NOMOS
Le attualità nel diritto
Quadrimestrale di Teoria generale,
Diritto pubblico comparato e Storia costituzionale

FLAVIA ZORZI GIUSTINIANI*

I LEGISLATORI EUROPEI RAGGIUNGONO UN ACCORDO SULLE PRIME REGOLE PER L'INTELLIGENZA ARTIFICIALE AL MONDO NONCHÉ SUI REQUISITI ESSENZIALI PER I PRODOTTI CON ELEMENTI DIGITALI**

SOMMARIO: 1. L'accordo provvisorio sul Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale. – 2. L'accordo provvisorio sul Regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali.

1. L'accordo provvisorio sul Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale

L'**8 dicembre** scorso il Parlamento europeo ed il Consiglio hanno raggiunto l'accordo provvisorio sul Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale, proposto dalla Commissione nell'aprile 2021[1]. L'accordo è stato raggiunto ad esito di un trilogo di eccezionale durata (37 ore in tre giorni), a dimostrazione del rilievo del tema.

L'esigenza di una regolamentazione della materia era stata indicata dalla Presidente della Commissione europea Ursulta von der Leyen, all'inizio del suo mandato, tra le priorità della Commissione per il periodo 2019-2024[2]. Nel Libro Bianco sull'intelligenza artificiale (di seguito IA), pubblicato il 19 febbraio 2020, la Commissione aveva poi definito le opzioni strategiche utilizzabili per il conseguimento del duplice obiettivo di promuovere l'adozione dell'IA e affrontare i rischi connessi a determinati utilizzi di siffatta tecnologia[3]. La successiva proposta di Regolamento sull'intelligenza artificiale è stata poi adottata dalla

* Professoressa associata di Diritto dell'Unione europea – Università degli Studi "Link Campus University" di Roma.

** Contributo sottoposto a *peer review*.

[1] Cfr. COMMISSIONE EUROPEA, *Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (Legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione*, Bruxelles, 21 aprile 2021, COM(2021) 206 final.

[2] Cfr. *Un'Unione più ambiziosa. Il mio programma per l'Europa, Orientamenti politici per la prossima Commissione europea 2019-2024*, https://commission.europa.eu/system/files/2020-04/political-guidelines-next-commission_it.pdf.

[3] COMMISSIONE EUROPEA, *Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia*, Bruxelles, 19 febbraio 2020, COM(2020) 65 final.

ISSN 2279-7238

Commissione al fine di attuare il secondo obiettivo, creando le condizioni per lo sviluppo e l'utilizzo di un'IA affidabile nell'Unione[4].

Si deve altresì rilevare che un intervento legislativo in materia era stato specificamente richiesto sia dal Parlamento europeo che dal Consiglio europeo. Quest'ultimo, in particolare, nelle sue conclusioni sul piano coordinato sullo sviluppo e l'utilizzo dell'intelligenza artificiale "Made in Europe" aveva sottolineato l'importanza di garantire il pieno rispetto dei diritti dei cittadini europei rivedendo a tal uopo la normativa esistente[5]. Quanto al Parlamento, dal 2020 ha adottato un numero considerevole di risoluzioni concernenti aspetti vari attinenti all'IA[6]. Tra queste rileva soprattutto la risoluzione concernente un quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate, giacché la stessa contiene una vera e propria proposta legislativa di regolamento sui principi etici per lo sviluppo, la diffusione e l'utilizzo dell'IA, della robotica e delle tecnologie correlate[7]. Risoluzione di cui ha debitamente tenuto conto la Commissione nella sua proposta.

La proposta di Regolamento sull'IA, come presentata dalla Commissione, intende definire un quadro normativo armonizzato per lo sviluppo, l'immissione sul mercato e l'utilizzo di sistemi di IA nell'Unione che sia sicuro nonché rispettoso dei diritti fondamentali e dei valori dell'Unione, e altresì che segua un approccio "basato sul rischio". La scelta di regolamentare gli utilizzi, più che la tecnologia in quanto tale, è stata effettuata col preciso intento di contrastare l'obsolescenza della normativa. Trattandosi del primo tentativo mai effettuato di regolamentare la materia, la suddetta proposta costituisce un ulteriore contributo dell'Unione a fissare norme e standard con potenziale effetto globale promuovendo nel contempo i propri valori e interessi[8].

Nel suo approccio *risk-based*, la Commissione aveva classificato in quattro livelli i rischi associati agli usi specifici dell'IA (minimi o nulli, limitati, elevati e inaccettabili), differenziando di conseguenza le norme applicabili. L'accordo provvisorio raggiunto da

---

[4] COMMISSIONE EUROPEA, *Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (Legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione*, 21 aprile 2021, COM(2021) 206 final, punto 1.4.1.

[5] CONSIGLIO DELL'UNIONE EUROPEA, *Intelligenza artificiale b) Conclusioni relative al piano coordinato sull'intelligenza artificiale* - Adozione 6177/19, 2019. Un primo riferimento all'IA tra le tendenze emergenti a cui far fronte era stato fatto dal Consiglio europeo già nella sua riunione del 19 ottobre 2017 (cfr. *Conclusioni EUCO 14/17*, 2017, p. 8). V. anche CONSIGLIO DELL'UNIONE EUROPEA, *Conclusioni della presidenza – La Carta dei diritti fondamentali nel contesto dell'intelligenza artificiale e della trasformazione digitale*, 11481/20, 2020.

[6] Cfr. Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate, 2020/2012(INL); 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); Risoluzione del Parlamento europeo del 20 ottobre 2020 sui diritti di proprietà intellettuale per lo sviluppo di tecnologie di intelligenza artificiale, 2020/2015(INI); Progetto di relazione del Parlamento europeo sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale, 2020/2016(INI); Progetto di relazione del Parlamento europeo sull'intelligenza artificiale nell'istruzione, nella cultura e nel settore audiovisivo, 2020/2017(INI).

[7] Cfr. Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate, 2020/2012 (INL).

[8] Si è parlato al riguardo di "effetto Bruxelles" (espressione coniata da Anu Bradford in *Effetto Bruxelles. Come l'Unione Europea regola il mondo*, Milano, Franco Angeli, 2021) per descrivere la capacità unilaterale dell'Unione di regolare i mercati globali stabilendo i propri standard.

Consiglio e Parlamento si concentra precipuamente su modelli di IA per finalità generali[9] ad alto impatto e su sistemi di IA ad alto rischio. I sistemi di IA che presentano solo un rischio limitato dovrebbero pertanto essere soggetti esclusivamente ad obblighi di trasparenza molto leggeri, come l'avvertimento che il contenuto è frutto dell'IA. Quanto ai sistemi ad alto rischio, i colegislatori hanno convenuto di autorizzarne una cospicua serie ridefinendo al contempo i requisiti di conformità in modo da rendere il loro rispetto più semplice dal punto di vista tecnico e meno oneroso per i portatori di interessi. È prevista inoltre una valutazione d'impatto sui diritti fondamentali prima della loro immissione sul mercato.

Tra i sistemi di IA che sono stati vietati, in quanto comportanti rischi inaccettabili, figurano invece tra l'altro: sistemi di manipolazione cognitiva del comportamento; la raccolta indiscriminata di immagini del volto da Internet o da telecamere a circuito chiuso per creare database di riconoscimento facciale; i sistemi di riconoscimento delle emozioni, installati nei luoghi di lavoro o in istituti di formazione; sistemi di punteggio sociale; i sistemi di categorizzazione biometrica per dedurre dati sensibili quali convinzioni politiche, religiose, filosofiche, orientamento sessuale, etnia; e in alcuni casi, i sistemi di polizia predittiva (*predictive policing*) volti a prevedere un reato prima che questo avvenga.

Quanto ai sistemi di identificazione biometrica remota a fini di attività di contrasto, l'accordo provvisorio definisce le situazioni, eccezionali, e le tipologie di reati con riferimento alle quali le autorità di contrasto saranno autorizzate a servirsene. Più in generale, le modifiche introdotte con riguardo all'uso dei sistemi di IA a fini di attività di contrasto rispondono all'esigenza di rispettare la riservatezza dei dati operativi sensibili. È stato inoltre predisposto un meccanismo volto a garantire la tutela dei diritti fondamentali da eventuali abusi di detti sistemi.

L'accordo provvisorio è intervenuto anche sulla definizione stessa di sistema di IA, allineandola allo standard – globalmente riconosciuto - delineato dall'OCSE, e ciò al fine di distinguere chiaramente l'IA da sistemi software più semplici. Quanto al suo ambito di applicazione, viene chiarito che il regolamento non dovrebbe intaccare le competenze degli Stati membri in materia di sicurezza nazionale e che non si applicherà ai sistemi utilizzati esclusivamente per scopi militari o di difesa né a quelli utilizzati soltanto per fini di ricerca e innovazione o a coloro che utilizzano l'IA per motivi non professionali.

Sono state poi fatte delle integrazioni, rispetto alla proposta originale, al fine di tenere specifico conto di quelle applicazioni dell'IA caratterizzate dalla loro versatilità, impiegabili per finalità generali, come l'IA generativa. É stata pertanto introdotta una disciplina specifica per i sistemi di IA per finalità generali e, più in particolare, per i modelli di base, ovvero i grandi sistemi capaci di svolgere con competenza un'ampia gamma di compiti distintivi, quali la generazione di video, testi, immagini, la conversazione in linguaggio laterale, il calcolo di dati o la generazione di codici informatici. Detti modelli di base dovranno rispettare specifici requisiti di trasparenza per poter essere immessi sul mercato. Per i modelli di base ad alto impatto, che sono addestrati con grandi quantità di dati e di

[9] Si tratta di sistemi che possono essere utilizzati ed adattati ad un'ampia gamma di applicazioni.

complessità, capacità e prestazioni particolarmente avanzate, è poi previsto un regime *ad hoc* volto a scongiurare rischi sistemici, con ulteriori obblighi relativi alla gestione dei rischi e al monitoraggio degli incidenti gravi.

Per quanto concerne la *governance*, oltre alle autorità nazionali di controllo, già indicate dalla proposta della Commissione per il controllo dell'attuazione delle nuove norme a livello nazionale, l'accordo provvisorio prevede la creazione di un apposito ufficio per l'IA all'interno della Commissione con il compito di supervisionare i modelli di IA per finalità generali, contribuire a promuovere norme e pratiche di prova e far rispettare le norme comuni in tutti gli Stati membri. Il suddetto ufficio potrà avvalersi del supporto di un gruppo scientifico di esperti indipendenti, che fornirà consulenza in merito allo sviluppo di metodologie per valutare le capacità dei modelli di base e ai rischi di sicurezza connessi a siffatti modelli.

In tema di sanzioni pecuniarie, l'accordo provvisorio prevede dei massimali più proporzionati con riguardo alle PMI e alle start-up rispetto a quanto generalmente previsto (7% del fatturato annuo globale realizzato nell'esercizio finanziario precedente all'illecito per le violazioni relative ad applicazioni di IA vietate, 3% per violazioni degli obblighi del Regolamento e 1,5% per la fornitura di informazioni inesatte).

Infine, i legislatori hanno modificato sostanzialmente le disposizioni concernenti le misure destinate a promuovere l'innovazione. È stato così stabilito che i sandbox regolamentari sull'IA, destinati a creare un ambiente controllato per lo sviluppo, le prove e la convalida di sistemi di IA innovativi, dovrebbero anche consentire il test di sistemi di IA innovativi in condizioni simili al mondo reale. L'accordo provvisorio include poi un elenco di azioni volte a sostenere le aziende più piccole, alleviando i relativi oneri amministrativi e prevedendo alcune deroghe specifiche e limitate.

L'applicazione effettiva del Regolamento negli Stati membri avverrà dopo due anni dalla sua entrata in vigore, ad eccezione delle norme sui divieti e sull'IA per finalità generali, che diverranno vincolanti già dopo rispettivamente 6 e 12 mesi.

2. L'accordo provvisorio sul Regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali

Un secondo, e non meno importante, accordo provvisorio tra Parlamento e Consiglio è stato raggiunto il 30 novembre scorso e concerne il **Regolamento relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020** (*Cyber Resilience Act*, di seguito CRA). La Commissione europea aveva presentato la sua proposta di CRA il 15 settembre 2022[10], dando seguito a

[10] Cfr. Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020, Bruxelles, 15 settembre 2022, 2022/0272 (COD).

quanto annunciato dalla Presidente Von der Leyen nel suo discorso sullo stato dell'Unione del 2021[11], nell'intento di rendere più coerente e armonizzata la normativa in vigore in materia di cibersicurezza e di garantire un'efficace protezione dei prodotti digitali (*hardware* e *software*). Attualmente, infatti, il quadro normativo è frammentato e lacunoso, essendo costituito da diversi strumenti, vuoi dell'Unione vuoi degli Stati membri, relativi ai requisiti di cibersicurezza per i prodotti con elementi digitali che non rispondono pienamente ai problemi di sicurezza riscontrati lungo l'intera catena di approvigionamento.

Il CRA si applicherà ai "prodotti con elementi digitali il cui uso previsto o ragionevolmente prevedibile include una connessione dati logica o fisica diretta o indiretta a un dispositivo o a una rete"[12], ad eccezione dei software o servizi *open source* nonché di prodotti già soggetti a requisiti di cibersicurezza sulla base di norme europee vigenti quali i dispositivi medici, i prodotti aeronautici e le automobili. L'accordo provvisorio prevede inoltre la classificazione, secondo una metodologia più semplice, dei dispositivi interessati in tre elenchi diversi sulla base della loro criticità e del livello di rischio per la sicurezza informatica. Su richiesta del Parlamento gli *assets* coperti dalla nuova regolamentazione includono prodotti quali software per sistemi di gestione dell'identità, gestori di password, lettori biometrici, assistenti domestici intelligenti e telecamere di sicurezza private. Il Consiglio invece ha ottenuto l'inclusione del terzo elenco, relativo a *critical products* che dovrebbero essere in possesso di uno specifico certificato di cibersicurezza.

Il Regolamento impone degli obblighi specifici per tipologie di operatori economici: i fabbricanti, gli importatori e i distributori. Al riguardo l'accordo provvisorio mantiene l'impostazione iniziale della Commissione, riguardo in particolare i seguenti punti: l'assolvimento da parte dei fabbricanti di una serie di obblighi finalizzati a garantire che i prodotti digitali siano stati progettati e sviluppati in conformità a precisi requisiti essenziali (indicati nell'Allegato I del CRA); i processi di gestione delle vulnerabilità per i fabbricanti e gli obblighi degli operatori economici quali gli importatori e i distributori in relazione a detti processi; una maggiore trasparenza sulla sicurezza dei prodotti hardware e software per i consumatori e gli utilizzatori commerciali; un quadro di vigilanza del mercato ai fini dell'applicazione delle norme.

Rispetto alla proposta i colegislatori sono intervenuti inoltre in merito agli obblighi di segnalazione di incidenti e vulnerabilità: destinatarie primarie di tali segnalazioni saranno le autorità nazionali competenti invece dell'Agenzia dell'UE per la cibersicurezza (ENISA), la quale era stata inizialmente posta al centro del quadro procedurale di dette notifiche secondo un modello centralizzato di *governance*. Il ruolo dell'ENISA è stato comunque rafforzato e l'Agenzia sarà informata tempestivamente dallo Stato membro interessato in

[11] Una siffatta proposta legislativa era stata peraltro previamente promossa dalla Strategia di *cybersecurity* 2020 dell'UE per il Decennio digitale (Commissione europea e Alto Rappresentante dell'UE per gli Affari Esteri e la Politica di Sicurezza, La strategia dell'UE in materia di cibersicurezza per il decennio digitale, JOIN(2020), 18 final), dalle conclusioni del Consiglio del 2 dicembre 2020 (Consiglio dell'Unione europea, *Council conclusions on the cybersecurity of connected devices*) e dalla Risoluzione del Parlamento europeo del 10 giugno 2021 (Risoluzione del Parlamento europeo del 10 giugno 2021 sulla strategia dell'UE in materia di cibersicurezza per il decennio digitale, (2021/2568(RSP)).

[12] Cfr. art. 2, par. 1, proposta CRA.

modo da poter valutare la situazione segnalata e informare a sua volta gli altri Stati membri in caso di rischi di natura sistemica.

Misure di sostegno supplementari sono state poi approvate a favore di piccole imprese e micro-imprese, come ad esempio particolari attività di sensibilizzazione e formazione, nonché il sostegno alle procedure di prova e di valutazione della conformità.

A partire dall'entrata in vigore del CRA, i fabbricanti, gli importatori e i distributori di prodotti hardware e software disporranno di 36 mesi per confermarsi alle nuove regole[13]. L'eventuale inosservanza dei requisiti essenziali di cibersicurezza e la violazione degli obblighi imposti comporteranno, oltre al ritiro del prodotto digitale dal mercato, l'irrogazione di sanzioni amministrative pecuniarie quali il pagamento di una somma di denaro fino al massimo edittale di 15.000.000 di euro o, nel caso di un'impresa, fino a 2,5% del fatturato totale annuo registrato nell'anno finanziario precedente.

[13] Più limitato (21 mesi) è invece il periodo di tolleranza in merito all'obbligo di comunicazione in caso di incidenti e vulnerabilità.