PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 28 - numero 6031 di Mercoledì 04 marzo 2026

Linee guida per rispettare la legge sull'uso dell'intelligenza artificiale

ETSI ha reso disponibili le norme ETSI EN 304 223 (2025-12) e TR 104 159 (2026-01) che definiscono requisiti di cybersecurity per modelli e sistemi AI e forniscono indicazioni per prevenire danni derivanti dall'uso di Generative AI.

Il 15 gennaio 2026 ETSI- European Telecommunication Standard istitute, uno degli organismi europei abilitato ad emettere normative, con pieno valore in tutta l'Unione Europea, ha annunciato la pubblicazione di una nuova norma, ETSI EN 304 223, che illustra i requisiti di base per la sicurezza informatica di modelli di intelligenza artificiale, anche generativa. Questo documento è basato su un rapporto tecnico, che illustriamo di seguito, e rappresenta il primo documento normativo europeo applicabile alla sicurezza informatica di applicativi di intelligenza artificiale.

Il documento è stato esaminato attentamente dagli esperti di settore di tutta Europa, che lo hanno approvato senza esitazioni.

Il documento permette di mettere a punto un quadro di riferimento, che protegge i sistemi di intelligenza artificiale dalle minacce informatiche, che ogni giorno diventano più incisive e più articolate. Questa norma garantisce una protezione avanzata, basata sul ciclo di vita del prodotto, indicando tutt'una serie di requisiti di base per la sicurezza di questi applicativi.

La norma prende buona nota del fatto che la protezione di applicativi di intelligenza artificiale rappresenta una sfida informatica ben diversa da quella presentata da software di tipo tradizionale. I nuovi rischi, che bisogna imparare a fronteggiare, riguardano l'avvelenamento dei dati, il camuffamento dei dati, nonché altre vulnerabilità associate a complessi sistemi di gestione dei dati.

Questa norma definisce 13 principi e requisiti, articolati in cinque fasi: progettazione sicura, sviluppo sicuro, utilizzo sicuro, manutenzione sicura e messa in sicurezza dell'applicativo al termine della vita utile.

La collaborazione con esperti di vario settore ha messo in evidenza la necessità, debitamente rispettata, di garantire la compatibilità di questa norma con altre norme esistenti; ci auguriamo che questa norma verrà utilizzata anche in fase di acquisto e fornitura di applicativi specifici, inserendola come prezioso riferimento nei capitolati di appalto.

Passiamo ora ad esaminare rapidamente il rapporto tecnico ETSI TR 104 159, il cui titolo già spiega molto: *Securing Artificial Intelligence (SAI); Understanding and Preventing Harm from Generative AI.*

Per dare un'idea della completezza e dell'articolazione di questo documento, segnaliamo che in esso vengono analizzati anche i documenti elaborati in altri paesi, sullo stesso tema, come ad esempio l'Australia, il Brasile, il Canada, la Cina, l'India, il Giappone, la Corea del Sud, il Regno Unito e gli Stati Uniti d'America.

L'esame attento di quanto fatto in altri paesi ha permesso agli sviluppatori di cogliere il meglio dei documenti già disponibili ed assemblare un nuovo documento, che permette di dare una risposta più che soddisfacente e legalmente corretta (principio del rispetto della regola d'arte), prevista esplicitamente dal regolamento europeo 2024 / 1686 sulla intelligenza artificiale.

Il documento analizza in particolare un aspetto, sul quale la magistratura inquirente e giudicante di vari paesi già si è mossa, vale a dire l'impatto nell'intelligenza artificiale generativa sui diritti di proprietà intellettuale.

Il documento inoltre analizza tutti gli utilizzi illeciti di questi applicativi, come la creazione di immagini parlanti e via dicendo.

Ad oggi, i due documenti sono disponibili solo in lingua inglese, ma ci auguriamo che quanto prima UNI provveda a tradurli in italiano, in modo da metterli a disposizione anche delle piccole e medie imprese, che sempre più spesso, secondo dati statistici aggiornati, fanno ricorso ad applicativi di intelligenza artificiale

ETSI EN 304 223 (2025-12) EUROPEAN STANDARD Securing Artificial Intelligence (SAI); Baseline Cyber Security Requirements for AI Models and Systems (pdf)

ETSI TR 104 159 (2026 -01) TECHNICAL REPORT Securing Artificial Intelligence (SAI); Understanding and Preventing Harm from Generative AI (pdf)

Adalberto Biasiotti