Dichiarazione Società civile sull'AI Act dell'UE - novembre 2023

L'UE ha una lunga storia di regolamentazione delle tecnologie che rappresentano un serio rischio per la sicurezza pubblica e la salute. Sia che si tratti di automobili, aerei, sicurezza alimentare, dispositivi medici o farmaci, i governi sono intervenuti per stabilire leggi a presidio della sicurezza del prodotto che assicurano un alto livello di fiducia pubblica e consentono alle aziende di ricevere regole chiare da seguire. Lo stesso vale per il settore delle infrastrutture, telecomunicazioni, elettricità o dell'acqua: senza regolamentazione, questi servizi essenziali potrebbero essere soggetti ad un uso improprio, rischiando di funzionare male. Rischi simili esistono con l'IA, che si integra sempre di più nella nostra vita quotidiana. Difatti l'IA non regolamentata potrebbe comportare a una serie di problemi di sicurezza (ad esempio, dati di addestramento distorti che portano al rifiuto di un prestito o la generazione automatizzata di contenuti su misura che facilita la manipolazione diffusa durante un'elezione), o anche rischi sistemici, tanto più possibili qualora vi sia un punto unico di fallimento a monte di una vasta gamma di applicazioni.

Questo è il punto di vista attraverso il quale considerare il dibattito attuale nell'UE sull'AI Act. **I foundation models presentano rischi significativi data la loro complessità, scala e pervasività, ed in particolare per la loro potenzialità intrinseca di formare un'infrastruttura centrale per le applicazioni successive.** Ecco perché i legislatori dell'UE hanno proposto norme da applicare direttamente ai fornitori di foundation models, comprese quelle per l'auditing indipendente, i test di sicurezza e cybersecurity, le valutazioni e mitigazioni dei rischi, e il monitoraggio e la correzione degli incidenti. Considerata l'ampia gamma e gravità dei rischi che i foundation models sollevano, queste proposte, quasi giunte a una definizione dopo due anni di dibattito, rappresentano presidi ragionevoli per garantire la sicurezza pubblica e la fiducia.

Ma la scorsa settimana, Francia e Germania, supportate dall'Italia, hanno respinto qualsiasi forma di regolamentazione vincolante e proposto che i foundation models dovrebbero essere esentati da qualsiasi obbligo normativo. Questa posizione ha ora messo in discussione l'intero AI Act dell'UE, che copre tutti i tipi di sistemi di intelligenza artificiale, dalle tecnologie biometriche ai sistemi che influenzano i nostri processi elettorali. Alcuni attori anti-regolamentari sono felici di poter sfruttare

questa opportunità per rinviare completamente la legislazione fino alle elezioni dell'anno prossimo. Chiaramente questo scenario comporterebbe il protrarsi di una disastrosa situazione di incertezza e di vuoto normativo.

Francia e Germania affermano che gli obblighi normativi sarebbero troppo onerosi per un pugno di aziende che sviluppano foundation models (Aleph Alpha e Mistral) che hanno raccolto centinaia di milioni di finanziamenti per costruire foundation models open source. **Sarebbe irresponsabile da parte dell'UE scartare l'intera regolamentazione da applicare su larga scala ai fornitori di foundation models per proteggere un paio di "campioni nazionali". Procedere in questo modo significherebbe soffocare l'innovazione nell'ecosistema dell'IA dell'UE, di cui le PMI e le startup a valle sono la grande maggioranza.** Queste aziende andranno a costituire l'IA europea, costruendo sopra i foundation models. Ma potrebbero non avere l'esperienza, la capacità o - cosa importante - l'accesso ai foundation models per rendere le loro applicazioni AI conformi all'AI Act. Pertanto non si può pretendere di far ricadere gli obblighi normativi su questi ultimi, ma occorre agire a monte. I fornitori di foundation models sono significativamente meglio posizionati per garantire output sicuri, e solo loro sono consapevoli dell'intera portata delle capacità e delle carenze dei foundation models. Pertanto, dei requisiti di conformità imposti a solo pochi attori potrebbero beneficiare migliaia di implementatori a valle, e ridurre al minimo il rischio di concentrazione nel mercato.

Per questo motivo, la DIGITAL SME Alliance, che rappresenta 45.000 PMI ICT in Europa, ha chiesto una giusta attribuzione di responsabilità nella catena del valore, quindi concentrata *in primis* sul livello dei foundation models. Se questa condizione non dovesse venire assolta, sarà estremamente difficile per le PMI rispettare i requisiti dell'AI Act. Significherebbe che le PMI potrebbero smettere di utilizzare del tutto i foundation models, o potrebbero altrimenti essere esposte in modo sproporzionato agli oneri di conformità e alle relative responsabilità.

Le posizioni di Francia e Germania sui foundation models si basano su un mito diffuso ma privo di prove che la regolamentazione sia in contrasto con l'innovazione. Tuttavia, la ricerca sugli impatti della regolamentazione in settori diversi mostra molti esempi di regolamentazione che permette una maggiore innovazione, concorrenza di mercato e adozione di determinate tecnologie nella società. La nostra ricerca sulle opinioni pubbliche mostra che le persone si aspettano che i prodotti dell'IA siano sicuri e desiderano che questi prodotti vengano regolamentati. L'Ordine Esecutivo degli Stati Uniti sull'IA, la Dichiarazione di Bletchley

e gli impegni del G7 riconoscono tutti i rischi dei foundation models avanzati e hanno delineato *best practices* volontarie per l'industria. Tali iniziative riconoscono esplicitamente i rischi che possono sorgere e diffondersi a partire dai foundation models. Sebbene queste proposte siano ben accette, una protezione significativa può essere fornita solo attraverso una regolamentazione rigorosa. Infatti, già in passato, tali politiche non vincolanti sono sostanzialmente fallite, ad esempio quando le grandi aziende tecnologiche hanno intrapreso impegni volontari sui discorsi di odio, senza di certo ottenere i risultati sperati.

L'UE ha l'opportunità di creare lo standard globale per un ecosistema di intelligenza artificiale basato sulla sicurezza e sulla fiducia. Lo ha fatto in altri settori in passato senza sacrificare il suo vantaggio economico, come nell'aviazione civile, dove la regolamentazione basata sulla sicurezza ha ridotto il rischio di mortalità dell'83% tra il 1998 e il 2008, registrando nel contempo un aumento annuo del 5% passeggeri volanti per chilometro. L'UE ha creato un ecosistema simile per la cybersicurezza, automobili, servizi finanziari e clima, tutti successi ottenuti sulla base di una regolamentazione rigorosa.

La proposta della Presidenza spagnola per un approccio multilivello c.d. “a gradini” offre un compromesso equo, garantendo la conformità e sicurezza dei foundation models su larga scala, al contempo alleviando il carico per gli attori economici dell'UE che stanno sviluppando foundation models più piccoli, fino a quando i loro foundation models non diventano altrettanto impattanti. Tutti i foundation models che, secondo una certa probabilità, possono impattare sulla società, dovrebbero essere sottoposti a audit indipendenti, gestione dei rischi e rigorosa supervisione. Per limitare gli oneri che ne possono derivare, conviene stabilire una soglia oltre la quale entrano in vigore regole più stringenti.

La posta in gioco non potrebbe essere più alta questa settimana. L'Europa ha un'opportunità rara di stabilire regole, istituzioni e processi armonizzati per proteggere gli interessi delle decine di migliaia di aziende che utilizzeranno foundation models e per proteggere i milioni di persone che saranno colpite dai loro potenziali danni. Questa opportunità non si presenterà ancora per molto tempo. Gli ultimi anni hanno dimostrato come l'IA non regolamentata possa causare danni su vasta scala alla società, oltre che generare disparità economica: questa è l'occasione dell'Europa per stabilire chiare obbligazioni regolamentari al fine di creare un campo di gioco più equo.