

# Un'intelligenza artificiale a misura di democrazia? Intervista a Brando Benifei

*di Francesco Nasi*

04-01-2024

L'8 dicembre Consiglio e Parlamento europeo hanno raggiunto un accordo politico sull'AI Act, il regolamento europeo sulle applicazioni dell'intelligenza artificiale che entrerà gradualmente in vigore nel corso dei prossimi due anni in tutti i Paesi membri dell'Unione Europea. Il pacchetto europeo di regole rappresenta la prima legge al mondo che ambisce ad affrontare complessivamente le numerose sfide poste dallo sviluppo e dalle applicazioni dell'intelligenza artificiale. Per riflettere su questi temi abbiamo intervistato Brando Benifei, eurodeputato e co-relatore dell'AI Act al Parlamento europeo.

Da dove nasce l'esigenza di una regolamentazione dell'intelligenza artificiale? Quali questioni e problematiche mirano ad essere affrontate dalla legislazione?

Brando Benifei: L'esigenza di costruire una legislazione ad hoc sull'intelligenza artificiale nasce innanzitutto dalla crescente importanza che questi sistemi stanno assumendo nella vita dei cittadini. Inizialmente, l'AI era utilizzata principalmente nell'ambito della ricerca scientifica e operativa. Successivamente, è stata introdotta nel mondo dell'impresa e del lavoro. Nel corso del tempo, è diventata sempre più parte integrante delle abitudini quotidiane dei cittadini, grazie all'utilizzo di applicazioni generative e altre tecnologie. Dal punto di vista dell'Unione Europea, l'intuizione dell'AI Act nasce da un percorso di confronto avviato dalle istituzioni europee con gli stakeholder del settore, che ha portato successivamente alla nascita dell'High Level Working Group on Artificial Intelligence. Già alla fine della scorsa legislatura, il Parlamento europeo aveva discusso l'impatto dei robot sul diritto civile, mentre nell'attuale legislatura si era focalizzato sull'uso dell'AI nel campo della cultura e dell'informazione, quando ancora si era lontani dall'esplosione dell'AI generativa. La commissione AIDA (Artificial Intelligence in a Digital Age) ha poi individuato dei rischi e dei beni da proteggere che sono stati la scintilla per arrivare ad una legislazione specifica. È stata individuata la necessità di una tutela preventiva rispetto alla mera azione giudiziaria ex post, assieme ad alcuni beni fondamentali: la salute, la sicurezza, i diritti fondamentali così come concepiti dalla Carta europea ecc. È emersa così la necessità di un framework di riduzione dei rischi e col negoziato che abbiamo concluso si sono poi aggiunti e consolidati i riferimenti alla tutela dell'ambiente e dei processi democratici.

Come si pone questo regolamento nei confronti della legislazione affine già esistente, come il General Data Protection Regulation (GDPR), il Digital Markets Act (DMA) e il Digital Services Act (DSA)? Qual è la differenza tra queste legislazioni? Non si corre il rischio di confusione o, per lo meno, di una certa sovrapposizione?

Brando Benifei: Dal punto di vista della normazione esistente, l'AI Act non arriva in uno spazio vuoto. Faccio un esempio emblematico: in Italia ChatGPT è stato bloccato per un certo tempo per via di una decisione del Garante della protezione dei dati personali, che ovviamente ha applicato delle norme esistenti, senza rifarsi all'AI Act o ad un altro tipo di legislazione specificamente pensata per l'intelligenza artificiale. L'AI Act sta infatti dentro un quadro più ampio sui dati e il mercato unico

digitale. Il Digital Markets Act e il Digital Services Act sono due legislazioni fondamentali, rispettivamente sul mercato digitale e le regole che devono rispettare le piattaforme. A questi, si aggiungono certamente il Data Governance Act, la Cyber Security Regulation, che ha da poco concluso la negoziazione e il già esistente GDPR. Io credo valga per l'AI Act quello che è valso per il Digital Services Act: all'inizio sembrava che fossimo gli unici a voler fare regole per le piattaforme e non limitarci solamente a codici di condotta volontari e linee guida. Passava che noi volessimo essere protezionisti e mettere regole impossibili, aspetti che avrebbero reso l'Unione Europea isolata. Questi ragionamenti sono stati superati: ora tutto il mondo sta procedendo verso una maggior regolamentazione. Lo stesso executive order sull'AI del presidente statunitense Joe Biden appare come una sorta di "vorrei ma non posso", in quanto istruisce le agenzie federali di portare avanti una serie di azioni per la gestione dei rischi che assomigliano a quello che noi prevediamo nell'AI Act. La differenza è che non può vincolare direttamente i privati, ma solo l'amministrazione pubblica, perché non è un atto del Congresso. In questo modo però prefigura e incoraggia un'azione futura in tale direzione.

Veniamo ora alla legge vera e propria. Innanzitutto, quali sono i principi fondamentali che ispirano l'AI Act?

Brando Benifei: Possiamo individuare due obiettivi ultimi di questa legge, strettamente legati l'uno all'altro. Il primo è rendere l'intelligenza artificiale compatibile con la democrazia. Il secondo è rafforzare la fiducia, far sapere ai cittadini che ci sono misure per ridurre i rischi e i pericoli. Avendo incontrato in presenza e online tanti governi e parlamenti del resto del mondo, soprattutto nell'ambito dei Paesi OCSE (che hanno un gruppo di lavoro specifico), del G7 e dei Paesi più industrializzati, si tratta di temi che vanno avanti in parallelo da tempo. La riduzione del rischio è ormai nel linguaggio comune. L'Unione Europea fa però una scelta che nessuno ha fatto finora: portare la regolamentazione soft allo step successivo, una vera e propria legge che implica responsabilità legali e nuovi strumenti per i cittadini per essere tutelati e protetti. Il senso del regolamento è infatti anche quello di dare un nuovo equilibrio alla catena delle responsabilità tra i vari attori dell'ecosistema dell'intelligenza artificiale. È necessario che gli sviluppatori si prendano le loro responsabilità, non scaricandola tutta sugli utilizzatori intermedi o i cittadini/utenti. Il processo richiederà in ogni caso un po' di tempo: dal voto finale previsto per marzo o aprile inizierà un'entrata in vigore graduale, partendo dai divieti in sei mesi, poi gli obblighi per i sistemi più potenti in dodici mesi fino al resto del regolamento in ventiquattro mesi. Serve infatti tempo per sviluppare standard riconosciuti per la verifica della conformità dei prodotti agli obblighi previsti, come la qualità dei dati usati per l'addestramento o il livello di cybersicurezza.

L'AI Act distingue i vari sistemi di intelligenza artificiale in base a diverse categorie di rischio. Che cosa significa questo? In base a cosa viene calcolato il rischio?

Brando Benifei: Le categorie di rischio sono tre, con una variante. La prima è il basso rischio. In questo caso i sistemi di AI devono sottostare solo ai principi generali di buona programmazione, gestione dei dati e rispetto dei diritti fondamentali. Non si tratta di obblighi cogenti, ma indirizzi con cui per esempio un giudice può valutare un comportamento particolarmente negligente. Il basso rischio è identificato per esclusione: sono i sistemi che non rientrano nelle altre categorie. Esiste poi una variante, il rischio limitato. Si fa riferimento a quei sistemi a cui chiediamo una maggiore trasparenza. Parliamo, per esempio, dei chatbot non generativi, che per essere conformi al nostro mercato dovranno rendere esplicito il fatto che sono sistemi autonomi e non esseri umani. L'alto rischio è il cuore del regolamento. È identificato sulla base di un allegato, l'allegato 3, che contiene le aree di potenziale alto rischio: luoghi di lavoro, amministrazione della giustizia, democrazia, impatto sui minori in alcuni contesti, assegnazione di diritti civili e sociali,

infrastrutture digitali critiche, ecc. A leggerlo, pare che sia tutto, ma in realtà non è così. Degli attuali sistemi di AI in uso, soltanto una percentuale tra il 20 e il 25% ricadrebbe in queste categorie. L'alto rischio viene identificato anche attraverso l'articolo 6, un "filtro" che esenta i sistemi meramente accessori che non influiscono su un processo decisionale. Per esempio, in ambito medico, non sono necessari ulteriori controlli per sistemi che migliorano il linguaggio della traduzione di una email per un paziente o l'organizzazione di un archivio. Il principale obbligo che i sistemi ad alto rischio devono rispettare è il superamento di un conformity assessment (CA) prima dell'immissione nel mercato, per verificare che il sistema non presenti rischi significativi per le persone. Il conformity assessment è svolto dagli stessi sviluppatori, ma è molto impegnativo e non può essere calato in un contesto specifico. Per questo motivo il Parlamento ha poi introdotto la cosiddetta verifica d'impatto sui diritti fondamentali (fundamental rights impact assessment), che va a vedere l'impatto sui diritti fondamentali di un sistema nel contesto in cui viene utilizzato. Questa è meno impegnativa e può essere allargata agli utilizzatori. Gli utilizzatori non sono tanto gli utilizzatori finali, ma i deployer, gli utilizzatori intermedi. Per fare un esempio concreto, se in una scuola un sistema di AI ha superato il conformity assessment ma è chiaramente ad alto rischio perché riguarda l'uso per la valutazione delle performance scolastiche dei minori, alcuni controlli ulteriori devono essere previsti. Ogni scuola, poi, nel momento in cui ha composizioni variegata, presenta rischi di discriminazioni molto diverse. Per questo è necessario uno strumento specifico come il fundamental rights impact assessment, che si cala nelle realtà particolari, prevedendo comunque un controllo più "semplice" e meno tecnico rispetto al conformity assessment. I divieti sono l'ultimo livello, il cosiddetto rischio inaccettabile. Un classico esempio è il riconoscimento biometrico in tempo reale negli spazi pubblici. Una telecamera indiscriminatamente utilizzata per prevenire crimini potrebbe infatti diventare uno strumento di sorveglianza di massa molto pericoloso, per questo non può essere utilizzata. Il centro del regolamento rimane comunque l'alto rischio. I divieti sono divieti, e una volta definiti la discussione finisce. Ma nel caso dell'alto rischio ci sono stati vari tentativi di annacquare e cercare scappatoie, per far sì che la normazione ci fosse ma allo stesso tempo fosse aggirabile, per esempio giocando sulla definizione di open source. Questo ambito è esentato dal rispetto del regolamento nel caso non ci sia una messa sul mercato del prodotto; dunque, l'esenzione è limitata allo sviluppo per fini di sperimentazione e non copre la commercializzazione, che diventa condizionata al rispetto delle regole previste. Su questo siamo stati molto attenti, per impedire che i grandi sviluppatori potessero usare questa scappatoia o altre per evitare regole e controlli.

Durante la fase di negoziazione che lei ha guidato, qual è stata la posizione dei diversi gruppi del Parlamento europeo sui contenuti del regolamento?

Brando Benifei: Siamo arrivati al voto favorevole del Parlamento europeo nel giugno del 2023 dopo una lunga negoziazione, a cui era seguita un'altrettanta lunga fase per capire quale commissione (e di conseguenza quale gruppo politico) si sarebbe dovuto occupare di questo tema. È stato il frutto di mesi di negoziazioni in seno all'organismo dei presidenti di commissione che decide l'attribuzione del file. Ci sono state pressioni significative che hanno mostrato l'interesse delle famiglie politiche ad avere un maggior peso in questo lavoro, che si iniziava a capire sarebbe stato di grande rilevanza. Le commissioni incaricate alla fine sono state due, la mia (Mercato interno e protezione consumatori) e quella Libertà civili e giustizia. Già nella fase preliminare, c'è stato un braccio di ferro con il Partito Popolare Europeo, che spingeva verso un assetto diverso delle commissioni coinvolte. Il PPE voleva attribuire il ruolo di commissione principale a quella giuridica, al limite in associazione con quella sulle libertà civili. Questo avrebbe dato a Popolari e Liberali la guida della negoziazione. Il fatto che il negoziato sia stato invece guidato da un collega di Renew Europe (Drago? Tudorache, ex ministro degli interni della Romania) e da me, un esponente dei Socialisti, ha permesso di costruire una maggioranza ampia con il coinvolgimento dei Verdi, che hanno avuto un impatto

importante. Abbiamo fatto più di un anno di discussioni con migliaia di emendamenti che abbiamo dovuto compattare in compromessi politici. I Verdi hanno lavorato molto sul tema ambientale. I Liberali sul tema della governance, per esempio in termini di rafforzamento della tutela dei consumatori e sul rapporto tra il board europeo dell'AI e le autorità nazionali, dando più poteri a quello che al termine del negoziato col Consiglio si è poi arrivati a chiamare AI Office, l'organismo europeo che sarà istituito all'interno della Commissione europea e dovrà sovrintendere all'implementazione del regolamento. Esso avrà un particolare ruolo nella gestione della regolamentazione dei modelli più potenti, come GPT o Gemini, ai cui sviluppatori abbiamo richiesto alcune verifiche di sicurezza prima che diventino sistemi posti sul mercato, in questo modo tutelando "all'origine" anche i tanti sviluppatori europei che usano e useranno sempre di più questi modelli. Noi socialisti ci siamo concentrati sulle tutele nel mondo del lavoro, ad esempio rendendo obbligatoria l'informazione dei lavoratori e delle forze sindacali sull'uso dei sistemi e permettendo agli Stati membri di fare ulteriore legislazione nazionale a tutela dei diritti senza incorrere in violazione di norme di mercato. Abbiamo poi spinto sulla tutela dei dati e sul tema dei divieti specie per gli ambiti a rischio discriminazioni come la categorizzazione biometrica volta a inferire opinioni politiche, orientamento sessuale o fede religiosa, questioni che hanno visto un fronte ampio delle forze progressiste impegnarsi assieme. I gruppi della destra hanno cercato di ridurre l'ambito di applicazione della norma, con il PPE che voleva dare più mano libera agli sviluppatori. Su altri punti c'è stata una visione comune, come nel caso della definizione dell'intelligenza artificiale e gli ambiti esclusi. Abbiamo infatti convenuto, ad esempio, l'esclusione della ricerca, che non verrà sottoposta alle regole dell'AI Act. Abbiamo trovato poi l'accordo politico con il Consiglio la notte dell'8 dicembre dopo trentasei ore di negoziati difficili, specialmente sulle regole per i modelli più potenti e sui divieti, precedute da altri quattro triloghi politici nell'arco di alcuni mesi in cui abbiamo trovato l'accordo sugli altri temi dirimenti.

Quali sono stati le novità portate dal lavoro del Parlamento europeo rispetto alla precedente proposta della Commissione europea?

Brando Benifei: La proposta della Commissione, pur non mancando di ambizione, sostanzialmente tralasciava alcuni aspetti che noi abbiamo invece ripreso, e su alcuni temi era meno coraggiosa di come poi l'abbiamo resa. Sembrava quasi che fosse già pronta per ricevere un facile assenso da parte dei governi nazionali, che in generale mirano ad una legislazione più soft. Il Parlamento, grazie ad una gestione politica di un certo tipo, ha messo in evidenza alcuni aspetti e nel negoziato è riuscito a portare a casa dei risultati importanti. Tra questi, abbiamo rafforzato i divieti. Abbiamo espanso tutti quelli che hanno a che fare con i temi della sicurezza e del controllo delle persone. Ad esempio, abbiamo vietato il controllo emotivo per studenti e lavoratori, mentre per i controlli della polizia e sui migranti abbiamo ottenuto il riconoscimento dell'alto rischio. Questi sono grossi cambiamenti perché nella proposta della Commissione erano usi considerati a basso rischio. Abbiamo poi rafforzato il divieto del riconoscimento biometrico in tempo reale negli spazi pubblici con solo pochissime eccezioni di possibile utilizzo per la ricerca di persone accusate di crimini gravissimi e sotto stretto controllo della autorità giudiziaria e dell'autorità di garanzia dei dati personali. Abbiamo poi vietato la polizia predittiva e il social scoring anche da parte dei privati. Per quanto riguarda i sistemi ad alto rischio, per l'uso da parte di autorità pubbliche e di privati che fanno attività legata ai servizi pubblici, a cui abbiamo aggiunto banche e assicurazioni, è stato introdotto il fundamental rights impact assessment menzionato prima, non presente nella prima versione della Commissione. Poi, abbiamo inserito il tema ambientale in modo molto più forte. Questo è anche il frutto del peso politico dato all'asse coi Verdi e con la parte più progressista di Renew Europe all'intero del negoziato. Si sono rafforzati i requisiti per la verifica di conformità e negli obblighi a vario livello. Il tema del consumo energetico e dell'impatto ambientale è stato inserito in più parti del

testo, con obblighi che prima non erano presenti. Allo stesso modo, c'era poco sul tema della tutela dei lavoratori e dell'uso dell'AI nel contesto lavorativo. Noi abbiamo invece previsto la consultazione con le parti sociali per l'adozione dei sistemi di AI nei luoghi di lavoro. I sindacati europei in particolare sono stati molto d'aiuto per rafforzare il riferimento alle parti sociali, che era assolutamente assente nel testo originario. Il PPE per accettare di sostenere alcune di queste proposte ha voluto che si trovasse un equilibrio tra l'allargamento degli ambiti potenzialmente ad alto rischio e la qualificazione di questi stessi sistemi attraverso l'articolo 6 che menzionavo prima. Oltre a questo, un altro punto avanzato dai popolari, ma che anche noi socialisti condividevamo a patto di rafforzare alcune salvaguardie, è il rafforzamento delle sandboxes, cioè gli strumenti di sperimentazione prima dell'ingresso del mercato. Abbiamo anche dato maggior organicità al rispetto del GDPR all'interno del regolamento. Nel tema della governance, abbiamo rafforzato il coordinamento europeo rispetto alla proposta della Commissione. Una modifica che è oggetto dell'attenzione dei media è l'introduzione di regole per i sistemi di AI generativa e a uso generale, come ChatGPT. Questi sistemi, non avendo un campo di utilizzo predefinito, sfuggivano alle definizioni del regolamento nella sua formulazione originaria.

Per quanto riguarda le definizioni, sappiamo che quella di intelligenza artificiale è contestata e non esiste un accordo all'interno della comunità scientifica. Come si è posto il Parlamento europeo rispetto a questo tema?

Brando Benifei: Noi non definiamo l'intelligenza artificiale, ma i sistemi di intelligenza artificiale. Si tratta di una definizione abbastanza ampia che include anche sistemi meno complessi, allineata con il lavoro dell'OCSE. Socialisti e Verdi avevano pensato di allargare magari anche ad algoritmi semplici, mentre il PPE voleva una definizione che andasse ad eliminare molti sistemi. Trovare un accordo col Consiglio non è stato semplice perché da parte dei governi c'è stata una forte spinta a restringere la definizione. Alla fine, ha però prevalso l'idea di una definizione abbastanza ampia, più di quella prevista dal testo originario della Commissione e in linea col lavoro più recente in sede OCSE. Si tratta di un aspetto importante per il "dialogo" tra questo regolamento con le decisioni prese in termini regolatori nel resto del mondo.

L'ultimo anno ha visto l'ascesa dei sistemi di intelligenza artificiale generativa, come ChatGPT, Midjourney, DALL-E, ecc. All'interno dell'AI Act sono previste misure ad hoc per questi sistemi?

Brando Benifei: L'AI generativa e i foundation models sono stato regolati facendo un'eccezione al principio di legare la regolazione agli usi specificamente intesi. Nel caso dei modelli alla base della AI generativa e dei sistemi ad essi sottostanti, questo uso previsto non è facilmente identificabile. Noi stabiliamo che per i modelli più potenti ci siano una serie di verifiche da parte degli sviluppatori, a prescindere dal loro utilizzo e dalla loro applicazione più nota, come l'AI generativa. Per quest'ultima, abbiamo inserito alcuni obblighi di "trasparenza rafforzata", come la necessità di inserire un watermarking dei contenuti, rendendoli così identificabili, riconoscibili come tali e non prodotti da esseri umani. Questo è utile, per esempio, per aumentare la riconoscibilità dei deep fakes. Inoltre, abbiamo inserito tutte le salvaguardie possibili per contrastare la produzione di contenuti illegali. È stata poi proposta la necessità di fare un riassunto sufficientemente dettagliato dei contenuti protetti da copyright utilizzati per allenare il sistema: questo protocollo non va a cambiare le regole sul copyright, ma vogliamo dare ai creativi uno strumento di trasparenza. Ugualmente prevediamo di rendere obbligatorio l'opt out e quindi la non utilizzabilità dei propri contenuti per allenare determinati sistemi senza un consenso raggiunto tramite un accordo. Con queste regole il New York Times avrebbe potuto evitare una causa, perché Open AI avrebbe dovuto dichiarare già di sua spontanea volontà i contenuti utilizzati e sarebbero quindi scattate le tutele della proprietà intellettuale senza una causa in tribunale lunga e costosa. Per noi deve essere il più

---

chiaro possibile quali dati sono stati utilizzati per allenare il sistema, in modo che autori e artisti possano chiedere una compensazione. Se un sistema di AI generativa viene utilizzato in un ambito della categoria ad alto rischio, dovrà poi seguire anche gli obblighi di cui abbiamo parlato prima.

Una delle principali critiche rivolte all'AI Act è quella di mettere un freno allo sviluppo tecnologico, in un momento storico in cui la competizione con giganti come Stati Uniti e Cina imporrebbe invece di dare "libero sfogo" al mercato. Secondo lei è corretta questa interpretazione?

Brando Benifei: Questo tipo di discussione verrà superata. Parlando con i policymakers di tutto il mondo (americani, canadesi, brasiliani, giapponesi) abbiamo notato l'attenzione globale su ciò che stiamo facendo. È un dibattito in corso, ma c'è una direzione di marcia in cui si dà per scontato che servono dei framework per la riduzione del rischio basati su leggi e non solo accordi volontari. L'obiezione che una maggior regolamentazione vada a creare dei divari competitivi io non la considero assolutamente fondata. Intanto, le regole vengono applicate a tutti gli sviluppatori. Quindi la legislazione non andrebbe ad attaccare esclusivamente quelli europei, ma chiunque voglia entrare nel nostro mercato, e dubito fortemente che gli sviluppatori oggi presenti sarebbero disposti ad uscire dal mercato europeo. Noi abbiamo anzi previsto con il sistema delle sandboxes un aiuto agli sviluppatori di startup che sono certamente in difficoltà rispetto alle grandi big tech ad ottemperare tutti gli obblighi che sono stati previsti, e quindi c'è un percorso di accompagnamento alla compliance. Tra l'altro lo stesso regolamento, stabilendo che avrà due anni di transizione, permette gradualità e uguaglianza di condizioni. Oggi l'Europa è indietro sull'intelligenza artificiale rispetto a Stati Uniti e Cina, per esempio in termini di condivisione della capacità computazionale, negli investimenti, nella capacità di avere un mercato finanziario e di ricerca di capitali di questi progetti. Non credo che il regolamento risolva o peggiori questi problemi, ma il punto è un altro. Serve una diversa impostazione dal punto di vista politico. Serve una maggior integrazione comunitaria, perché in maniera frammentaria non potremo competere con le grandi potenze. In questo senso, l'AI Act può essere utile per dare all'Unione Europea un ruolo di guida nel dibattito sulla regolazione dell'intelligenza artificiale.

Sam Altman, il CEO di OpenAI che produce ChatGPT, ha paventato il rischio che l'intelligenza artificiale raggiunga la cosiddetta "singolarità", rendendo l'essere umano di fatto obsoleto. Come si pone l'AI Act rispetto alla cosiddetta "intelligenza artificiale generale" e ad altri rischi sistemici, come quelli legati alla corsa alle armi letali autonome? Crede che questi pericoli siano concreti? O dovremmo concentrarci su altro?

Brando Benifei: Questi temi non possono essere ignorati. Sono questioni vere e serie. L'AI può essere usata come arma, e in questo caso deve stare dentro un contesto di accordi internazionali sulla circolazione delle armi. Allo stesso modo, per i sistemi più avanzati sarà necessaria una maggior collaborazione internazionale. In quest'ottica, noi supportiamo le iniziative della Commissione che vuole costruire accordi sul tema dell'AI generativa a livello internazionale, e le iniziative che si stanno prendendo come G7 per avere maggiore coordinamento globale sui rischi sistemici. Noi però siamo contrari a un dibattito che distrae dalla costruzione di norme per la tutela dei rischi che già ci sono: sulla salute, le discriminazioni, la tutela dei dati, la cybersicurezza, i possibili utilizzi per la perpetuazione dei crimini tradizionali, ecc. Non si tratta solo di questioni legate alla geopolitica o addirittura all'estinzione umana, ma di rischi che riguardano la vita concreta e quotidiana delle persone. In una battuta: sì a lavorare ai massimi livelli politici per la riduzione del rischio sistemico, ma non come distrazione contro la regolazione del mercato che l'AI Act propone di fare.

Negli ultimi anni abbiamo visto come il GDPR, seppur all'avanguardia nel panorama globale, abbia

presentato alcune criticità nella fase di implementazione e controllo. Quali misure si prenderanno affinché non accada lo stesso per l'AI Act?

Brando Benifei: Noi abbiamo dato un'indicazione chiara affinché la protezione dei dati sia centrale. Ogni Paese dovrà decidere come fare. In Italia si sta ancora discutendo se affidarsi a qualche struttura ad hoc all'interno di autorità esistenti, o su qualcosa di creato ex novo. Servirà un mix di competenze. Il ruolo delle autorità di supervisione sarà molto importante perché andrà ad incidere rispetto a qualunque azione di controllo per tutelare il rispetto delle norme: pensiamo alla verifica di conformità per gli sviluppatori, agli obblighi di notifica, alla pubblicazione in registri pubblici per i sistemi più pericolosi, ai reclami dei cittadini che si ritengono danneggiati ingiustamente da una decisione presa da un sistema automatizzato. Pensiamo anche all'obbligo di spiegabilità, affinché si capisca perché è stata presa una determinata decisione. L'AI Office sarà poi l'autorità europea che aiuterà quelle nazionali per le investigazioni, per il coordinamento e per l'interpretazione delle norme. In caso di violazioni sufficientemente ampie, abbiamo previsto diverse forme di sanzioni, come multe pecuniarie elevate sulle percentuali del fatturato che possono portare alla sospensione o l'espulsione del nostro mercato. Certamente, si tratta di un lavoro enorme che richiede molte persone formate. Serviranno quindi strutture più solide e investimento in risorse umane e per l'enforcement. Dopo che questa norma sarà approvata, la sfida sarà poi la costruzione della governance a livello europeo e nazionale, e poi le procedure di adeguamento volontario anticipato delle imprese e delle pubbliche amministrazioni. Non si dovrà aspettare il giorno in cui la legge diventerà pienamente obbligatoria, ma lavorarci per tempo. Il commissario Thierry Breton sta infatti lavorando all'AI Pact, il patto che sarà proposto a privati e pubbliche amministrazioni per adeguarsi prima della scadenza alle regole approvate all'AI Act, al fine di evitare le problematiche che si sono presentate ai tempi del GDPR, in termini di difficoltà a adeguarsi alle nuove norme con un sufficiente accompagnamento da parte dei regolatori nei confronti delle imprese e delle istituzioni pubbliche.