cepAdhoc

No. 2 | 2020 11 maggio 2020

Strategia europea sull'intelligenza artificiale

Una valutazione del Libro bianco della Commissione europea sull'IA

Alessandro Gasparotti e Lukas Harta

A metà gennaio è stata resa pubblica una bozza del Libro bianco della Commissione sull'intelligenza artificiale (AI), a cui è seguita la pubblicazione della versione ufficiale del Libro bianco il 19/2/2020. Essa mette in evidenza alcuni punti deboli dell'attuale legislazione e introduce tre principali opzioni normative per le azioni future in materia di IA. Il Cep valuta queste opzioni come segue:

► Opzione 1: schema di etichettatura volontario. Questa opzione rispetterebbe la libertà d'impresa, perché le aziende sono libere di decidere se usare o meno l'etichetta. Tuttavia, questo potrebbe non essere sufficiente per affrontare, ad es., i problemi di sicurezza e di responsabilità.

► Opzione 2: Requisiti settoriali per le pubbliche autorità. Questa opzione richiederebbe alle pubbliche autorità di pubblicare informazioni sull'efficacia delle applicazioni di IA che utilizzano. Questo è appropriato, in quanto le pubbliche autorità hanno un maggiore potere di ingerire nei diritti fondamentali delle persone di quanto non ne abbiano i soggetti privati.

► Opzione 3: requisiti obbligatori basati sul rischio (*risk based*) per le applicazioni AI ad alto rischio. Questa opzione prevede la regolamentazione di applicazioni AI ad alto rischio sia nel settore privato che in quello pubblico. Senza una definizione precisa di alto rischio, le aziende saranno incentivate a minimizzare i possibili rischi della loro applicazione di IA in modo che i loro prodotti non debbano conformarsi alle norme per le applicazioni AI ad alto rischio.

1 Contesto politico

Il 17 gennaio 2020 è stato reso pubblico un documento della Commissione Europea intitolato "*Structure for the White Paper on artificial intelligence – a European approach*" (Bozza per il Libro bianco sull'Intelligenza Artificiale - un approccio europeo)[1]. La pubblicazione ufficiale del Libro bianco è poi avvenuta il 19 febbraio 2020[2]. Essa fa parte della più ampia strategia della Commissione in materia di intelligenza artificiale (di seguito: "IA"), che comprende la Comunicazione sull'intelligenza artificiale per l'Europa[3], il Piano Coordinato sull'intelligenza artificiale[4] e la Comunicazione sulla creazione di un clima di fiducia nell'intelligenza artificiale umanocentrica[5] (cfr. cep**PolicyBriefs** sugli investimenti[6], sull'istruzione e i sistemi sociali[7], sulle norme giuridiche ed etiche[8], e sulle linee guida etiche[9]). A questo proposito, la Presidente della Commissione Europea Ursula von der Leyen si è impegnata a "presentare una proposta legislativa per un approccio europeo coordinato alle implicazioni umane ed etiche dell'intelligenza artificiale"[10] entro i primi 100 giorni del suo mandato. Inoltre, il 23 gennaio 2020, la Commissione per il Mercato Interno e la Protezione dei Consumatori del Parlamento Europeo ha approvato una risoluzione sui "processi decisionali automatizzati: garantire la tutela dei consumatori e la libera circolazione di beni e servizi"[11]. La risoluzione sottolinea, tra l'altro, la necessità di un approccio alla regolamentazione dell'IA basato sul rischio, ed invita la Commissione a sviluppare uno schema di valutazione del rischio per l'IA al fine di garantire un approccio coerente all'applicazione della legislazione sulla sicurezza dei prodotti nel mercato interno. Inoltre, in uno scambio di opinioni con la commissione giuridica del Parlamento europeo il 27 gennaio 2020, Margrethe Vestager, Vicepresidente Esecutivo della Commissione Europea per un'Europa pronta per l'era digitale, ha sottolineato la necessità di stabilire standard elevati per l'IA nell'UE, in particolare standard elevati di trasparenza e responsabilità per le tecnologie di IA utilizzate nel settore pubblico[12].

Il Libro Bianco reso pubblico afferma che "lo scopo dell'approccio europeo è quello di promuovere lo sviluppo e l'adozione dell'intelligenza artificiale in tutta Europa, garantendo al contempo che la tecnologia sia sviluppata e utilizzata nel rispetto dei valori e dei principi europei"[13]. Secondo la Commissione, tre campi di intervento sono fondamentali per raggiungere questi obiettivi: gli investimenti, l'accesso ai dati e la regolamentazione dell'intelligenza artificiale. Per promuovere gli investimenti nell'IA, la Commissione intende utilizzare i fondi di finanziamento dell'UE al fine di

- creare "un'infrastruttura di calcolo e dati di intelligenza artificiale leader mondiale in Europa"[14]
- rafforzare i centri di innovazione digitale che miglioreranno la diffusione dell'IA, e

---

1 https://euractiv.com/wp-content/uploads/sites/2/2020/01/AI-white-paper-EURACTIV.pdf.
2 Commissione Europea, Libro Bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia, COM(2020) 65 final, sul quale verrà pubblicato a breve uno specifico cep**PolicyBrief**.
3 COM (2018) 237.
4 COM (2018) 795.
5 COM (2019) 268.
6 Centre for European Policy: cep**PolicyBrief** No. 2019-10.
7 Centre for European Policy: cep**PolicyBrief** No. 2019-12.
8 Centre for European Policy: cep**PolicyBrief** No. 2019-13.
9 Centre for European Policy: cep**PolicyBrief** No. 2019-16.
10 Von der Leyen: Orientamenti politici per la prossima Commissione Europea 2019-2024, disponibile in: https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_it.pdf, p. 14.
11 2019/2915(RSP).
12 www.euractiv.com/section/digital/news/eus-vestager-calls-on-public-sector-to-establish-particularly-high-ai-standards/.
13 Commissione Europea: Libro bianco sull'IA reso pubblico, disponibile in: https://euractiv.com/wp-content/uploads/sites/2/2020/01/AI-white-paper-EURACTIV.pdf, p. 1.
14 Ibid p. 5.

- garantire l'accesso ai finanziamenti per gli innovatori dell'IA.

A tal fine la Commissione dovrebbe pubblicare una revisione del Piano coordinato sull'AI[15]. Inoltre, la Commissione mira a sviluppare spazi di dati comuni europei e intende adottare, entro l'inizio del 2021, un provvedimento attuativo relativo a dataset di alto valore per il settore pubblico. Questi dataset dovrebbero essere disponibili gratuitamente e in un formato leggibile con apparecchi meccanici. La parte principale del Libro bianco pubblicato riguarda il terzo campo di attività: la regolazione dell'IA. E' per questa ragione che questo cepAdhoc si concentra sulla regolazione dell'IA.

2 La bozza di Libro bianco sulla regolamentazione dell'IA

2.1 Carenze dell'attuale legislazione sull'IA

L'intelligenza artificiale offre molte opportunità, ad es. svolgere compiti complessi in una frazione del tempo richiesto da un essere umano, ma pone delle sfide in relazione alla sicurezza e alla responsabilità per i prodotti dotati di tale tecnologia.

Le sfide derivano, tra l'altro, dall'autonomia dei prodotti abilitati all'IA - ovvero quando i prodotti abilitati all'IA svolgono i loro compiti senza la supervisione umana - e dall'opacità del processo decisionale dell'IA - cioè quando comprendere il processo che ha portato a un risultato specifico è difficile o addirittura impossibile.

La Commissione riconosce nel Libro bianco che esiste già un solido corpus legislativo a livello di UE e di Stati membri che si applica all'IA[16]. I due principali atti legislativi dell'UE che regolano i requisiti di sicurezza e il regime di responsabilità per l'uso dell'IA sono la Direttiva sulla sicurezza generale dei prodotti[17] e la Direttiva sulla responsabilità del prodotto[18]. Ciononostante, la Commissione sottolinea anche che - a causa del rapido sviluppo dell'IA - la legislazione esistente potrebbe non coprire tutti i rischi specifici che sono destinati a sorgere con l'uso diffuso dell'IA. Dopo una prima fase di consultazione con gli Stati membri, le imprese e le altre parti interessate, la Commissione ha individuato, tra l'altro, i seguenti tre punti deboli dell'attuale legislazione:

(1) Aggravamento dei rischi dovuto all'autonomia decisionale dei prodotti abilitati all'IA

La Commissione menziona, tra l'altro, i rischi per la sicurezza personale, le minacce informatiche e i rischi associati alla perdita di connettività, specialmente se un prodotto abilitato all'IA si basa sul /operatività in cloud (*cloud computing*) per funzionare. Se, ad es., un automobilista usa un sistema di navigazione satellitare, una perdita di connettività non comporta gravi rischi per la sicurezza; è sempre l'automobilista che guida l'auto, e non il sistema di navigazione. Se, invece, un'auto a guida autonoma perde la connettività, l'auto non riceve più alcuna informazione sulla sua posizione attuale, sull'andamento della strada, sulle condizioni della strada o sulle condizioni del traffico. Questo può condurre ad una velocità inappropriata. Allo stesso modo, mentre un sistema di navigazione per auto hackerato che guida il conducente in modo errato può essere molto scomodo per l'utente, un'auto a guida

[15] COM (2018) 795.

[16] Commissione Europea, Libro Bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia, COM(2020) 65 final, p. 10.

[17] Direttiva 2001/95/CE del Parlamento europeo e del Consiglio, del 3 dicembre 2001, relativa alla sicurezza generale dei prodotti.

[18] 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.

autonoma hackerata potrebbe essere usata per causare gravi incidenti o addirittura condurre attacchi terroristici. Pertanto, gli attacchi informatici possono aggravare le conseguenze dell'azione prodotta da un processo decisionale autonomo.

(2) Cambiamento della natura dei prodotti abilitati all'IA durante il loro ciclo di vita

È probabile che i prodotti abilitati all'IA mutino durante il loro ciclo di vita, in particolare a causa dell'apprendimento automatico (*machine learning*) - ovvero quando un'applicazione di IA esegue un determinato compito senza essere esplicitamente programmata per svolgerlo, utilizzando invece modelli ed inferenze - o sostanziali aggiornamenti del database che i prodotti abilitati all'IA adoperano per esercitarsi.

Un prodotto abilitato all'IA potrebbe soddisfare gli standard di sicurezza al momento della prima immissione sul mercato, che è il punto temporale rilevante sia ai sensi della Direttiva sulla responsabilità del prodotto[19] che della Direttiva sulla sicurezza generale dei prodotti[20]. Tuttavia, esso potrebbe non rispettare questi standard in una fase successiva, a causa di un'evoluzione del suo comportamento, ad es. se emergono risultati diversi a causa dei nuovi dati. Ad es., se un orologio per fitness abilitato all'uso dell'IA tarato su dati equilibrati viene immesso sul mercato, potrebbe, con il tempo, raccogliere dati di persone prevalentemente attive e sane.

Se l'orologio utilizza questi dati per suggerire un certo tipo di allenamento agli utenti, potrebbe incoraggiare le persone anziane o inadatte ad allenarsi troppo, con rischi per la loro salute. Inoltre, ad es. se l'orologio controlla autonomamente un dispositivo di stimolazione muscolare elettrica, gli utenti potrebbero venire danneggiati dal dispositivo senza avere il controllo sulla decisione assunta per tramite dell'IA.

(3) Difficoltà legate all'applicazione della legge

I prodotti abilitati all'IA spesso non si basano più su un codice di facile lettura. Mentre il risultato nella maggior parte dei casi è più preciso, non sempre è possibile comprendere la causalità o il processo decisionale dell'IA. Ad es., se un software abilitato all'IA intervista i candidati a un'offerta di lavoro, i criteri che portano alla sua decisione possono risultare non trasparenti. Pertanto, se un candidato ritiene di essere stato discriminato, l'individuazione ed il possibile il risarcimento della discriminazione potrebbero risultare irrealizzabili.

2.2 Opzioni normative per la legislazione futura

Per affrontare i punti deboli dell'attuale legislazione, il Libro Bianco presenta tre possibili opzioni normative:

Opzione 1: Sistema di etichettatura volontario

Gli sviluppatori di IA che soddisfano determinate condizioni sarebbero autorizzati ad utilizzare l'etichetta di "IA etica/affidabile". La conformità a tale sistema di etichettatura andrebbe implementata. Inoltre, la Commissione ritiene che un programma di etichettatura aiuterebbe l'Europa a svolgere un ruolo importante nelle discussioni internazionali su un'IA etica ed affidabile[21]. Tuttavia, la Commissione

[19] Art. 7 lett. b della Direttiva 85/374/EEC.
[20] Art. 3 par. 1 della Direttiva 2001/95/EC.
[21] Centre for European Policy: cep**Input** No. 2019-07.

afferma che i sistemi volontari potrebbero non essere sufficienti a risolvere, ad es., le questioni relative alla sicurezza e alla responsabilità.

cep**Assessment**: Questo approccio è il meno oneroso per gli sviluppatori e gli utenti di IA, perché l'uso dell'etichetta è volontario. Pertanto, l'opzione 1 rispetta la libertà d'impresa. Gli sviluppatori di IA sosterranno costi aggiuntivi solo se decideranno di conformarsi al programma. Tuttavia, se l'etichetta è altamente apprezzata dai consumatori, le aziende saranno spinte ad aderire al sistema volontario, in modo da segnalare ai consumatori la loro "affidabilità". Anche in questo caso, tuttavia, lo schema di etichettatura è appropriato perché porta le aziende a soddisfare i desideri dei consumatori e aumenta la trasparenza per i consumatori. La questione relativa a quale autorità dovrebbe essere responsabile della concessione e dell'applicazione di tali etichette non viene discussa nel Libro Bianco. Lo schema di certificazione introdotto dal Regolamento Generale sulla Protezione dei Dati (di seguito: "GDPR")*, che dimostra che le aziende rispettano le sue regole, indica tuttavia che questo aspetto è molto importante. Lo schema di certificazione GDPR è utilizzato raramente, perché non viene applicato in modo coerente nell'UE** in quanto le autorità nazionali interpretano il GDPR in modo diverso e stabiliscono standard differenti per ottenere la certificazione. Questo distorce la concorrenza nel mercato interno, e riduce la certezza del diritto per le imprese certificate in un Paese quando operano in un altro. È quindi fondamentale creare un sistema armonizzato e chiari requisiti da rispettare per ottenere il marchio UE per una IA affidabile.

* Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche in relazione al trattamento dei dati personali e alla libera circolazione di tali dati.

** Centre for European Policy: cep** PolicyBrief** No. 2020-01.

Opzione 2: Requisiti settoriali per le autorità pubbliche e riconoscimento facciale

Questo approccio stabilisce i requisiti per le autorità pubbliche quando utilizzano prodotti abilitati per l'IA. Come la direttiva canadese sul processo decisionale automatizzato, questi requisiti comportano regole per

- valutazioni d'impatto degli algoritmi utilizzati (ovvero i requisiti per valutare gli impatti degli algoritmi su decisioni amministrative, per cui le decisioni più importanti verrebbero esaminate più attentamente),
- garanzia di qualità (cioè requisiti che garantiscano che i dati utilizzati dall'applicazione di IA siano testati rispetto alla possibilità di alterazioni indesiderate dei dati e di altri fattori che possono distorcere i risultati),
- meccanismi di ricorso,
- rendicontazione (ad es., l'obbligo per le pubbliche autorità di pubblicare informazioni sull'efficacia e l'efficienza delle applicazioni di IA nel soddisfare gli obiettivi delle autorità pubbliche su un sito web).

L'obiettivo dell'opzione 2 sarebbe quello di garantire che le pubbliche autorità utilizzino l'IA in modo da ridurre i rischi per le pubbliche istituzioni e determinare decisioni più efficienti, accurate, coerenti e comprensibili.

cep**Assessment**: Il vantaggio di questa opzione è la regolamentazione settoriale e specifica dell'IA. Dal momento che le autorità pubbliche hanno un potere significativamente maggiore di quello degli attori privati di interferire con i diritti fondamentali delle persone, la regolamentazione dell'uso dell'IA da parte delle autorità pubbliche è più urgente che tra attori privati. Inoltre, la chiara definizione del campo di applicazione della legislazione sull'IA aiuterebbe gli sviluppatori e gli utenti di IA a stabilire se tale regolamentazione (ad es. l'obbligo di segnalazione) si applica o meno anche a loro. Le autorità pubbliche saprebbero con certezza che è così, gli utenti privati saprebbero con certezza che non è così. Pur disciplinando solo l'uso dell'IA da parte delle autorità pubbliche, la regolamentazione prevista dall'opzione 2 potrebbe tuttavia avere un effetto di indirizzo anche per il settore privato, incoraggiando le aziende a rispettare gli standard essenziali del settore pubblico per dimostrare la loro "affidabilità" ai consumatori. Alcuni consumatori potrebbero preferire prodotti che soddisfano i requisiti delle autorità pubbliche rispetto a prodotti più economici che non lo fanno. Un tale approccio alla regolamentazione potrebbe ottenere, nel settore privato, il risultato previsto

Nell'ambito dell'opzione 2 la Commissione discute inoltre se sia opportuno introdurre norme specifiche per l'uso di sistemi di riconoscimento facciale negli spazi pubblici, o se l'uso di tale tecnologia negli spazi pubblici debba essere vietato, ad es., per un periodo da tre a cinque anni. Durante questo periodo, occorrerebbe individuare e sviluppare una solida metodologia per valutare gli impatti di questa tecnologia e le possibili misure di gestione del rischio. Il divieto dei sistemi di riconoscimento facciale si applicherebbe sia agli attori pubblici che a quelli privati. Andrebbero valutate eccezioni, ad es., per scopi di ricerca e sviluppo e di sicurezza.

cep**Assessment**: Se è vero che la tecnologia di riconoscimento facciale pone più sfide ai diritti fondamentali rispetto a molte altre applicazioni di IA, una misura di ampia portata come il divieto totale della tecnologia di riconoscimento facciale potrebbe ostacolarne lo sviluppo all'interno dell'UE, come riconosciuto dalla stessa Commissione. Ciò è tanto più vero in quanto questo mercato è già dominato da imprese esterne all'UE. Inoltre, oltre a vietare la tecnologia di riconoscimento facciale, la legislazione sull'IA non coprirebbe affatto i soggetti privati.

Opzione 3: Requisiti obbligatori basati sul rischio (*risk-based*) per le applicazioni IA ad alto rischio

La nuova legislazione sull'IA si applicherebbe solo alle applicazioni di IA ad alto rischio, mentre la legislazione esistente - ad es. il GDPR - continuerebbe ad applicarsi a tutte le applicazioni. Un modo per definire le applicazioni di IA ad alto rischio sarebbe quello di valutare se un'applicazione

- rientra in uno dei settori particolarmente sensibili, che andrebbero chiaramente specificati (ad es. sanità, trasporti, polizia e giustizia),
- soddisfa una definizione più astratta di applicazione "ad alto rischio"; tale definizione potrebbe essere la seguente: "Per applicazioni ad alto rischio si intendono le applicazioni di intelligenza

artificiale che possono produrre effetti giuridici per persone fisiche o giuridiche, o comportare il rischio di lesioni, morte o danni materiali significativi per persone fisiche o giuridiche"[22].

cep**Assessment**: Il vantaggio principale di questa opzione è che potrebbe coprire tutte le applicazioni IA ad alto rischio - anche quelle del settore privato - in modo dinamico e flessibile. L'interpretazione del termine "ad alto rischio" è comunque discrezionale e, se non definita con precisione, offrirà alle imprese un incentivo a minimizzare i possibili rischi del loro prodotto in modo che le loro applicazioni di IA non debbano soddisfare gli standard per le applicazioni ad alto rischio.* Inoltre, il Libro bianco reso pubblico lascia aperto quale potrebbe essere il contenuto dei requisiti basati sul rischio, limitandosi ad affermare che un tale strumento potrebbe richiedere requisiti di trasparenza

2.3 Ulteriori opzioni di regolamentazione

Inoltre, la Commissione prende in considerazione due ulteriori opzioni di regolamentazione che possono essere combinate con una qualsiasi delle tre opzioni sopra menzionate:

(1) Legislazione in materia di sicurezza e responsabilità

La Commissione sta valutando la possibilità di modificare la legislazione esistente in materia di sicurezza e di responsabilità - tra cui la direttiva sulla sicurezza generale dei prodotti, la direttiva sui macchinari[23], la direttiva sulle apparecchiature radio[24] e la direttiva sulla responsabilità dei prodotti - al fine di affrontare i rischi specifici dei prodotti abilitati all'IA.

cep**Assessment**: Il vantaggio di questo approccio è che affronta i punti deboli dell'attuale legislazione che la Commissione ha individuato, senza introdurre atti legislativi specifici per l'IA. Ciò evita di creare obblighi specifici per distinti settori, attori o categorie di applicazioni di IA.

(2) Governance

Gli Stati membri dovrebbero incaricare le autorità esistenti o istituirne di nuove, con il compito di monitorare l'applicazione e lo sviluppo del futuro quadro normativo per l'IA.

cep**Assessment**: Come ha dimostrato l'applicazione del GDPR, è fondamentale che le autorità nazionali siano sufficientemente finanziate e dispongano degli strumenti per cooperare con le altre autorità dell'UE. Inoltre, alcuni metodi operativi delle autorità nazionali dovrebbero essere armonizzati, altrimenti la frammentazione giuridica potrebbe distorcere la concorrenza nel mercato interno, ad es. per quanto riguarda l'imposizione di sanzioni.*

[22] Commissione Europea: Libro bianco sull'IA reso pubblico, disponibile in: https://euractiv.com/wp-content/uploads/sites/2/2020/01/AI-white-paper-EURACTIV.pdf, p. 16.
[23] Direttiva 2006/42/CE del Parlamento europeo e del Consiglio, del 17 maggio 2006 , relativa alle macchine.
[24] Direttiva 2014/53/UE del Parlamento europeo e del Consiglio, del 16 aprile 2014 , concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di apparecchiature radio.

2.4 Osservazioni finali

La Commissione sembra essere a favore di un approccio basato sul rischio (opzione 3). Tale approccio potrebbe essere applicato dalle autorità nazionali ed accompagnato da una legislazione aggiornata in materia di sicurezza e di responsabilità. È interessante notare come la Commissione scoraggi il divieto delle tecnologie di riconoscimento facciale, favorendo invece la sua regolamentazione attraverso la piena attuazione delle pertinenti disposizioni del GDPR.