PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 28 - numero 6097 di Mercoledì 10 giugno 2026

Una norma per la sicurezza degli applicativi di intelligenza artificiale

La nuova norma ETSI EN 304 223 definisce requisiti e linee guida per valutare e garantire la sicurezza dei sistemi di intelligenza artificiale lungo tutto il loro ciclo di vita: un riferimento essenziale per sviluppatori, utilizzatori e committenti.

Ora che anche il Papa si è reso conto di quanto gli applicativi di intelligenza artificiale possano essere potenzialmente utili e potenzialmente pericolosi per la società civile, assume una rilevanza significativa la disponibilità di una norma, che stabilisce la conformità alla regola d'arte, che offre linee guida per la valutazione della sicurezza degli applicativi di intelligenza artificiale, sia in fase di progetto, sia in fase di utilizzo.

Il codice della norma è il seguente: ETSI EN 304 223 V2.1.1 (2025-12) -Securing Artificial Intelligence (SAI); Baseline Cyber Security Requirements for AI Models and Systems.

Ormai ci rendiamo tutti conto di come gli applicativi di **intelligenza artificiale** stiano trasformando la nostra vita quotidiana. Il fatto che perfino il Santo Padre abbia ritenuto opportuno elaborare un'enciclica su questo argomento non fa' altro che sottolineare la crescente importanza di questi applicativi ed anche, al contempo, i crescenti rischi, ad essi collegati.

Ecco il motivo per cui, mentre la tecnologia IA continua a svilupparsi e si inserisce sempre più in profondità nella vita della popolazione, è indispensabile attuare degli sforzi significativi per proteggere questi sistemi da rischi informatici.

È bene sottolineare anche il fatto che i rischi legati agli applicativi di **intelligenza artificiale** possono essere assai diversi dei rischi legati a software di tipo tradizionale: ad esempio, gli applicativi IA presentano rischi afferenti alla corruzione dei dati, al mascheramento dei dati e simili.

La norma in questione utilizza buone pratiche da attuare nella sicurezza informatica, insieme a nuove misure, che offrono una serie di indicazioni di alto livello applicabili a tutti i vari stadi di evoluzione di un applicativo IA.

L'obiettivo di questa norma è quello di fornire a tutti coloro che sono coinvolti nello sviluppo e distribuzione dei sistemi IA dei requisiti di base, afferenti alla sicurezza.

Il documento separa i principi ed i requisiti in cinque fasi.

Queste fasi fanno riferimento al progetto sicuro, allo sviluppo sicuro, all'utilizzo sicuro, alla manutenzione sicura e alla sicurezza delle operazioni di termine della vita utile dell'applicativo.

I principi descritti in questa norma possono anche essere collegati agli stadi del ciclo di vita di un applicativo, come descritti nella norma ISO/IEC 22989.

Raccomandiamo caldamente a tutti i lettori di leggere attentamente questa norma e citarla, sia in fase di approvvigionamento di applicativi, sia in fase di sviluppo interno di applicativi di IA.

ETSI EN 304 223 V2.1.1 (2025-12) -Securing Artificial Intelligence (SAI); Baseline Cyber Security Requirements for AI Models and Systems. - Protezione dell'Intelligenza Artificiale (SAI); Requisiti fondamentali di sicurezza informatica per modelli e sistemi di intelligenza artificiale.

Adalberto Biasiotti