S&D
Gruppo dell'Alleanza Progressista dei
Socialisti & Democratici
al Parlamento europeo

EURODEPUTATI PD
Partito Democratico

Regolamento Europeo sull' Intelligenza Artificiale. Prospettive, nodi, strategie

"Il modello europeo per l'Intelligenza Artificiale deve essere un modello affidabile e centrato sull'uomo, che rispetti i nostri diritti e valori fondamentali, che non lasci indietro nessuno, che lavori per la protezione dell'ambiente, che supporti e promuova l'innovazione positiva per il bene della società. L'Europa non dovrebbe essere timida di fronte alla Cina o agli Stati Uniti per promuovere e sostenere i propri standard come leader globale."

Brando Benifei
Capodelegazione PD/S&D
relatore IMCO per l'AI Act

1. L' Intelligenza artificiale

Definizione di intelligenza artificiale
L'intelligenza artificiale (IA) è la capacità di una macchina di riprodurre abilità finora esclusive degli umani quali il ragionamento, l'apprendimento, la pianificazione o la creatività.

Si tratta di una tecnologia dalle innumerevoli declinazioni, e per questo si parla generalmente di "sistemi di intelligenza artificiale", per identificare la varietà di processi e applicazioni in grado di elaborare una risposta complessa ai dati ricevuti.

I sistemi di intelligenza artificiale, infatti, sono in grado di comprendere il proprio ambiente, dare significato alle informazioni che registrano, risolvere problemi anche attraverso l'autocorrezione sulla base delle esperienze pregresse e agire verso un obiettivo preciso.

L'impiego dell'intelligenza artificiale è già endemico: le nostre case, le nostre città, i sistemi di trasporto pubblici e privati sono sempre più intelligenti, ovvero più sicuri, più efficienti, più sostenibili. Le IA più sofisticate sono oramai in grado di proporre modelli predittivi utilissimi ad organizzare servizi essenziali o di risposta all'emergenza, per esempio nel caso di catastrofi naturali, di attacchi alla cybersicurezza o di talune crisi di salute.

Più del 60% della popolazione europea guarda positivamente a IA e robot, ma l'81% ritiene che sia indispensabile una gestione attenta di tutti questi risvolti tecnologici. I cittadini europei hanno ragione: i sistemi di IA presentano coni d'ombra. Ad esempio, l'opacità degli scopi per cui possono essere utilizzati, la dipendenza dai dati per il loro funzionamento, la complessità dei flussi informativi che devono organizzare, i problemi di responsabilità legale e di verifica di legittimità per il loro utilizzo.

L'Unione Europea è il primo attore a livello internazionale che ha deciso di regolamentare i

sistemi di IA, affrontandone gli aspetti più problematici. Il regolamento europeo sull'Intelligenza Artificiale sarà il testo legislativo più importante per questo settore, e sono lieto di esserne relatore nella Commissione Mercato Interno e Tutela dei Consumatori.

Vogliamo sostenere l'innovazione, ma renderla "responsabile", al servizio della persona e delle comunità.

L'importanza della promozione della conoscenza dell'IA
Da legislatori progressisti, la prima preoccupazione sul tema dell'impatto dell'intelligenza artificiale sulla società è quella di verificare che i diritti fondamentali siano tutelati adeguatamente. È vero, infatti, che l'intelligenza artificiale porterà con sé un impatto positivo sull'economia, le imprese, e quindi la popolazione europea tutta, ma dobbiamo comunque fare i conti con la protezione dei diritti dei cittadini. Che, da parte loro, hanno diverse gradazioni di conoscenza del digitale, utilizzano diversamente le applicazioni tecnologiche, hanno bisogni differenti e un grado di rischio differente rispetto all'essere oggetto passivo di applicazioni di IA.

Lo dicono chiaramente i dati dell'indice DESI sullo sviluppo economico digitale in Italia: essere una delle più grandi economie al mondo non comporta automaticamente che la propria popolazione sia altrettanto preparata sui temi del digitale. In Italia, ci posizioniamo molto sotto alla media europea in termini conoscenze digitali medie, e tendiamo alla parte bassa della classifica verso il quartultimo posto.
E se pertanto non agiamo sulla digital literacy a livello comunitario per colmare subito i gap, anche quelle che oggi sono considerate economie di primo livello, come noi, perderanno sempre più posizioni per mancanza di digital skills. Lo abbiamo visto nell'ultimo decennio in cui a raggiungere la classifica delle prime dieci imprese per valore di mercato sono per lo più imprese digitali.

È dunque nostro dovere porre l'attenzione sulla formazione tanto degli studenti che iniziano il loro percorso scolastico e universitario oggi quanto dei lavoratori già inseriti in azienda e che vedranno l'intelligenza artificiale sempre più presente nel loro lavoro quotidiano. Dobbiamo tutelare le persone più deboli che non devono essere lasciate indietro da una società troppo tecnologica e tutti i lavoratori oltre che i cittadini cui i servizi e i prodotti dell'intelligenza artificiale sono destinati. Dobbiamo tenere sempre a mente che l'AI funzione solo se è costruita per l'uomo, se mette l'uomo al centro, altrimenti non serve.
Non dobbiamo permettere che accada quanto già successo nei Paesi Bassi per cui una mancata attenzione nell'impostazione degli algoritmi nel settore pubblico ha messo in crisi moltissime famiglie che si sono viste revocare il proprio diritto a benefici fiscali. Non dobbiamo consentire che l'uso incontrollato di algoritmi di intelligenza artificiale possa penalizzare gli studenti che non che non vengono da università private come è successo nel Regno Unito. Non dobbiamo consentire che dei cittadini innocenti siano arrestati solo per un uso sconsiderato del riconoscimento facciale. Ciò che collega tutti questi casi è la mancata conoscenza del funzionamento dell'intelligenza artificiale.

La formazione a cui dobbiamo pensare tanto per i cittadini quanto per gli addetti ai lavori non è solamente tecnica. Dobbiamo pensare a percorsi formativi nuovi, dove le discipline si intersechino e si completino. Come questi due anni di pandemia ci hanno insegnato che la giusta interazione fra lavoro in presenza e da remoto può essere la soluzione migliore per tutti, allo stesso

modo la contaminazione di materie tecnico scientifiche, etiche, filosofiche, linguistiche, giuridiche, culturali, sarà la strada migliore da percorrere per avere un'intelligenza artificiale che il più possibile riesca a tenere in considerazione le tante sfaccettature della società in cui viviamo. Dobbiamo ricordare che non stiamo costruendo qualcosa di statico, ma qualcosa che interagisce di continuo con le persone e l'ambiente circostante, per loro natura mutevoli.

Dobbiamo insegnare a chi sarà in prima linea su queste tecnologie che l'automazione dei processi che parte da premesse sbagliate avrà come risultato quello di violare i diritti di migliaia di persone con il rischio che sia troppo tardi in alcuni casi per porre rimedio agli errori commessi. Per questo motivo, questa fase di confronto è particolarmente cruciale per anticipare il più possibile i potenziali effetti negativi.

Solo una comunità formata, che capisce le basi dell'IA, può comprenderne il funzionamento senza subirlo. La formazione è un pilastro fondamentale della strategia dell'intelligenza artificiale, per garantire la massima fiducia nel futuro.

2. Sistemi di Intelligenza artificiale in un'economia che cambia

Regole nuove per un'economia nuova
L'attuale mandato delle istituzioni europee, il quinquennio 2019-2024, vede il digitale occupare senza dubbio il primo poto in termini di sforzo legislativo dedicato al settore.
Digital Services Act, sulla responsabilità delle piattaforme,
Digital Markets Act, per regolare i rischi che le big tech pongono al mercato competitivo,
Data governance Act e al Data Act. per regolare il modo in cui i dati possono essere trasferiti da una impresa all'altra e al pubblico per generare valore;
La riforma dei diritti dei lavoratori della gig economy come i rider.
Questi alcuni degli esempi principali del lavoro legislativo in corso d'opera presso il Parlamento Europeo, la Commissione Europea e il Consiglio.
Il nostro impegno come socialisti&democratici è quello di promuovere un'economia digitale antropocentrica, che favorisca soprattutto quelle situazioni nazionali – come la nostra - che non primeggiano in questi settori, ovvero che non lascino indietro nessuno e permettano ai paesi meno moderni di recuperare il gap fin qui accumulato.
In generale le linee guida di tutti i Paesi per l'AI sono simili: attrarre talenti, puntare sulla formazione e sulla connessione tre università e centri di ricerca e imprese, aiutati dalla creazione di Digital Innovation Hubs. Il piano italiano vuole favorire gli investimenti e l'adozione di queste tecnologie tanto nel privato quanto nel pubblico, senza dimenticare il rispetto dei diritti fondamentali e la sostenibilità ambientale.

La formazione
Un nodo cruciale è dunque la formazione, come i dati mostrano. Occorrerà dunque investire in formazione sia con borse di dottorato, sia iniziando l'educazione all'AI dai primi anni di scuola. L'obiettivo dovrà essere, nel lungo periodo, formare operatori per essere competitivi e anche saperli trattenere nella nostra economia, evitando il brain drain – ad esempio innalzando le borse di studio per dottorato più vicino ai livelli degli altri paesi europei; considerato che la borsa di studio in Italia vale oggi circa 15.000 Euro l'anno contro i 48.000 Euro della Germania; e mantenendo un buon livello di opportunità accademiche perché sia il mondo dell'università che il mondo produttivo abbiano forza lavoro formata e in grado di formare le giovani leve.

La gestione della forza lavoro
Le trasformazioni radicali in atto nel mondo economico sempre più digitalizzato rendono improrogabile, urgente una riflessione sul futuro della forza lavoro, in particolare quella che potrebbe uscire prematuramente dal mercato del lavoro con l'adozione più massiva di sistemi di intelligenza artificiale.

Se è vero che le stime del World Economic Forum parlano di 97 milioni di posti di lavoro creati a fronte di 85 milioni persi, non tutti quelli persi saranno riconvertiti nei nuovi. Che fine faranno autisti, controllori, macchinisti? È questo un tema che stiamo già toccando con mano con la perdita di posti di lavoro nella transizione dai motori a scoppio all'elettrico. Quella della re-skilling e up-skilling deve essere una priorità per la politica, nazionale ed europea.

La formazione oggetto del piano sembra guardare solo a chi entra oggi a scuola o all'università ma non a chi si trova a metà del suo percorso lavorativo. Se è vero che l'obiettivo è quello di avere una IA che lavori con l'essere umano a vantaggio di tutti e non di pochi, sarà opportuno prevedere formazione e incentivi ad hoc per queste persone prima che il futuro bussi alla porta.

Contemperare i diritti dei cittadini e l'innovazione delle imprese
La sfida più grande dell'economia digitale è forse questa: da un lato abbiamo la necessità di tutelare tutti i diritti fondamentali, introducendo opportune salvaguardie, in un contesto che, come sappiamo, è particolarmente difficile da regolamentare e i cui output possono essere imprevedibili. Dall'altro abbiamo l'innovazione e le imprese da tutelare, facendone crescere il valore per renderle competitive in un mercato che mai come oggi è da considerarsi globale. Un mercato, quello europeo, che sempre più cerchiamo di rendere "unico", con regole uguali per tutti, dove sia più facile scalare.

Per la famiglia progressista dei socialisti e democratici, tuttavia, è chiara la cornice entro cui vogliamo muoverci: non siamo dell'idea che l'innovazione vada perseguita ad ogni costo. È sempre la tecnologia che deve essere al servizio dell'uomo, mai il contrario.

Se una tecnologia viene messa sul mercato senza una adeguata valutazione dei rischi, in nome della concorrenza con le omologhe cinesi o americane, deve essere sanzionata.

In tutto il percorso della commissione AIDA e della redazione degli emendamenti al testo della Commissione, comunque, abbiamo però naturalmente anche ascoltato le imprese, accogliendo alcune delle loro richieste come l'introduzione dell'aspirazione ad avere data sets per il training e la validazione privi di errori, senza rendere sanzionabile quanti non raggiungano quel livello ottimale.

Abbiamo rafforzato il coinvolgimento delle parti interessate e delle organizzazioni della società civile in diverse disposizioni chiave del regolamento, come gli aggiornamenti dell'allegato III (articolo 7), il processo di standardizzazione, così come le attività del board e i sandbox. Riteniamo fondamentale che tutti questi stakeholder, inclusi i rappresentanti delle PMI, abbiano una sedia al tavolo di queste importanti decisioni, per non lasciare nessuno indietro. Questo non deve essere il regolamento delle big tech, ma di tutte le imprese.

Il FinTech
Il settore finanziario sta subendo una vera e propria rivoluzione dovuta a una forte accelerazione dei processi di digitalizzazione per cui molte delle operazioni che un tempo facevamo allo sportello ora le possiamo fare comodamente grazie al nostro smartphone.

La rivoluzione in arrivo grazie all'intelligenza artificiale sarà ancora più dirompente, e sebbene il settore non sia nuovo all'attività di "regolamentazione" propria dei settori che hanno un forte impatto sui diritti delle persone, non dobbiamo farci cogliere impreparati come legislatori.

Per questo motivo, in questo settore specifico, l'articolo 63 prevede che l'Autorità che dovrà vigilare sull'adozione di sistemi di IA da parte di istituti finanziari sarà quella già competente per questo settore. Questo comporta una fondamentale educazione di queste autorità ai temi dell'intelligenza artificiale e dei possibili bias che questa tecnologia porta inevitabilmente con sé. Non vogliamo infatti che alcuni cittadini siano tagliati fuori dall'accesso al credito per via dell'adozione di sistemi che, guardando magari solo allo storico di chi chiede un credito, non veda il potenziale di un giovane che voglia comprare casa o di uno startupper con una grande idea e poche risorse per realizzarla.

La tutela del cittadino
È frutto del lavoro coordinato del gruppo dei socialisti&democratici se prevarrà una impostazione a difesa netta dei diritti dei cittadini nel nuovo regolamento. Il nostro impegno, infatti, è andato nella direzione di emendamenti sostanziali per tutelare e garantire diritti inalienabili.

Abbiamo inserito un esplicito riferimento al rispetto dei principi fondamentali europei, elencati nell'art. 2 del Trattato dell'Unione. Abbiamo inoltre vietato l'uso da parte della polizia dell'intelligenza artificiale per fare ipotesi predittive, per scongiurare un futuro che veda sostituire al principio della presunzione di innocenza quello della presunzione di colpevolezza.
Abbiamo chiesto che quando l'intelligenza artificiale ad alto rischio è usata nel settore pubblico, tali usi siano riportati nel registro tenuto dalla Commissione. Abbiamo aggiunto ulteriori tutele per i soggetti più deboli come i bambini, prevedendo come ad alto rischio quei software loro indirizzati che abbiano un impatto sul loro sviluppo cognitivo o emozionale.

Abbiamo inserito nella categoria degli usi ad alto rischio gli usi di sistemi per influenzare gli elettori nelle loro scelte politiche.

Un altro punto critico che riguarda l'aspetto della tutela dei diritti del cittadino sorge in relazione alle pratiche che intendiamo proibire: a nostro avviso, rispetto alla proposta della Commissione Europea, è assolutamente necessario ampliare il ventaglio di casi in cui ipotizziamo – e dunque proibiamo- lo sfruttamento delle vulnerabilità di un soggetto, andando oltre l'età e la disabilità, e toccando ulteriori dati sensibili come il sesso, l'orientamento sessuale, l'etnia, la razza, la religione. Anche il social scoring a nostro avviso crea delle problematicità sostanzialmente insormontabili ed è quindi bene eliminarlo, sia nel settore pubblico che in quello privato. Non vogliamo infatti favorire lo sviluppo di una società che utilizzi una serie di informazioni decontestualizzate che possa sfavorire interi gruppi sociali, solitamente i più svantaggiati. Non parliamo di qualcosa di teorico, ne vediamo già gli effetti in altri paesi che non condividono i valori europei. Ci rendiamo conto che l'uso di informazioni di questo tipo possa favorire una profilazione migliore del cliente potendo offrire una offerta più personalizzata, molto utile nel settore bancario che deve valutare il rischio di solvibilità, ma forse i rischi sono ben maggiori delle opportunità.

Lo stesso vale per il rispetto della protezione dei dati personali: abbiamo eliminato infatti ogni esenzione prevista dall'AI Act e abbiamo espressamente aggiunto che il marchio CE sia utilizzabile solo dopo una valutazione d'impatto sulla protezione dei dati.

L'articolo 22 del GDPR già prevede delle salvaguardie in tutti quei casi in cui un processo automatizzato abbia delle conseguenze sui diritti fondamentali delle persone. Tuttavia, è pur vero che, nonostante in GDPR sia in vigore da ormai quattro anni, non tutte le imprese sono sufficientemente trasparenti in questo senso.

L'AI Act è pertanto un'occasione ulteriore per rafforzare le garanzie per il cittadino di richiedere in qualsiasi momento un intervento umano qualora pensi di essere stato discriminato. Non dobbiamo dimenticare che ogni volta che viene utilizzato un processo automatizzato gli errori che normalmente vengono fatti dal singolo operatore sono ripetuti a cascata con un effetto potenziale per la vita di migliaia di persone.

3. Il futuro regolamento europeo per l'Intelligenza Artificiale

Perché una normativa europea
L'Unione Europea è la prima a voler regolare l'intelligenza artificiale, scegliendo una via diversa da quella di altri paesi, che hanno preferito prima accelerare sull'innovazione per arrivare primi sul mercato per poi eventualmente verificare e correggere successivamente le storture che questa porta con sé. Si tratta senza dubbio di un approccio che ha il suo valore, ma che non corrisponde alla "nostra storia".

Non pensare sin da subito agli effetti negativi e ai danni collaterali di un'intelligenza artificiale non adeguatamente progettata significa, in concreto, avere studenti che non possono entrare all'università che vorrebbero, rider costretti a sotterfugi per poter lavorare ingannando l'algoritmo, persone costantemente fermate ai controlli per il colore della pelle, sbagliato, vedersi negato il diritto ad acquistare un biglietto del treno perché si sono prese delle multe. È successo in Asia, succede negli Stati Uniti, inizia a succedere anche in Europa.

L'Olanda, ad esempio, è stata esemplare nel mostrare cosa potrebbe andare storto quando i processi di automazione tramite algoritmi non vengono gestiti con adeguata supervisione e a seguito di una adeguata valutazione d'impatto. L'amministrazione pubblica olandese ha erroneamente chiesto indietro alcuni sussidi agli aventi diritto. In Italia un caso analogo ha riguardato, in questi anni di pandemia, gli studenti universitari: a causa della mancata di serie valutazioni d'impatto, si sono usati inadeguati strumenti di controllo automatizzato degli studenti durante i loro esami online: uno sguardo distolto dalla webcam bastava a bloccare l'esame in quanto visto come indizio di uno studente che copiava.

Per quanto possiamo ritenere un bene che i singoli Stati inizino dunque a comprendere, e correggere, storture come queste, è chiaro che solo una normativa europea può garantire uno sviluppo armonico di tutto il settore dei sistemi di IA.

La Commissione Parlamentare speciale AIDA
Durante la seduta plenaria dell'Europarlamento del 18 giugno 2020 è stata istituita la commissione AIDA, una commissione speciale sull'intelligenza artificiale creata nell'intento di stabilire una tabella di marcia a lungo termine sull'IA.

Il mandato di questa commissione speciale è durato 12 mesi ed è stato poi rinnovato.
La commissione ha organizzato audizioni e seminari con le parti interessate (esperti, responsabili politici, comunità degli imprenditori). A seguito di tali appuntamenti è stato possibile trarre alcune conclusioni e delineare una sorta di "roadmap" strategica per il futuro dell'Intelligenza Artificiale, votata e condivisa da tutto il Parlamento.

Anche grazie al lavoro costante di AIDA, la Commissione Europea – che inizialmente aveva prescelto in materia un approccio di soft power limitato alla pubblicazione nel 2019 delle "linee guida" per l'attuazione di sistemi di IA rispettosi dei diritti individuali, ha virato verso un approccio più solido. Nella primavera 2021 la Commissione Europea ha proposto la propria bozza di regolamento orizzontale in tema di Intelligenza Artificiale, forse il più importante testo legislativo della legislatura.

Ambiti di applicazione
Abbiamo tentato di studiare alcuni principali ambiti di potenziale applicazione dell'Intelligenza artificiale, per anticipare le necessità che il contesto normativo dovrà saper individuare e accogliere.
Salute: l'IA porta diversi benefici, ma non dobbiamo fare troppo affidamento sul suo utilizzo in questo campo, i suoi limiti in alcuni settori sono già stati individuati. Dovrebbe prima di tutto includere una forte etica per progettazione, e piuttosto supportare i medici, non sostituirli, rimangono invece preoccupazioni sui dati sanitari particolarmente sensibili.
Green Deal: bisogna considerare la potenziale impronta negativa dell'IA, nel suo consumo di energia per l'immagazzinamento dei dati, così come il suo uso massiccio di materie prime rare, per assicurarci di compensarle abbastanza da far sì che l'IA contribuisca alla neutralità del clima, al consumo sostenibile e alla protezione dell'ambiente.

Competenze digitali: importanza dell'apprendimento permanente, necessario per superare alcuni pregiudizi, dalla diversità alla promozione dell'uguaglianza di genere, anch'essa fondamentale in questo senso. Necessario un livello base di alfabetizzazione digitale per tutti i cittadini, compresi gli anziani, affinché possano partecipare attivamente alla società. L'adozione dell'IA dovrebbe infatti porre particolare attenzione ai gruppi vulnerabili, come i bambini, gli anziani, le persone con disabilità e altri gruppi discriminati, anche in termini di salute mentale.
Lavoro: il nostro puntuale riferimento è quello alla proposta S&D in commissione EMPL "AI in the workplace", che peraltro importante paragrafo sulla sorveglianza dei lavoratori: vi è un rischio di abusi nell'utilizzo di AI da parte dei datori di lavoro. Maggiore coinvolgimento delle parti sociali nell'adozione dell'IA sul posto di lavoro.

Difesa, l'uso dell'IA per scopi militari dovrebbe rispettare pienamente il diritto internazionale umanitario e la legge sui diritti umani, riferimento alla richiesta del Parlamento per un divieto internazionale sullo sviluppo, la produzione e l'uso di sistemi di armi autonome letali, così come il regime di restrizioni al controllo delle esportazioni dell'UE per le tecnologie a doppio uso, che non possono essere esportate a regimi autoritari per essere utilizzate per la sorveglianza di massa e la repressione.

Competitività, preoccupazione per la frammentazione ancora persistente del mercato unico digitale UE, importante completare il quadro sui dati e approvare rapidamente una legislazione come il DSA, il DMA e l'AI Act, che stabilirà un mercato unico per l'IA e creerà certezza giuridica e condizioni di parità per sostenere le nostre imprese e i nostri ecosistemi di innovazione.

Minimo comune denominatore: un approccio antropocentrico per la bozza di regolamento
Già attraverso la lettura della bozza di regolamento come proposta dalla Commissione Europea, si è evidenziato che le istituzioni comunitarie sono concordi nel ritenere che far primeggiare il mercato significherebbe sacrificare il modello sociale basato sui diritti dell'individuo che tanto faticosamente abbiamo costruito nei decenni passati.

Tuttavia, sostanzialmente le opinioni comuni si risolvono qui, ovvero la materia si presenta così articolata che il lavoro per allargare il consenso comune sulla disciplina da adottare è lungo, faticoso, titanico.

Proprio per la difficoltà intrinseca di normare tutte le variabili che l'intelligenza artificiale copre, sono state coinvolte molte commissioni parlamentari per esprimere pareri, e addirittura due sono le commissioni responsabili del file: la Commissione Mercato Unico (IMCO) e la Commissione LIBE per i diritti interni.

Siamo già a oltre a un anno di lavoro parlamentare. Auspichiamo che entro il 2023 la posizione del Parlamento Europeo, che prevediamo venga raggiunta in un lasso di tempo ragionevole, sia discussa nei triloghi interistituzionali con la Commissione Europea ed il Consiglio e si concluda in tal modo l'iter legislativo del regolamento nel quadro di questa legislatura.

4. AI, stress test di fronte a scenari immaginari

L'AI Act è forse il regolamento che meglio incorpora il concetto di stress test. La sua natura orizzontale e il fatto che ci troviamo ancora nella fase iniziale dello sviluppo potenziale della tecnologia di IA sono la più grande sfida per un legislatore che si ponga l'obiettivo di favorire una vera e propria rivoluzione tecnologia e sociale con l'introduzione di basi legislative valide per i prossimi 10 o 20 anni.

Come legislatori, infatti, è nostro dovere scrivere delle leggi che possano resistere bene al passare del tempo, elastiche a sufficienza per regolare i cambiamenti futuri, ma non troppo predittive senza appesantire troppo la normativa.

La strategia di affiancare al regolamento anche strumenti più flessibili come gli atti delegati potrebbe risultare vincente per garantire elasticità e certezza del diritto al tempo stesso.

In questa cornice, lo stakeholder istituzionale EPRS- Servizio Ricerche del Parlamento Europeo ha provato a verificare la bozza di regolamento alla luce di immaginifici scenari di eventi su larga scala. Un esperimento interessante.

Attacco informatico
Il test avrebbe rivelato che la legislazione non prevede disposizioni in un'eventualità di un attacco informatico su larga scala, in particolare non prevede cosa accadrebbe se l'intero sistema di documentazione, registrazione, monitoraggio, ecc. dei sistemi di IA ad alto rischio (richiesto da diversi articoli del regolamento) crollasse e i dati andassero irrimediabilmente persi in alcuni o tutti i settori.

Le principali conclusioni del test rispetto a questo scenario sono:
che l'introduzione di obblighi di stoccaggio fuori rete potrebbe essere presa in considerazio-

ne, ma richiederebbe una valutazione dal punto di vista dei costi-benefici;
che non è chiaro come altri atti legislativi dell'UE potrebbero colmare questa lacuna (con l'eccezione della direttiva NIS2 salvaguardia, creando così sinergie tra l'AI Act e la NIS2 quando si tratta di entità critiche.

Massiccia inondazione
Nel caso una massiccia inondazione dovuta all'innalzamento del livello del mare, il test considera il danno o la distruzione delle infrastrutture critiche, compresi i server che memorizzano i dati e considera che l'attuale proposta normativa non contemplerebbe soluzione a problemi eventuali di resilienza fisica.
Il test suggerisce quindi: server da immagazzinare in condizioni impermeabili/ lo stoccaggio di backup in aree che certamente non saranno colpite dall'innalzamento del livello del mare. Gli autori dello studio però concludono che questo aumenterebbe il costo dell'IA in modo significativo nell'UE, danneggiando così la competitività dell'UE nel campo.

Disordini civili per mancanza di risorse
Un alto problema identificato nel test riguarda l'aumento dei disordini civili, dovuti alla diminuzione delle risorse, della terra, del cibo e delle materie prime disponibili per la popolazione europea, e la migrazione di massa dalle zone inondate a quelle aree che sono rimaste sopra il livello del mare. In queste circostanze di emergenza, gli Stati membri potrebbero nuovamente ricorrere a sistemi di sorveglianza AI per gli spazi pubblici al fine di identificare precocemente gli scontri violenti. Questo potrebbe limitare notevolmente le libertà civili, compreso il diritto di riunirsi, il diritto alla privacy, ecc.
Lo stress-test conclude che (sulla base dell'articolo 5) la legislazione permette reazioni politiche a un'emergenza di questo tipo, ma in limiti molto stretti come nel caso delle eccezioni ai diritti fondamentali più in generale.

5. L'impianto normativo

Livelli di rischio
La proposta della Commissione Europea si radica attorno ad un impianto che divide la materia da disciplinare sulla base dei livelli di rischio derivati dalle applicazioni di Intelligenza Artificiale – e su questa base concettuale propone regole diverse per il mercato.

La gradazione dei livelli di rischio è sicuramente da apprezzare, perché permette un approccio flessibile verso diversi scenari e la natura cross-settoriale dell'IA. Tuttavia, il lavoro parlamentare del relatore S&D nella Commissione IMCO Brando Benifei è andato nella direzione di verificare puntualmente la suddivisione dei sistemi nelle categorie individuate, nonché la disciplina che ne deriva, in larga parte in un senso restrittivo per l'impresa ovvero di maggiore tutela dei cittadini.

In breve, il regolamento prevede quattro livelli di rischio.
Il rischio inaccettabile riguarda i casi in cui l'IA è considerata una minaccia alla sicurezza e ai diritti fondamentali delle persone. Tra gli esempi ci sono il credito sociale (del modello cinese), i sistemi che in modo subliminale modificano il comportamento di una persona tanto da provocare loro un danno fisico o psichico.

L'alto rischio contempla i casi in cui l'IA è usata per infrastrutture critiche come i trasporti; l'accesso all'istruzione o ad un corso professionale; componenti di sicurezza dei prodotti (per

esempio l'applicazione dell'IA nella chirurgia assistita da robot); l'occupazione e la gestione dei lavoratori (come software di selezione dei cv per le procedure di assunzione); servizi pubblici e privati essenziali; in usi che interferiscano con i diritti fondamentali; alle frontiere; in ambito giuridico.

Il rischio limitato prevede per il fornitore di IA solamente obblighi specifici di trasparenza. Per esempio, nel caso di uso di chatbot, l'utente dovrebbe essere informato che non sta interagendo con un essere umano così come dovrebbe sapere quando sta vedendo un video generato con deepfake.

Da ultimo il rischio minimo prevede invece il libero uso di applicazioni come i videogiochi abilitati dall'IA o i filtri antispam.

L'impegno del gruppo S&D è andato nella direzione di fare chiarezza su tutte le possibili applicazioni dei sistemi IA non solo a rischio inaccettabile, ma anche ad alto rischio, per

I nodi problematici
Riconoscimento biometrico e social scoring, in ambienti pubblici e privati, anche per mano delle forze dell'ordine: le forze progressiste sono disponibili a votare solo se vengono inseriti adeguati meccanismi di controllo, verifica e appello.
Assenza di riferimento all'ambiente come valore da tutelare va corretta.

Certificazioni: necessità di approfondire per quali usi di applicazioni IA la autocertificazione marchio CE da parte del produttore sia adeguata e dove invece sia necessaria una parte terza indipendente certificatrice.

Grazie al lavoro S&D, sono stati inseriti molti riferimenti ai diritti fondamentali, principi etici, alfabetizzazione digitale, gender gap, diritti dei lavoratori e tutele dalla eccessiva concentrazione nel mercato di poche compagnie big tech.

Un punto molto discusso è il compromesso sulle sandbox, ovvero quelle aree di test ove gli sviluppatori provano un nuovo programma prima di lanciarlo online. Le imprese chiedono qui un grande spazio di manovra, e dunque la possibilità nelle sandbox di non adeguarsi alla normativa del GDRP.

6. Governance, nuovi obblighi

Sul tema della governance, che sta a cuore a molti, abbiamo raccolto le istanze nate con l'esempio del GDPR e abbiamo suggerito una modifica ambiziosa, dando alla Commissione il ruolo di esecutore europeo in casi specifici che configurino violazioni diffuse a livello UE o di inazione da parte di uno Stato membro con impatto su almeno altri due Stati membri.
Nell'ambito di questo nuovo meccanismo, abbiamo dato alla Commissione il potere delle autorità di vigilanza del mercato, nonché il diritto di imporre multe, al fine di garantire che sia pienamente attrezzata per applicare in modo efficace l'AI Act.

Inoltre, stiamo lavorando con i colleghi sui poteri del Board che, in modalità diverse, in generale si pensa debbano essere rafforzati. Ci sono ancora discussioni in corso se debba essere istituito un AI Office, una agenzia nuova o si debbano solo rafforzare i poteri del board.

Poiché i sistemi ad alto rischio di IA possono influenzare la nostra salute, la sicurezza o i diritti fondamentali, concordiamo sulla necessità di dare alla proposta legislativa un meccanismo di applicazione efficace, per evitare di ottenere come risultato una tigre di carta.

Per garantire che i provider esteri siano sempre reperibili, abbiamo previsto che essi debbano avere sempre un rappresentante all'interno dell'Unione.
Gli user di AI ad alto rischio invece, dovranno assicurarsi che gli addetti alla supervisione umana siano adeguatamente qualificati e abbiano le risorse sufficienti per compiere il proprio lavoro.

A maggio a Bruxelles si è chiusa la conferenza del Garante europeo della privacy che, forte dell'esperienza del GDPR, ha evidenziato i problemi di una eccessiva decentralizzazione dell'enforcement, soprattutto per quanto riguarda i casi che toccano Big Tech e multinazionali. Noi stessi siamo stati ispirati dalle recenti proposte legislative europee come il DMA.

Non spetta al Parlamento Europeo definire chi se ne occuperà in Italia, ma stiamo lavorando però perché i Garanti della privacy siano in qualche modo coinvolti essendo le autorità al momento più preparate sul tema della gestione dei dati. D'altro canto, è vero che governare l'Intelligenza artificiale vuol dire andare ben oltre la sola protezione dei dati personali, benché questa sia fondamentale. È qualcosa di molto più amplio e complesso, che deve tenere in conto la tutela di diversi diritti fondamentali e gli interessi di tanti soggetti, pubblici e privati.