PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 27 - numero 5870 di Lunedì 16 giugno 2025

Una norma che qualifica il livello di sicurezza degli applicativi di IA

Lo European Telecommunication Standard Institute (ETSI) ha pubblicato alla fine di aprile una preziosa norma sulle misure da attuare per rendere sicuro un applicativo di intelligenza artificiale.

Si chiama " *ETSI TS 104 223 - Securing Artificial Intelligence (SAI); Baseline Cyber Security Requirements for AI Models and Systems*" una norma recentemente pubblicata, che stabilisce un quadro di riferimento per mettere in sicurezza i sistemi di intelligenza artificiale contro i crescenti rischi di attacchi informatici.

La nuova specifica offre una linea guida, tanto affidabile quanto relativamente semplice da attuare, per attivare procedure che garantiscano un sufficiente livello di protezione per gli utenti finali. Affrontando il problema in maniera globale, la norma stabilisce 14 principi di base, che possono essere estesi fino a un totale di 72 principi, che sono stati definiti dell'ambito di cinque fasi del ciclo di vita, nelle quali fasi è articolato il livello di sicurezza di questi applicativi.

La norma offre principi trasparenti e di alto livello ed offre indicazioni concrete per aumentare il livello di sicurezza degli applicativi.

Il ricorso a questa norma è particolarmente utile per tutti coloro che non solo sviluppano questi applicativi, ma anche li acquistano da fornitori terzi e li utilizzano nelle proprie attività. Inserendo nel capitolato uno specifico riferimento a questa norma, si aiutano i venditori e gli utenti nel proteggere questi sistemi da attacchi informatici, in costante evoluzione.

I lettori sanno bene come l'intelligenza artificiale presenti dei rischi affatto particolari, in confronto ai software tradizionali, tra questi rischi particolari si possono inserire quelli relativi:

- alla corruzione dei dati,
- allo oscuramento del modello razionale,
- alla iniezione di elementi in grado di falsare il giudizio finale emesso dall'applicativo, nonché
- a vulnerabilità connesse alla complessità di gestione dei dati, che è tipica di questi applicativi.

Questa norma è stata sviluppata dalla commissione tecnica ETSI, che ha dedicato la sua attività alla messa in sicurezza degli applicativi di intelligenza artificiale. Di questo comitato tecnico fanno parte rappresentanti non solo provenienti da ogni parte del mondo, ma anche in grado di rappresentare le esigenze di organizzazioni internazionali, enti governativi e associazione di esperti di sicurezza informatica.

L'abbinamento di questi profili professionali, così diversificati, ha permesso di sviluppare una norma di rilevanza internazionale e attuabile senza eccessive difficoltà.

Di particolare interesse il fatto che ETSI ha pubblicato anche una linea guida, in fase di applicazione di questa norma, che prende in considerazione le esigenze particolari delle piccole e medie imprese e altri utenti, con profili particolari. Questa guida presenta tutt'una serie di esempi applicativi in una varietà di contesti, proprio per permettere ad una utenza quanto più allargata possibile di conoscere ed applicare questa norma.

Dopo la consueta introduzione, con riferimento a normative già esistenti ed una proposta di glossario, la norma indica, al quarto capitolo, quali sono i destinatari della norma stessa.

L'intero quinto capitolo è destinato alla illustrazione dei principi di sicurezza dell'intelligenza artificiale, articolati in:

- progetto sicuro, articolato in cinque principi,
- sviluppo sicuro, anch'esso articolato in cinque principi,
- attuazione sicura, articolata in un principio
- manutenzione sicura, articolata in due principi
- messa in sicurezza dell'applicativo in fase di dismissione finale, articolata in un principio.

È appena il caso di ricordare a tutti i lettori che la prestazione di un servizio o l'offerta di un bene, conforme a una norma italiana, europea od internazionale, rappresenta una prestazione od una fornitura conforme alla regola d'arte, secondo il codice civile italiano e anche secondo altri codici nazionali e internazionali. Il fatto di inserire uno specifico riferimento a questa norma, in fase di approvvigionamento di questi applicativi, rappresenta una garanzia per l'acquirente e per gli utenti finali e di questo fatto le compagnie di assicurazione, in Italia un'Europa, sono già ben consapevoli

ETSI TS 104 223 - Securing Artificial Intelligence (SAI); Baseline Cyber Security Requirements for AI Models and Systems (pdf)

Adalberto Biasiotti

www.puntosicuro.it