La centralità dei requisiti normativi di *cybersecurity* dei sistemi di Intelligenza Artificiale

di Flavia Bavetta

L'utilizzo massivo di tecnologie che si servono di sistemi di Intelligenza Artificiale (IA) per lo svolgimento di molte funzioni pubbliche o per l'erogazione di numerosi servizi offerti da soggetti privati rende centrale la tematica relativa all'applicazione e alla corretta implementazione delle misure di sicurezza cibernetica. In particolare, vivendo in società altamente digitalizzate e costantemente interconnesse è necessario riflettere come ogni dispositivo collegato alle reti sia un potenziale canale per l'ingresso nei sistemi di attori pubblici e privati di minacce informatiche (ad esempio, attacchi *ransomware*, *Distributed Denial of Services,* etc.), le quali possono determinare non solo l'interruzione dei servizi erogati, ma anche l'impossibilità di garantire alcuni diritti fondamentali come quelli relativi alla riservatezza e alla protezione dei dati personali.

Pertanto, riuscire ad assicurare alti livelli di impenetrabilità dei sistemi utilizzati, nonché dei dati – anche personali – in essi contenuti e la loro resilienza a possibili attacchi o a malfunzionamenti risulta essere cruciale. Nello specifico, la raccolta e l'utilizzo di risorse, processi e strutture volte alla protezione del cyberspazio e dei sistemi che vi gravitano è senza dubbio un elemento essenziale per costruire e rafforzare la fiducia degli utenti, dei cittadini e degli individui nell'ecosistema digitale, nonché per assicurare la protezione dei sopracitati diritti.

Sulla base di queste premesse, guardando allo sviluppo delle politiche pubbliche dell'UE è innegabile come l'attenzione alla tematica della *cybersecurity* anche applicata all'IA da parte delle autorità competenti sia cresciuta fortemente negli ultimi anni. Infatti, l'interesse del Consiglio Europeo e della Commissione Europea era già chiaro nel 2020 grazie alla definizione della strategia dell'UE per la *cybersecurity*, volta a creare un *framework* omnicomprensivo che – seppur indirettamente – si applica ai sistemi di IA. Nello specifico, nel dicembre 2020 la Commissione europea e il Servizio Europeo per l'Azione Esterna (SEAE) hanno presentato una nuova strategia dell'UE per la cybersicurezza con l'obiettivo di rafforzare la resilienza dell'Europa a fronte delle minacce informatiche e garantire che tutti i cittadini e le imprese possano beneficiare pienamente di servizi e strumenti digitali affidabili e attendibili. La nuova strategia include proposte concrete per l'introduzione di strumenti normativi, strategici e di investimento. Inoltre,

più di recente, e in particolare il 22 marzo 2021, il Consiglio ha adottato le sue conclusioni sulla strategia in materia di cybersicurezza, sottolineando che la *cybersecurity* è essenziale per costruire un'Europa resiliente, verde e digitale.

Pertanto, è in tale contesto che sono recentemente nate specifiche iniziative legislative e di *policy* relative all'utilizzo dell'IA e all'applicazione di misure di sicurezza cibernetica. Ad esempio, è degno di nota il lavoro dell'Agenzia Europea per la Difesa (EDA) che ha sviluppato una tassonomia completa per l'IA nel campo della difesa. In aggiunta a quanto sopra, identificando il potenziale impatto dell'IA sulla sicurezza delle telecomunicazioni, l'Istituto Europeo per le Norme di Telecomunicazione (ETSI) ha istituito un gruppo per individuare le specifiche industriali da implementare in materia di cybersicurezza sui sistemi di IA applicati ai sistemi di telecomunicazione (ISG SAI). L'obiettivo dell'ISG SAI è quello di creare *standard* per preservare e migliorare la sicurezza delle nuove tecnologie IA. Inoltre, il Centro Comune di Ricerca (CCR) ha istituito e promosso l'iniziativa AI Watch al fine di monitorare lo sviluppo, l'adozione e l'impatto dell'IA e promuovere la ricerca nel campo della *cybersecurity*.

Da un punto di vista strettamente normativo, essendo i dati personali e le informazioni elementi essenziali per il funzionamento di tecnologie che utilizzano sistemi di IA, è necessario comprendere come il Regolamento (UE) 2016/679 (GDPR o Regolamento) affronti la tematica relativa all'applicazione di misure di cybersicurezza. Nello specifico, una delle principali novità apportate dal GDPR è proprio il ruolo attribuito alla sicurezza cibernetica nel trattamento di dati personali. Si tratta, infatti, di un cambiamento quasi concettuale rispetto al passato, in quanto precedentemente la *cybersecurity* era più legata a disposizioni tecnico-organizzative. Con il Regolamento la sicurezza cibernetica dei dati personali raccolti diviene un prerequisito. Pertanto, la sicurezza delle informazioni non è più considerata un'opzione ma diviene una necessità. Di questo avviso, è ad esempio il dettato dell'articolo 32 del Regolamento, il quale richiede l'implementazione di misure graduate in base al rischio e alla gravità per i diritti e le libertà degli interessati. Pertanto, l'*asset* da proteggere non è più solo il dato personale in sé, ma più in generale il corretto esercizio dei diritti e delle libertà degli interessati.

In aggiunta a quanto sopra, all'interno del *framework* normativo e di *public policy* sopra-delineato non può non menzionarsi la recente "*Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza Artificiale (legge sull'Intelligenza Artificiale) e modifica alcuni atti legislativi dell'Unione*" (Proposta di Regolamento o Proposta), la quale è stata accolta come un passo fondamentale per il "futuro digitale dell'Europa", nonché come strumento di garanzia dei diritti fondamentali dei cittadini nell'ambito dell'utilizzo di tali nuovi tecnologie. Nello specifico, secondo quanto dichiarato nella Relazione, la Proposta mira a sviluppare un ecosistema di fiducia proponendo un quadro giuridico per un'IA affidabile, basato sui valori e sui diritti fondamentali dell'UE.

Tuttavia, nonostante i chiari obiettivi preposti, sussistono ancora diversi dubbi sulla capacità della Proposta di Regolamento di fornire un quadro giuridico chiaro che miri a garantire non solo gli obiettivi

del mercato europeo, ma altresì la protezione dei valori europei, compresa una valutazione delle minacce legate alla sicurezza informatica. Infatti, la scelta della Commissione Europea di un approccio *top-down* e *risk-based*, attraverso il quale le soglie di rischio sono individuate *ex-ante* direttamente dal legislatore, lascia meno spazio ad una valutazione *ex post* da parte degli operatori che, di conseguenza, sono tenuti a rispettare solo le soglie identificate dalla Proposta di Regolamento. Inoltre, questo approccio comporta la totale esclusione di intere categorie di sistemi di IA, come quelli considerati a basso rischio, determinando un significativo vuoto normativo.

Tale problematica investe, altresì, i requisiti di sicurezza cibernetica. In particolare nel Considerando 51 il legislatore chiarisce che "*la cibersicurezza svolge un ruolo cruciale nel garantire che i sistemi di IA siano resilienti ai tentativi compiuti da terzi con intenzioni malevole che, sfruttando le vulnerabilità del sistema, mirano ad alterarne l'uso, il comportamento, le prestazioni o a comprometterne le proprietà di sicurezza*". Inoltre, dato che gli attacchi informatici possono far leva sulle risorse specifiche dell'IA, o sfruttare le vulnerabilità delle risorse digitali di tali sistemi o dell'infrastruttura sottostante, viene indicato come sia opportuno che i fornitori dei sistemi di IA ad alto rischio adottino misure adeguate, anche tenendo debitamente conto dell'infrastruttura sottostante. Pertanto, come risulta chiaro dalla lettera della norma, obblighi specifici di implementazione di misure di sicurezza cibernetica vengono imposti solo in relazione a quei sistemi che, secondo la Proposta di Regolamento, presentano un alto rischio. Coerentemente il Considerando 43 prevede espressamente che "*tali requisiti dovrebbero applicarsi ai sistemi di IA ad alto rischio per quanto concerne la qualità dei set di dati utilizzati, la documentazione tecnica e la conservazione delle registrazioni, la trasparenza e la fornitura di informazioni agli utenti, la sorveglianza umana e la robustezza, l'accuratezza e la cibersicurezza*".

In aggiunta a tale restrizione applicativa, deve inoltre notarsi come il legislatore nel corpo normativo della Proposta di Regolamento si limiti a dettare alcuni macro-obiettivi di sicurezza, lasciando ampio spazio all'interprete sulla modalità per raggiungerli. Infatti, l'articolo 15[1] richiede la realizzazione di meri propositi, quali ad esempio la garanzia di un "*adeguato livello di accuratezza, robustezza e cibersicurezza*", nonché l'applicazione di "*soluzioni tecniche di ridondanza, che possono includere piani di backup o fail-safe*". Pertanto, la suddetta disposizione non solo ha un ambito applicativo ristretto, ma contiene meri obiettivi di sicurezza, concedendo un'ampia discrezionalità interpretativa ed applicativa in capo a soggetti che solitamente svolgono funzioni di natura prettamente tecnica.

[1] Art. 15 "i sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da conseguire, alla luce della loro finalità prevista, un adeguato livello di accuratezza, robustezza e cibersicurezza e da operare in modo coerente con tali aspetti durante tutto il loro ciclo di vita. […] I sistemi di IA ad alto rischio sono resilienti per quanto riguarda errori, guasti o incongruenze che possono verificarsi all'interno del sistema o nell'ambiente in cui esso opera, in particolare a causa della loro interazione con persone fisiche o altri sistemi. La robustezza dei sistemi di IA ad alto rischio può essere conseguita mediante soluzioni tecniche di ridondanza, che possono includere piani di backup o fail-safe. I sistemi di IA ad alto rischio che proseguono il loro apprendimento dopo essere stati immessi sul mercato o messi in servizio sono sviluppati in modo tale da garantire che gli output potenzialmente distorti a causa dell'utilizzo di output come input per operazioni future ("circuiti di feedback", feedback loops) siano oggetto di adeguate misure di attenuazione. I sistemi di IA ad alto rischio sono resilienti ai tentativi di terzi non autorizzati di modificarne l'uso o le prestazioni sfruttando le vulnerabilità del sistema. Le soluzioni tecniche volte a garantire la cibersicurezza dei sistemi di IA ad alto rischio sono adeguate alle circostanze e ai rischi pertinenti".

In tale contesto, considerato il chiaro vuoto normativo e la centralità che deve essere riconosciuta alla chiara individuazione dei requisiti normativi di *cybersecurity*, è auspicabile che il Regolamento nella sua versione definitiva sani tale lacuna. Infatti, è doveroso ricordare come il diritto sia l'unica risorsa capace di mettere la tecnica al servizio dell'uomo, della sua libertà e della garanzia dei suoi diritti fondamentali. In particolare, nel contesto della società digitale in cui ciascun oggetto può rappresentare il canale d'ingresso di potenziali attacchi informatici e in cui, quindi, le fonti di rischio si moltiplicano a dismisura, è indispensabile fare della protezione dei dati, dei sistemi e delle infrastrutture l'obiettivo prioritario delle politiche pubbliche, dato che da questo dipende la tutela della persona e in ultima istanza dei suoi diritti fondamentali.