

L'intensità della regolazione dell'Intelligenza Artificiale*

di Federico Marini Balestra

Sommario: 1. Differenziazione della regolazione a seconda che l'applicazione di IA sia ad "alto rischio" o non ad "alto rischio" nell'esperienza europea e internazionale; 2 (segue) che il servizio digitale usi IA o meno; 3. (segue) che la piattaforma che usa IA sia un *gatekeeper* o no

1. Differenziazione della regolazione a seconda che l'applicazione di IA sia ad "alto rischio" o non ad "alto rischio" nell'esperienza europea e internazionale

Con la pubblicazione del Libro Bianco della Commissione Europea nel febbraio 2020, è andata via via configurandosi una vera e propria *summa divisio* nel dibattito sulla regolazione dell'IA nell'Unione Europea, vale a dire la distinzione tra sistemi di IA ad "alto rischio" e sistemi di IA "non ad alto rischio".

Dietro tale distinzione si cela una scelta di approccio regolamentare e legislativo dell'IA basato sul rischio.

Essa garantirebbe, infatti, secondo la Commissione europea, un equilibrio tra la necessità, da un lato, di aumentare la fiducia dei cittadini nei sistemi di IA, dietro assicurazione di contemperarne i rischi, e, dall'altro, l'esigenza di non creare un fardello regolamentare eccessivo per le imprese che sviluppano sistemi di IA, limitando l'applicazione di norme più stringenti unicamente ai sistemi considerati ad "alto rischio".

* 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

Con la presentazione della proposta di regolamento sull'Intelligenza Artificiale¹, tale approccio è stato ulteriormente declinato in un approccio basato sul rischio proporzionale.

Il nuovo dogma attorno al quale la Commissione europea ha plasmato il suo primo intervento legislativo in materia di IA può essere infatti riassunto tramite il seguente principio: *“più alto è il rischio, più stringenti saranno le norme”*².

La proposta di Regolamento ha infatti superato la dicotomia “alto/basso rischio”, introducendo una classificazione che si snoda intorno a quattro categorie di utilizzo dei sistemi di IA, identificate in base al livello di rischio che possono determinare:

- Pratiche di IA proibite;
- Alti rischi;
- Rischi limitati; e
- Rischi minimi.

Le pratiche rientranti nel primo gruppo sono vietate in quanto considerate *ex se* tali da determinare dei rischi inaccettabili, ad esempio, perché in violazione dei diritti fondamentali.

All'interno di questa prima categoria rientrano *“i sistemi di IA che utilizzano tecniche subliminali in grado di distorcere il comportamento dell'utente in modo tale da provocarne un danno fisico o psicologico”*³ o da sfruttarne le vulnerabilità, così come i sistemi di IA di *“social scoring”* utilizzati dalle autorità pubbliche⁴.

All'estremo opposto vi sono, invece, i sistemi di IA cui vengono ricollegati rischi minimi (che quindi non necessitano di un alcun tipo di intervento normativo) e sistemi di IA che potrebbero determinare rischi limitati, nei confronti dei quali l'unico obbligo previsto è quello di rispettare determinati *standard* di trasparenza, che consentano all'utente, quando interagisce con tali sistemi, di prendere consapevolezza del fatto che non vi sia una persona fisica dall'altro lato.

Il fulcro della proposta di Regolamento risiede dunque nei sistemi di IA “ad alto rischio”.

¹ *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*, COM/2021/206 final, disponibile all'indirizzo: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206&qid=1620039310151>.

² *Speech by Executive Vice-President Margrethe Vestager at the press conference on fostering a European approach to Artificial Intelligence*, Bruxelles, 21 aprile 2021, disponibile all'indirizzo: https://ec.europa.eu/commission/presscorner/detail/en/speech_21_1866.

³ Articolo 5, Proposta di Regolamento COM/2021/206 final (cfr nota 19).

⁴ Il testo di compromesso presentato dalla Presidenza slovena del Consiglio dell'Unione europea il 29 novembre 2021 ha esteso il divieto di utilizzo dei sistemi di IA con finalità di *social scoring* anche agli attori privati.

Quest'ultima categoria, nell'impostazione della Commissione, è da considerarsi come una lista aperta, che andrà di volta in volta aggiornata in base ai futuri sviluppi tecnologici e ai relativi nuovi sistemi di IA di cui si richiede l'immissione nel mercato interno.

Il criterio utilizzato per individuare i sistemi di IA assume come base di riferimento il settore in cui il sistema viene utilizzato.

Al momento, i sistemi di IA “ad alto rischio” fanno riferimento ai seguenti settori: infrastrutture critiche (si pensi alle auto senza conducente), componenti di sicurezza dei prodotti (ad esempio, nell'ambito dell'*e-health*), selezione professionale, formazione scolastica e professionale, amministrazione della giustizia e processi democratici, servizi pubblici e privati essenziali, gestione dell'immigrazione e controllo dei confini. Si tratta, cioè, di quei settori che, per loro natura, risultano maggiormente suscettibili di causare danni ai soggetti coinvolti.

Nel Testo di compromesso presentato dalla presidenza slovena del Consiglio dell'Unione europea il 29 novembre 2021, sono state aggiunte due ulteriori aree rilevanti ai fini della classificazione di un sistema di IA come sistema ad “alto rischio”: le infrastrutture digitali e la protezione dell'ambiente⁵.

L'utilizzo e la diffusione di tali sistemi saranno consentiti sul mercato interno solamente se rispettino determinati requisiti obbligatori e qualora abbiano “superato” una valutazione di conformità operata *ex ante*.

Per quanto attiene al primo profilo, i requisiti obbligatori discendono direttamente dai principi indicati nei documenti frutto dei lavori del Gruppo di esperti di Alto Livello sull'Intelligenza Artificiale e possono riassumersi nei seguenti principi: l'implementazione di un sistema di gestione del rischio; la *governance* effettiva dei dati; la conservazione della documentazione rilevante; la trasparenza tramite la predisposizione di informazioni per l'utente; la garanzia della sorveglianza umana sui sistemi che rientrano in questa categoria e il loro rispetto dei principi di robustezza, accuratezza e sicurezza.

L'operatività pratica di tali requisiti ha già suscitato ampi dibattiti tra gli Stati membri, i quali ne hanno criticato l'eccessiva vaghezza e rigidità e hanno, di conseguenza, invocato la necessità di fornire alcuni orientamenti pratici alle imprese per rendere loro meno oneroso il conformarsi ai nuovi standard, ad esempio per quanto riguarda la

⁵ In particolare, sono stati inseriti nell'Annex III, e dunque da classificare come sistemi “ad alto rischio”, i sistemi di IA destinati ad essere utilizzati per controllare le infrastrutture digitali (o come loro componenti di sicurezza) e i sistemi di IA destinati ad essere utilizzati per controllare le emissioni e l'inquinamento.

qualità e l'adeguatezza dei requisiti relativi ai dati, l'appropriatezza delle informazioni agli utenti⁶.

Il controllo di conformità è stato invece articolato sul modello già attualmente in vigore in riferimento al rilascio del marchio CE.

Il sistema proposto si baserà infatti su standard armonizzati e sul rilascio di certificati da parte degli organi incaricati di svolgere la valutazione di conformità. Il controllo esterno, da parte di autorità selezionate, è considerato necessario soprattutto in riferimento ai sistemi di IA che costituiscono componenti di sicurezza dei prodotti.

Al contrario, per i sistemi di IA che hanno “vita autonoma” (cd. *stand-alone*) un controllo interno, senza obbligo di notifica all'autorità competente, è, per la Commissione, ritenuto sufficiente.

All'interno della categoria dei sistemi di IA “ad alto rischio”, un discorso a parte va effettuato in riferimento ai sistemi di IA impiegati nell'identificazione biometrica. Per questi sistemi, infatti, è stato proposto un duplice controllo, sia di natura interna, sia di tipo esterno, coinvolgendo l'autorità preposta mediante notifica. Tale tecnologia viene infatti considerata particolarmente intrusiva e rischiosa ed anche il relativo utilizzo ne è stato quindi specificatamente limitato ai soli casi di applicazione della legge in cui risulta strettamente necessario (attacchi terroristici, rapimenti, ricerca di criminali)⁷, previa autorizzazione delle autorità giurisdizionali competenti e pur sempre nel rispetto di limiti spazio-temporali predefiniti.

La scelta di graduare la regolazione dei sistemi di IA sulla base dell'intensità del rischio che il loro utilizzo possa provocare riflette la volontà dell'esecutivo dell'UE di ancorare la regolamentazione delle nuove tecnologie, e del mondo digitale più in generale, ai valori fondamentali dell'Unione europea (come stabiliti dall'Articolo 2 TUE). Il rispetto del sostrato valoriale stabilito nei Trattati si pone infatti come *condicio sine qua non*, nell'impostazione della Commissione, per la creazione dell'ecosistema di fiducia che è alla base del quadro normativo europeo per l'IA.

Tale sostrato valoriale ha dettato dunque, in definitiva, la scelta del modello regolatorio prescelto in Europa, proporzionale all'impatto del rischio determinato dai sistemi di IA sul paradigma valoriale di riferimento. In altre parole, i valori fondamentali costituiscono una base talmente imprescindibile da qualificare come “rischio” tutto ciò che possa minacciarli.

⁶ *Artificial Intelligence Act Progress Report*, paragrafo 25, disponibile al seguente indirizzo: <https://www.consilium.europa.eu/en/meetings/tte/2021/12/03/>.

⁷ La proposta di compromesso della Presidenza slovena ha specificato che i sistemi di identificazione biometrica *real-time*, negli spazi accessibili al pubblico, possono essere utilizzati non solo dalle autorità di polizia, ma anche da altri soggetti di cui le forze dell'ordine si avvalgono. A tali ulteriori soggetti verrebbe dunque esteso il relativo processo di notifica/autorizzazione.

Ancorché maggiormente funzionale a promuovere i benefici dell'IA (v. § precedente), anche negli Stati Uniti è stata ipotizzata l'adozione di un approccio regolamentare, che tenesse conto del rischio.

Già nelle Linee Guida sulla Regolazione delle Applicazioni di IA del novembre 2020, la Casa Bianca stabiliva che “*gli approcci regolamentari e non regolamentari in riferimento all'IA dovessero basarsi sull'applicazione uniforme di valutazione e gestione del rischio*” da parte delle varie agenzie federali.

Anche secondo l'amministrazione statunitense, non risulta necessario regolare ogni rischio prospettabile, ma unicamente quei rischi che siano in grado di determinare un danno considerato inaccettabile o un danno che sia tale da superare i benefici prospettati. Ancor prima dell'adozione delle Linee Guida, nel 2019, sotto la previgente amministrativa USA, era stata avanzata una proposta di legge al Congresso per regolare gli algoritmi: *l'Algorithmic Accountability Act*.

Quest'ultima, poi non approvata, avrebbe attribuito alla *Federal Trade Commission* (“FTC”) il potere di richiedere alle entità che sviluppano, diffondono ed utilizzano sistemi di IA di condurre *impact assessment* per ogni sistema (sia esso nuovo o esistente) di decisione automatizzata ad alto rischio e per i sistemi di informazione “ad alto rischio”.

Ciò al fine, sempre in uno schema funzionale a promuovere i sistemi di IA, di valutare correttamente i benefici delle singole applicazioni e bilanciare così rischi/benefici nell'ottica di incentivare questi ultimi.

Come detto nel precedente capitolo, infatti, la principale differenza tra gli approcci europeo e statunitense consiste nel fatto che, da questa parte dell'Atlantico, l'obiettivo regolamentare è evitare che i rischi danneggino i valori umani condivisi, mentre dall'altra parte che i rischi non ostacolino il perseguimento dei benefici derivanti dall'uso di IA. In altri termini, la visione europea è più ideologica, mentre quella statunitense più utilitaristica.

Nella proposta americana, per “alto rischio” si intendeva un sistema in grado di determinare un rischio significativo per la *privacy* o la sicurezza delle informazioni personali dei consumatori e che potessero risultare in decisioni discriminatorie, ingiuste e inaccurate nei confronti degli utenti.

Oggetto della proposta legislativa erano quindi in questo caso soprattutto i sistemi che utilizzano informazioni personali dei consumatori o che fossero utilizzati per monitorare gli spazi pubblici, al fine di stabilire fino a che punto i sistemi in questione fossero in grado di proteggere la *privacy* e la sicurezza dei dati personali processati e conservati.

All’approccio basato sul rischio (*risk-based approach*), si contrappone un modello costruito intorno all’obiettivo che la regolamentazione si è prefissata (*goal-based approach*).

Questa seconda opzione regolamentare è stata presa in considerazione in Giappone.

Nell’interim report “*AI Governance in Japan ver. 1.0*”⁸, pubblicato il 15 Gennaio 2021, l’*Expert Group on Architecture for AI Principles to be Practiced* ha indicato l’approccio *goal-based* come l’approccio ideale per regolare l’IA in Giappone.

Questo modello si fonda sull’idea che a guidare la regolazione non debba essere il grado di rischio discendente da un determinato sistema di IA, ma quei principi di IA, che, tramite il quadro di *governance*, vengono resi “operativi”.

Per principi di IA si fa qui riferimento ai principi sui quali si sono concentrate i primi dibattiti intorno alla regolazione dell’IA, soprattutto nei *fora* sovranazionali⁹. Con specifico riferimento al Giappone, i “*Social Principles of Human-centric AI*” sono: 1. Centralità dell’individuo; 2. Educazione/Alfabetizzazione; 3. Protezione della *Privacy*; 4. Sicurezza; 5. Concorrenza leale; 6. Correttezza, Responsabilità e Trasparenza; e 7. Innovazione.

Secondo l’*Interim Report* nipponico, data la convergenza di tali principi individuati in sede nazionale con i principi di IA sui quali si è andato consolidandosi un consenso sovranazionale, si dovrebbe favorire una traduzione di tali principi in obiettivi sui quali fondare una *governance* “condivisa” dell’IA.

Oltre alla possibilità di estendersi al di là dei confini nazionali, tale approccio avrebbe una serie di vantaggi ulteriori.

Innanzitutto, considerata la rapidità di evoluzione che caratterizza l’IA, questo modello, meno prescrittivo, presenterebbe una maggiore duttilità rispetto alla *governance* tradizionale, che potrebbe rischiare di porre un freno all’innovazione. Ad essere attivamente coinvolti, infatti, nel *goal-based approach*, sono proprio le imprese, chiamate a disegnare e sviluppare i sistemi di IA sulla base degli specifici obiettivi individuati.

La partecipazione attiva delle imprese consentirebbe anche di risolvere la questione dell’asimmetria informativa, che concentra nelle mani dell’industria i dati sui quali si sviluppano i sistemi di IA.

⁸ Expert Group on Architecture for AI Principles to be Practiced, *AI Governance in Japan ver. 1.0 – An interim report*, disponibile all’indirizzo: <https://www.meti.go.jp/press/2020/01/20210115003/20210115003-3.pdf>.

⁹ *OECD Principles on AI*, disponibili all’indirizzo: <https://www.oecd.org/going-digital/ai/principles/>; UNESCO, *Elaboration of a Recommendation on the ethics of artificial intelligence*, disponibile all’indirizzo: <https://en.unesco.org/artificial-intelligence/ethics>.

D'altro canto, per evitare che si crei un *gap* tra i principi-guida e le operazioni pratiche intraprese a livello di impresa, secondo l'*Interim Report* giapponese, è necessario introdurre linee guida intermedie non-vincolanti che prendano in considerazione i punti seguenti: evitare di utilizzare standard che si basino su livelli specifici di esperienza nell'utilizzare l'IA, evitare un'applicazione “*one-size-fits-all*” alle imprese interessate, non impedire alle imprese leader di innovare, supportare la gestione del rischio, fissare una soglia di affidabilità del sistema di IA nelle transazioni tra imprese e facilitare le spiegazioni da fornire ai consumatori.

Allo stesso tempo, in considerazione del fatto che tali linee guida non hanno natura vincolante, secondo il Gruppo di Esperti nipponico, dovranno predisporre alcuni incentivi per le imprese ad utilizzare tali linee guida in ogni fase del ciclo di vita del sistema di IA.

All'*Interim Report* ha fatto seguito la pubblicazione, il 9 luglio 2021, delle “*Linee guida di governance per l'attuazione dei principi dell'IA – versione 1.0*”¹⁰, che hanno inserito esplicitamente, tra gli obiettivi d'azione suggeriti alle aziende che sviluppano e gestiscono sistemi di IA, l'opportunità di fissare “*AI governance goals*”, che dovrebbero avere come punto di partenza i sopracitati “*Social Principles of Human-centric AI*”.

Inoltre, pur non essendo formalmente vincolanti, le Linee Guida precisano che, qualora un'azienda dovesse ritenere non necessario fissare un obiettivo di *governance* dell'IA, sul presupposto che gli impatti negativi del proprio sistema di IA siano di entità trascurabile, tale azienda dovrebbe comunque essere in grado di spiegare la ragione di tale scelta a qualunque parte interessata. Di conseguenza, anche in presenza di strumenti regolamentari caratterizzati da una maggiore flessibilità per le aziende, resta comunque imprescindibile la necessità di garantire un elevato grado di trasparenza in riferimento allo sviluppo e all'utilizzo dei sistemi di IA.

1. (segue) che il servizio digitale usi IA o meno.

L'applicazione del nuovo quadro normativo europeo sull'IA ai servizi digitali risulta al momento un punto ancora oggetto di dibattito.

Secondo il considerando 9 della proposta di Regolamento della Commissione europea, quest'ultima non si applicherebbe agli spazi *online*, ma unicamente agli spazi fisici. Questa precisazione sembrerebbe quindi limitare notevolmente l'ambito di applicazione del nuovo quadro normativo.

¹⁰ Expert Group on How AI Principles Should be Implemented, *Governance Guidelines for Implementation of AI Principles Ver. 1.0*, disponibile all'indirizzo: https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20210709_9.pdf.

D'altro lato, il modello prescelto dalla Commissione con la proposta legislativa in esame sembra rappresentare, non tanto un testo unico onnicomprensivo in grado di regolare ogni aspetto dell'IA, quanto piuttosto un frammento del ben più ampio mosaico normativo che definirà, nella sua globalità, la regolamentazione dell'IA.

In particolare, questo primo segmento normativo sembra voler far riferimento ad una standardizzazione dei prodotti di IA, sul modello della marchiatura CE, più che ai sistemi di IA incorporati in servizi digitali.

Alla luce di ciò, risulta quindi ancora più necessaria la coordinazione del presente testo di proposta legislativa con il diritto dell'UE già esistente e con quello attualmente *in fieri*. In riferimento ai servizi digitali, un ruolo preminente è infatti da attribuire al *Digital Services Act* (“DSA”), attualmente in discussione nel Parlamento europeo.

Pur non essendovi espressa menzione di sistemi di IA nel DSA, l'IA è indirettamente toccata da tale proposta in considerazione degli algoritmi incorporati in molte applicazioni digitali che ne costituiscono il *target* principale. Il DSA intende aggiornare le norme in materia di responsabilità degli intermediari di servizi *online*, attualmente ancora disciplinate dall'*e-commerce Directive* adottata nel lontano 2000. Attraverso il DSA, la Commissione europea spera di chiarire le responsabilità poste in capo alle piattaforme *online*, soprattutto in riferimento alla rimozione di contenuti, beni e servizi illegali.

A tal proposito, l'attività di filtraggio su *internet* viene affidata principalmente ad algoritmi. Ecco, dunque, che torna in gioco la necessità di regolare l'IA, anche in rapporto al suo utilizzo associato ai servizi digitali.

Come già evidenziato in riferimento alla proposta di Regolamento sull'IA, anche nel caso del DSA il fine ultimo è quello di assicurare il rispetto dei diritti fondamentali degli utenti che utilizzano i servizi digitali ricompresi nel suo ambito di applicazione.

La chiave di lettura per comprendere dunque i tentativi della Commissione europea di regolare il mondo digitale e le nuove tecnologie sembra dunque essere quella di garantire una traslazione dei valori fondamentali che regolano l'ambiente *offline* e i prodotti “tradizionali” all'ecosistema *online* e ai prodotti frutto dei più recenti sviluppi tecnologici.

In quest'ottica, la proposta IA dunque non va letta come un *corpus iuris* a sé stante, ma come un tassello di un *puzzle* ancora in costruzione che andrà a definire la regolamentazione del prossimo *digital decade* nell'UE.

La vera sfida che si pone in questo momento in Europa, dunque, è quella di garantire che i vari pezzi del *puzzle* combacino insieme e non si sovrappongano indebitamente.

L'approccio metodico, basato sul rischio e che pone le sue fondamenta nel sostrato valoriale dell'Unione, sembra costituire una buona base di partenza. Resta però da vedere come si articolerà l'edificio normativo che poggerà su di essa.

2. (segue) che la piattaforma che usa IA sia un *gatekeeper* o no

Discorso analogo a quello sui servizi digitali si può effettuare rispetto a sistemi di IA che siano parte di una piattaforma *gatekeeper*.

Anche in questo caso, la proposta di Regolamento sull'IA pubblicata il 21 Aprile 2021 dalla Commissione europea nulla prevede in merito, rendendo pertanto necessario il ricorso al testo che si pone come obiettivo specifico la regolazione dei *gatekeeper*: il *Digital Markets Act* ("DMA"). Come si evince dal termine inglese che li identifica, i problemi associati alle piattaforme *gatekeeper* risiedono essenzialmente nella loro capacità, in virtù delle loro grandi dimensioni, di essere guardiane dell'accesso a determinati mercati digitali.

Su tali piattaforme, dunque, per via della loro capacità di "filtraggio" si sono concentrate principalmente le attenzioni delle Autorità *antitrust* europee in virtù dei potenziali danni che esse possono arrecare nei confronti dei consumatori e/o di piattaforme appartenenti a parti terze.

Le piattaforme *gatekeeper* hanno spesso favorito i propri servizi e prodotti rispetto a servizi e prodotti analoghi forniti dai concorrenti¹¹. Tali corsie preferenziali si sviluppano grazie a sistemi di classificazione dei prodotti e dei servizi che si basano, nella maggior parte dei casi, su algoritmi predefiniti.

Pur nulla prevedendo specificatamente in materia, dunque, l'IA riveste ancora una volta un ruolo cruciale in riferimento al funzionamento di tali meccanismi anticoncorrenziali. Si pensi, ad esempio, agli algoritmi che sono alla base dei servizi di pubblicità digitale, spesso generati sulla base dei dati forniti dall'utente.

In tal senso, un settore che merita particolare attenzione, anche per il suo porsi in una zona di confine tra i prodotti che potrebbero ricadere nell'ambito di applicazione della proposta di Regolamento e le piattaforme *gatekeeper*, sono i sistemi di IA incorporati nei prodotti di assistenza vocale (spesso prodotti da società esse stesse qualificabili come *gatekeeper*).

Questo settore, meglio noto come *Internet of things* ("IoT"), costituisce un modello paradigmatico della necessità di convergere i diversi tentativi di regolare il mondo digitale e le nuove tecnologie.

¹¹ Cfr., ad esempio, la recentissima sentenza del giudice europea nella causa *Google Shopping*, T-612/17.

Non solo regolazione dell'IA e diritto *antitrust*, ma anche tutela dei dati personali e *data governance* si rivelano dunque essere inscindibilmente legati tra loro nell'approccio al diritto del futuro.

Non a caso, la Commissione europea, nell'estate 2020, ha condotto un'indagine di settore proprio sui rischi *antitrust* che possono generarsi dall'IoT.

Tale indagine si collocava, in modo sinergico, nell'ambito di un più ampio *assessment* condotto “*nel quadro della strategia digitale europea e mirata a valutare le iniziative regolatorie sull'IA; sui dati e sulle piattaforme digitali*”¹².

Il risultato dell'indagine è stato pubblicato il 9 giugno 2021.

Nel *report* preliminare¹³, la Commissione europea ha confermato che, sebbene l'IoT costituisca una tecnologia ancora in fase di evoluzione, solleva numerose preoccupazioni sotto il punto di vista del diritto della concorrenza.

In particolare, la Commissione ha evidenziato come vi siano quattro grandi operatori nel mercato che si pongono sempre più come *gatekeepers* in riferimento ai programmi di assistenza vocale, impedendo in tal modo l'ingresso di altri concorrenti sul mercato per via dei costi proibitivi per sviluppare e lanciare sistemi analoghi.

Emerge quindi con evidenza, anche in relazione agli algoritmi utilizzati all'interno dei cosiddetti *smart device*, un chiaro collegamento con il concetto di *gatekeeper* delineato nell'ambito del DMA.

Sorprendentemente, però, i sistemi di assistenza vocale non sono stati inseriti nell'ambito di applicazione della proposta della Commissione in questione. L'espressa inclusione degli assistenti vocali e dei servizi abilitati con la voce è stata espressamente richiesta dal relatore del DMA nel Parlamento europeo. L'estensione dell'ambito di applicazione del DMA, tale da ricoprire l'IA stessa, sembra quindi essere ancora un punto del tutto aperto.

Uno studio specifico dei danni che gli algoritmi potrebbero causare alla concorrenza nel mercato e ai consumatori è stato pubblicato dall'Autorità britannica della concorrenza (*Competition Markets Authority*, “CMA”) lo scorso 19 gennaio 2021¹⁴. Tale *report* analizza i rischi potenziali non solo con riferimento ai *gatekeepers*, ma anche in relazione ad una serie di condotte normalmente considerate anti-competitive e realizzate

¹² *EC press release on IoT sector inquiry*, disponibile all'indirizzo: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1326.

¹³ Commissione Europea, *Internet of Things Preliminary Report* https://ec.europa.eu/competition-policy/system/files/2021-06/internet_of_things_preliminary_report.pdf.

¹⁴ Competition & Markets Authority, *Algorithms: how they can reduce competition and harm consumers*, disponibile all'indirizzo: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/954331/Algorithms_++.pdf.

mediante l'uso di algoritmi (ad esempio, la personalizzazione dei prezzi, il *ranking* discriminatorio, pratiche collusive, pratiche esclusive).

Secondo la CMA, il problema comune che caratterizza tali condotte, riguarda l'assenza di un'effettiva supervisione della piattaforma che utilizza l'algoritmo in grado di determinare la condotta anti-competitiva.

Una tale mancanza risulta poi acuita nel caso in cui la piattaforma digitale in questione sia anche un *gatekeeper*, dal momento che dai loro algoritmi dipende l'esistenza di un grande numero di altre piattaforme di minori dimensioni.

La conclusione principale cui è giunta la CMA è dunque quella di imporre alle imprese un obbligo di trasparenza rispetto agli algoritmi utilizzati.

Soltanto se le piattaforme sono infatti in grado di spiegare il funzionamento dell'algoritmo stesso, l'Autorità competente potrà adottare misure efficaci per contrastare eventuali danni concorrenziali.