10/05/2021
Sito Web

ai4business.it

Regolamento europeo sull'AI: il punto sui sistemi "ad alto rischio"

LINK: https://www.ai4business.it/intelligenza-artificiale/regolamento-europeo-sullai-il-focus-sui-sistemi-ad-alto-rischio/

I sistemi di intelligenza artificiale ad alto rischio costituiscono il principale oggetto della proposta di Regolamento recentemente pubblicata dalla Commissione Europea. Requisiti obbligatori, test di conformità e monitoraggio post-vendita sono solo alcuni degli obblighi previsti a carico dei fornitori di tale tecnologia Alessandro Vasta Partner, Tonucci & Partners Nicola Sandon Associate, Tonucci & Partners Regolamento europeo alto rischio HOMEINTELLIGENZA ARTIFICIALERegolamento europeo sull'AI: il punto sui sistemi "ad alto rischio" 10 Maggio 2021 Intelligenza Artificiale Il 21 aprile scorso la Commissione Europea ha orgogliosamente presentato al mondo la prima bozza del c.d. "Artificial Intelligence Act", ovverosia la propria proposta di regolamentazione dei sistemi basati sull'intelligenza artificiale armonizzata a livello europeo. La bozza è stata concepita sotto forma di Regolamento, di modo da consentire in futuro la diretta applicazione in tutti gli Stati Membri e contestualmente evitare quella frammentazione normativa che gli stakeholder temono, a causa della potenziale contrazione degli investimenti legata all'incertezza del diritto e al costo della compliance. L'A.I. Act si fonda su quell'approccio basato sul rischio che negli ultimi anni appare caro al legislatore europeo (esempio ne è anche il GDPR), prevedendo oneri e gradi di tutele crescenti all'aumentare del livello di rischio per la sicurezza, la salute e i diritti fondamentali dei cittadini europei posto dalle singole tipologie di software. Nello specifico, il regolamento individua espressamente tre diversi livelli di rischio: inaccettabile, alto e limitato. A questi deve aggiungersi un quarto livello, quello "minimo", che, non raggiungendo la soglia di rilevanza ai sensi della bozza della Commissione, non viene ricompreso nel suo ambito di applicazione. Mentre i sistemi di AI che presentino un livello inaccettabile di rischio, in quanto in contrasto con gli stessi valori fondanti dell'Unione, sono tout court vietati (pur con la previsione di una serie di eccezioni che mette in dubbio l'assolutezza di tale divieto), e per i sistemi che presentino un rischio limitato (quali chatbot e deepfake) il regolamento si limita a prevedere limitati obblighi di trasparenza, il vero fulcro normativo della normativa europea sull'intelligenza artificiale sono i sistemi "ad alto rischio", disciplinati nel Titolo III del regolamento. Ma quali sono questi sistemi ad alto rischio, e, soprattutto, quali oneri prevede il legislatore in capo ai fornitori di tali sistemi? Indice degli argomenti: 1 Regolamento europeo: elenco e criteri di classificazione dei sistemi ad alto rischio 2 Regolamento europeo: requisiti obbligatori per i sistemi ad alto rischio 3 Valutazione di conformità, marchio CE e registrazione 4 Gli obblighi di monitoraggio post-commercializzazione 5 Conclusioni Regolamento europeo: elenco e criteri di classificazione dei sistemi ad alto rischio È importante sottolineare sin da subito che per il Regolamento europeo esistono due diverse tipologie di sistemi ad alto rischio, i fornitori dei quali sono soggetti ai medesimi obblighi, fatta eccezione per alcune distinzioni di non scarsa

rilevanza nell'ambito della valutazione di conformità che vedremo meglio nei paragrafi successivi. Da un lato troviamo i sistemi destinati ad essere utilizzati come componenti di sicurezza in un prodotto, o che siano essi stessi un prodotto, destinato ad essere sottoposto a una valutazione di conformità da parte di soggetti terzi ai sensi della normativa europea ad essi applicabile (esplicitata dettagliatamente nell'Allegato II alla bozza di regolamento). Si pensi a giocattoli, dispositivi medici, aeromobili, ecc. Dall'altro troviamo invece i sistemi di AI autonomi (c.d. "stand-alone") che, in considerazione dei rischi posti per la sicurezza o la salute, o dell'impatto negativo che essi possono comportare sui diritti fondamentali delle persone fisiche, vengono classificati come ad alto rischio dalla stessa Commissione. Il giudizio dell'autorità europea deve fondarsi su una serie di fattori, individuati espressamente dalla normativa, tra i quali rientrano lo scopo del sistema, la probabile estensione dell'applicazione dello stesso, il numero di persone interessate, l'eventuale presenza di notizie in merito a danni già causati da sistemi simili, la correlazione tra l'impiego del sistema e i possibili danni nonché la reversibilità degli stessi, la misura in cui la legislazione vigente preveda misure efficaci per misure efficaci per prevenire o minimizzare sostanzialmente tali rischi. Tali sistemi sono elencati nell'Allegato III alla proposta di regolamento, che al momento include i sistemi destinati a trovare applicazione nell'ambito dei seguenti settori: identificazione biometrica e categorizzazione delle persone fisiche; gestione di infrastrutture critiche (quali trasporti, fornitura di acqua, gas e elettricità) istruzione (accesso e valutazione delle performance) contesto lavorativo e occupazionale, inclusa la fase di selezione e assunzione del personale accesso a servizi essenziali, pubblici e privati (inclusa la valutazione del merito creditizio) sicurezza gestione dei flussi migratori e delle richieste di asilo, sicurezza dei confini amministrazione della giustizia Per garantire la necessaria flessibilità - visto il contesto applicativo che vede un'evoluzione tecnologica rapida e continua - l'Allegato III potrà essere periodicamente soggetto a revisione da parte della Commissione, mediante appositi atti delegati. regolamento europeo alto rischio Regolamento europeo: requisiti obbligatori per i sistemi ad alto rischio Identificati a grandi linee i sistemi di AI ad alto rischio, analizziamo gli obblighi imposti dal Regolamento europeo nei confronti degli sviluppatori di tali tecnologie. La cornice normativa prevista dal Regolamento in tale ambito si presenta come piuttosto complessa e onerosa e si rivolge a tutti i soggetti coinvolti - seppur a diverso titolo - nello sviluppo e successiva commercializzazione dei sistemi di AI ad alto rischio. Sebbene la maggior parte degli obblighi previsti dal Regolamento siano diretti ai fornitori (i "providers"), ovverosia il soggetto che sviluppa un sistema di AI o dispone di un sistema sviluppato con l'intenzione di immetterlo sul mercato o metterlo in servizio sotto il proprio nome o marchio, anche a titolo gratuito, obblighi specifici sono previsti anche a carico di altre figure, quali utenti, importatori e distributori, il cui ruolo è delineato dal Regolamento stesso. Trattandosi in linea di massima di previsioni più circoscritte, non ci occuperemo di tali obblighi specifici in questo contesto, mentre daremo ampio spazio alla disciplina prevista a carico dei fornitori. L'A.I. Act prevede in primo luogo una serie di

"requisiti obbligatori" cui i fornitori devono attenersi sin dalla fase di progettazione e sviluppo e la conformità ai quali dovrà essere attentamente valutata prima della commercializzazione del sistema stesso. In particolare, si tratta di: sistema di gestione del rischio: il fornitore è tenuto a implementare, in maniera documentata, un sistema che consenta di identificare e analizzare i possibili rischi derivanti dal suo impiego, farne una stima e adottare idonee misure. Il sistema deve essere mantenuto durante l'intero ciclo di vita del software ad alto rischio; data governance e qualità dei dataset: i dataset utilizzati dal fornitore in fase di addestramento, validazione e test devono essere gestiti in maniera appropriata, e rispondere ad elevati requisiti in materia di pertinenza, rappresentatività, correttezza e completezza, onde limitare la possibilità di incorrere in bias dannosi e discriminatori; documentazione tecnica: i fornitori devono redigere e mantenere una documentazione tecnica completa e aggiornata che sia in grado di dimostrare il rispetto della normativa; tracciabilità: il fornitore deve garantire la verificabilità e tracciabilità delle decisioni e dei processi posti in essere dai sistemi ad alto rischio prevedendo meccanismi di registrazione automatica dei log, al fine di attenuare l'effetto "black-box" e la conseguente opacità del funzionamento del software; trasparenza: la trasparenza del sistema nei confronti degli utenti[1] deve essere garantita mediante predisposizione di istruzioni per l'uso chiare, concise e comprensibili, che contengano almeno una serie di elementi specificamente individuati dal legislatore; supervisione umana: i fornitori devono porre in essere misure appropriate a consentire un'effettiva supervisione umana sul funzionamento dei sistemi ad alto rischio[2]; accuratezza, robustezza e sicurezza informatica: i sistemi ad alto rischio devono essere progettati e sviluppati in modo da garantire un elevato livello di accuratezza, robustezza e sicurezza informatica durante l'intero ciclo di vita del software. WHITEPAPER Roadmap verso la Smart Logistic - Le 4 tecnologie per migliorare efficienza e sicurezza Intelligenza Artificiale IoT Scopri di più! Scarica il Whitepaper Tali requisiti costituiscono il sostrato normativo minimo che deve guidare i fornitori nello sviluppo dei sistemi ad alto rischio, favorendo la realizzazione di tecnologie in linea con i valori europei. L'importanza dei requisiti obbligatori risulta ancor più evidente se andiamo a esaminare il profilo sanzionatorio: la non conformità agli stessi è infatti punibile con l'applicazione delle sanzioni più elevate che siano previste dalla bozza di Regolamento, pari nel massimo a 30 milioni di euro o, per le aziende, al 6% del fatturato globale annuo dell'anno precedente. regolamento europeo alto rischio Valutazione di conformità, marchio CE e registrazione Prima di commercializzare un sistema di AI ad alto rischio, i fornitori sono tenuti a porre in essere un processo di verifica della conformità ex ante del sistema AI ai requisiti descritti al paragrafo precedente. Il Regolamento prevede diverse modalità di svolgimento di tale verifica, a seconda della tipologia di sistema. La distinzione più rilevante è la seguente: i sistemi destinati a essere utilizzati come componenti di sicurezza in un prodotto, o che siano essi stessi un prodotto ai sensi della normativa europea rilevante, saranno soggetti unicamente al processo di valutazione di conformità da parte di soggetti terzi previsto da tale normativa. L'ente che condurrà la verifica dovrà pertanto

tenere in considerazione anche la compliance del sistema rispetto alle previsioni dell'A.I. Act; i sistemi c.d. stand-alone potranno invece essere oggetto di un processo interno di verifica della conformità, eseguito direttamente dal fornitore, seguendo la (sintetica) procedura descritta all'Allegato VI. Fanno eccezione i sistemi operanti ai fini dell'identificazione biometrica e categorizzazione delle persone fisiche, per i quali in alcuni casi è previsto l'intervento di terze parti indipendenti e la conduzione di un processo di verifica ben più oneroso. Al termine della procedura di valutazione, i fornitori di servizi stand-alone sono inoltre tenuti a: redigere una dichiarazione di conformità Europea, dai contenuti predeterminati dalla Commissione in apposito allegato, che avrà validità di 10 anni dalla commercializzazione del sistema e, in caso di richiesta, dovrà essere fornita alle autorità competenti; apporre il marchio di conformità CE al sistema (o alla confezione dello stesso), in modo che esso risulti visibile, leggibile e indelebile; procedere alla registrazione del sistema all'intero di un apposito elenco pubblico gestito dalla Commissione. Gli obblighi di monitoraggio post-commercializzazione Gli obblighi previsti dal Regolamento europeo in materia di sistemi ad alto rischio non terminano però con la commercializzazione del sistema: la compliance viene infatti vista come un processo continuo, non un adempimento una tantum, e prevede dunque nella pratica la necessità di procedere a regolari aggiornamenti e revisioni, soprattutto quando si ha a che fare con sistemi in grado di apprendere in maniera autonoma, particolarmente dinamici e potenzialmente soggetti a continue trasformazioni. Una volta che un sistema ad alto rischio è stato messo sul mercato, i fornitori devono implementare, in maniera documentabile, un sistema di monitoraggio, "proporzionato" alla finalità e alle caratteristiche del sistema, che sia in grado di consentire la raccolta e l'analisi dei dati di utilizzo derivanti dal sistema e, se del caso, di intervenire con misure correttive adeguate, garantendo il rispetto della normativa. Il sistema di monitoraggio dovrà peraltro essere oggetto di puntuale pianificazione preventiva mediante la redazione di un apposito piano, che dovrà essere incluso nella documentazione tecnica relativa al sistema ad alto rischio. Sarà interessante vedere come tale obbligo si coordinerà con quanto previsto dal Regolamento (UE) 2016/679 in materia di protezione dei dati, la cui applicazione viene fatta espressamente salva dalla bozza di regolamento. I fornitori sono poi tenuti a notificare i casi di gravi malfunzionamenti o incidenti alle autorità dello Stato Membro ove questi si siano verificati, non appena sia possibile identificare un nesso tra il funzionamento del sistema di AI e l'incidente o malfunzionamento e comunque non più tardi di 15 giorni dopo che il fornitore abbia avuto conoscenza dello stesso. In considerazione della "perpetuità" che caratterizza il processo di conformità, in aggiunta a quanto sopra, secondo il Regolamento europeo i fornitori di sistemi di AI ad alto rischio sono tenuti ad implementare un idoneo sistema di gestione della qualità, mediante policy, istruzioni o procedure scritte che siano in grado di garantire la conformità dei sistemi alla normativa e di minimizzare i rischi per gli utenti e le persone interessate. Tale "quality management system" deve coprire l'intero ciclo di vita del sistema ad alto rischio, a partire dalla fase di progettazione e sviluppo a

quella di monitoraggio successiva alla commercializzazione. Conclusioni L'A.I. Act si trova all'inizio del complesso procedimento legislativo europeo, potrà senz'altro essere soggetto a modifiche e impiegherà anni per essere concretamente applicabile. Ciononostante, esso ha le potenzialità per condizionare sin da ora il futuro sviluppo dei sistemi di AI, offrendo spunti fondamentali per lo sviluppo di best practice e linee guida e ponendosi come modello per l'elaborazione di ulteriori normative. Pur apprezzando lo spirito di iniziativa europea e la carica innovativa della proposta della Commissione, non si può non riconoscere come la disciplina prevista dal legislatore europeo in materia di sistemi di AI ad alto rischio ponga in capo agli sviluppatori e ai fornitori degli stessi variegati e rilevanti obblighi in materia di conformità. Volendo raggruppare gli oneri in macro-gruppi, si mettono in evidenza le seguenti voci: produzione documentale: dalle procedure in materia di risk management, alla documentazione tecnica, dalle istruzioni d'uso alle policy in tema di gestione della qualità, sono molteplici i documenti che dovranno essere predisposti ad hoc dai fornitori. Documenti che dovranno essere preparati con cura e spesso con il supporto di consulenti esterni, in quanto in taluni casi rappresenteranno la miglior chance dar prova alle autorità del corretto adempimento degli obblighi previsti dalla bozza di regolamento (nel rispetto del proverbio, non propriamente innovativo, che recita "scripta manent"...); processo di sviluppo: il Regolamento ha un forte impatto anche sugli accorgimenti da adottare nella fase di sviluppo dei sistemi di AI, richiedendo un comportamento attivo e consapevole del fornitore sin dalle prime fasi di progettazione La scelta e la composizione dei dataset impiegati, l'introduzione di sistemi di log precisi e invasivi e la garanzia dell'intervento umano sono solo alcuni dei fattori che possono concretamente comportare oneri aggiuntivi di non scarsa importanza a carico degli sviluppatori; conformità a ulteriore normativa europea o nazionale: collocandosi la proposta di Regolamento in un contesto normativo ben più ampio, gli oneri relativi alla compliance risultano ancor più ragguardevoli alla luce del necessario coordinamento dell'A.I. Act con l'ulteriore normativa prevista a livello unionale o dei singoli Stati Membri che possa, anche solo incidentalmente, applicarsi a un sistema di AI. Responsabilità civile, protezione dei dati personali, proprietà intellettuale, tutela dei consumatori sono solo alcuni dei (fondamentali) temi di cui i fornitori dovranno tenere conto nel momento in cui intendano commercializzare un sistema di AI sul mercato europeo. Altro tema da tenere in debita considerazione è l'impatto della modifica dell'allegato al Regolamento che contiene l'elenco dei sistemi di AI. Se da un lato questo meccanismo risultava indispensabile per non rischiare di rendere il testo normativo obsoleto ancor prima della sua entrata in vigore, dall'altro esso è in grado di porre non pochi problemi agli sviluppatori, che potrebbero trovarsi a dover recuperare in una fase successiva alla progettazione tutta una serie di adempimenti originariamente non previsti a loro carico o ad aver investito nel processo di conformità fondi e tempo per poi vedere il sistema espunto dalla lista. Non è poi ancora del tutto chiaro come si coordinerà l'imponente impianto regolatorio previsto dal Regolamento con le eventuali diverse e ulteriori

normative che potrebbero essere sviluppate nei prossimi anni da parte degli altri giganti che competono con l'U.E. nella corsa allo sviluppo di sistemi di AI, quali gli Stati Uniti e la Cina: sebbene l'A.I. Act presenti una forte carica espansiva, e sia destinato - per lo meno nelle intenzioni della Commissione - a trovare applicazione anche ai fornitori che abbiano il proprio stabilimento al di fuori del territorio dell'Unione, non è assolutamente detto che gli altri player accettino di buon grado di veder limitata (o quanto meno imbrigliata) la carica innovativa che porta con sé lo sviluppo di sistemi di AI. dalla visione europea. L'Unione Europea con la propria bozza di regolamento sull'AI. ha tracciato un solco profondo nel proprio tessuto normativo, affermando con forza che non esiste innovazione senza tutela dei diritti fondamentali. Ad oggi, tuttavia, è impossibile stabilire (o anche solo tentare di prevedere) se i fattori sopra descritti fungeranno da volano per lo sviluppo di una AI umano-centrica ed etica o contribuiranno a disincentivare il ricorso massivo a tale tecnologia e la fuga di aziende e investitori dall'Unione. Note Con "utente" si intende non la persona fisica che sia oggetto dell'elaborazione del sistema, bensì del soggetto che utilizzi un sistema di I.A. sotto la propria autorità, a condizione che l'utilizzo non avvenga nell'ambito di un'attività personale non professionale. Ad esempio, mediante la previsione della possibilità di bypassare l'output ottenuto o bloccare il funzionamento del sistema.