

# **Cybersecurity, GDPR e le sfide sull'intelligenza artificiale**

***Per l'occasione sarà presentato il volume "Privacy, Data Protection, Cybersecurity e Artificial Intelligence" a cura di Fabio Di Resta***

Con il patrocinio da parte della Regione Lazio

Nel Convegno del 10 ottobre prossimo organizzato dalla associazione Centro Europeo per la Privacy (EPCE) che si terrà a Roma presso la Regione Lazio, ente che patrocina anche l'evento, con la presenza di regolatori istituzionali dell'Agenzia nazionale per Cybersicurezza (ACN), dell'Agenzia per l'Italia digitale (Agid), del Garante per la protezione dei dati personali si farà il punto sulle sfide nazionali ed europee nella società digitale, sia nell'ambito della protezione dei dati personali e della cybersecurity, con riguardo all'Intelligenza artificiale, sia con riferimento alle minacce e alla crescente disinformazione derivante dal conflitto russo ucraino.

Il contesto internazionale attuale, il cui equilibrio risulta essere particolarmente precario, richiede agli operatori economici e agli enti pubblici ulteriori attenzioni dirette alla protezione delle reti e dei sistemi informativi. Analogamente tali attenzioni devono essere rivolte alla protezione dei dati personali e dei dati particolari che vengono gestiti sia in ambito pubblico che in ambito privato.

In tal senso, gli operatori economici e le pubbliche amministrazioni devono conoscere le diverse tipologie di

rischi attuali per prevenirli e gestirli in modo adeguato. Il nostro Paese dovrà gestire non solo sfide derivanti dal contesto geopolitico attuale ma prepararsi alle scadenze imminenti già ad inizio anno 2025 previste dalla **Direttiva UE 2022/2555 (c.d. Direttiva NIS 2)** e dal suo recepimento nell'ambito della normativa sulla **cybersecurity** avvenuto tramite il decreto legislativo n. 138 del 4 settembre 2024.

Inoltre, la deflagrazione e l'escalation dei conflitti russo-ucraino ed israelo-palestinese con connessa propaganda ha mostrato come le fake news possano influenzare non solo l'opinione pubblica dei Paesi ma anche la classe dirigente, con impatti anche istituzionali, l'intelligenza artificiale gioca un ruolo importante nell'informazione dei cittadini ed utenti dando origine a nuovi rischi connessi all'impossibilità di distinguere informazioni false da informazioni vere e/o verificate, occorre pertanto intervenire a vari livelli per garantire la democrazia del nostro Paese.

In tale ampio contesto, da alcuni decenni si inserisce l'ambito della protezione dei dati personali, nel nostro Paese ma anche in Europa, nel quale si affrontano questioni legate alla sicurezza del trattamento dei dati personali. Le sfide future e le nuove e crescenti minacce, chiedono sempre maggiore attenzione compreso l'obbligo per le aziende e la pubblica amministrazione di scegliere, selezionare e monitorare i **fornitori di tecnologia** affinché gli stessi garantiscano al contempo **sicurezza e conformità normativa**. Questa attività di selezione dei fornitori di tecnologia, è fondamentale per il raggiungimento del risultato, richiedono alle organizzazioni di essere efficienti e di acquisire nuove competenze digitali e legali, sia in ambito di protezione dei dati, sia soprattutto in ambito di cybersecurity, ma anche in ambito dell'Intelligenza Artificiale (IA).

Come è noto, serve al nostro Paese una strategia di medio e lungo periodo, ma occorre anche operare immediatamente per prevenire e gestire gli incidenti di sicurezza evitando in tal

modo la compromissione delle funzioni essenziali del nostro Paese.

Purtroppo, la diffusione esponenziale di ransomware nel nostro Paese in questi ultimi anni ci pone di fronte a scelte di governance pubblica tempestive ed efficaci.

Strettamente connesso a tali questioni urgenti vi è il tema di grande attualità relativo allo sviluppo dell'Intelligenza Artificiale (IA) che costituisce secondo molti versi una rivoluzione con nuovi benefici e nuovi rischi che necessitano di essere gestiti in modo proattivo.

L'IA nel settore della cybersecurity ha potenzialità enormi, sia per difendere le pubbliche amministrazioni e le imprese da numerosi attacchi di criminalità informatica che si realizzano ogni giorno, sia per i criminali informatici che, abbattendo costi e i tempi degli attacchi, concretizzano sempre più azioni efficaci e in modo massivo.

L'evento organizzato da EPCE sarà l'occasione per fare chiarezza sugli adempimenti e sulle imminenti scadenze, nonché sulle questioni sopra descritte in presenza di relatori istituzionali ed esperti del settore, sarà pertanto rivolto ad enti pubblici e al settore privato, imprese e liberi professionisti.

Per info su orari e programma:

<https://www.europeanprivacycentre.eu/it/cybersecurity-gdpr-e-l-e-sfide-sullintelligenza-artificiale-10-ottobre-2024/>