali mansioni dovrebbero essere in capo all'entità (utente o fornitore) che è più vicina all'operato effettivo del sistema di IA (non necessariamente il fornitore). Riteniamo preferibile un approccio in cui l'attribuzione di obblighi di questo tipo è definita a priori e per via contrattuale tra fornitore e utente.

6.1.2 Articolo 64 – Accesso ai dati e documentazione

Contenuto dell'articolo: *Per quanto riguarda l'accesso ai dati e alla documentazione nell'ambito delle loro attività, alle autorità di vigilanza del mercato è concesso pieno accesso ai set di dati di addestramento, convalida e prova utilizzati dal fornitore, anche attraverso interfacce di programmazione delle applicazioni ("API") o altri mezzi tecnici e strumenti adeguati che consentano l'accesso remoto.*

L'accesso ai dataset e agli strumenti come i codici sorgente è una materia estremamente delicata (la conservazione dei dataset comporta, come notato per l'art. 43, il rispetto del diritto di autore e di privacy, mentre i codici sorgente possono essere protetti da segreto industriale), per questa ragione riteniamo che l'autorità di vigilanza debba agire con proporzionalità e considerare l'accesso a tali risorse come *extrema ratio* (idealmente anche prevedendo che sia necessaria una preventiva autorizzazione giudiziaria).