UNIONCAMERE VENETO
Delegazione di Bruxelles

Le tecnologie emergenti e il futuro della sicurezza interna dell'UE: una sfida da cogliere con responsabilità

Le nuove tecnologie stanno trasformando profondamente ogni ambito della nostra vita, dalla comunicazione alla salute, fino alla sicurezza. Proprio in quest'ultimo settore, le implicazioni sono, forse, tra le più significative, perché se da un lato le tecnologie emergenti offrono strumenti innovativi per contrastare la criminalità e migliorare la prevenzione, dall'altro pongono sfide inedite, complesse e potenzialmente molto pericolose. Proprio per questo la Commissione europea ha recentemente presentato una nuova strategia per la sicurezza interna, con l'obiettivo di rafforzare la resilienza dei Paesi membri dell'Unione e migliorare la capacità collettiva di rispondere in modo efficace e tempestivo alle minacce emergenti. L'iniziativa si basa anche su un nuovo rapporto elaborato dal Joint Research Centre (JRC), che analizza in modo approfondito i rischi e le opportunità legati alle tecnologie emergenti. Il rapporto si rivolge a decisori politici, forze dell'ordine e stakeholder del settore, proponendo una guida concreta per affrontare le sfide future. Il cuore del documento ruota attorno a un'idea chiave: la tecnologia, di per sé, non è né buona né cattiva; a fare la differenza è il modo in cui viene utilizzata.

Nel contesto della sicurezza interna, alcune tecnologie in particolare sembrano destinate a cambiare radicalmente gli equilibri in gioco: l'intelligenza artificiale, per esempio, rappresenta uno strumento sempre più diffuso per l'analisi dei dati, il monitoraggio delle minacce e la polizia predittiva. Tuttavia, gli stessi algoritmi che possono aiutare a prevenire un crimine, possono anche essere utilizzati da malintenzionati per generare deepfake ingannevoli, condurre attacchi informatici automatizzati o commettere sofisticate frodi d'identità. Si tratta, quindi, di una tecnologia bifronte, che richiede un attento bilanciamento tra opportunità e rischi. Un discorso simile vale per i droni, diventati ormai strumenti fondamentali per il monitoraggio delle frontiere, le operazioni di soccorso e la sorveglianza del territorio; tuttavia, questi dispositivi possono anche essere impiegati in attività criminali, dal traffico di droga alla sorveglianza illegale, fino alla possibilità di interferire con il traffico aereo. L'ambivalenza dell'innovazione non si ferma qui: l'informatica quantistica, considerata uno dei prossimi salti tecnologici, promette di rivoluzionare la crittografia e la sicurezza delle

comunicazioni, ma potrebbe anche minacciare le attuali infrastrutture crittografiche, esponendo a gravi rischi i sistemi governativi, finanziari e informatici.

Un ulteriore elemento da considerare è la blockchain, una tecnologia spesso associata alla sicurezza e alla trasparenza delle transazioni digitali. Se da un lato consente una gestione più sicura e decentralizzata dell'identità digitale, dall'altro facilita anche il riciclaggio di denaro e altre attività finanziarie illecite, rendendo difficile tracciare i movimenti di soggetti criminali che operano in anonimato.

Alla luce di queste complessità, la strategia dell'UE si concentra su alcuni pilastri fondamentali per affrontare il futuro della sicurezza con responsabilità e lungimiranza. Una delle prime azioni proposte riguarda il potenziamento della capacità di previsione e monitoraggio del rischio: l'adozione di strumenti di analisi prospettica e pianificazione di scenari estremi permetterà di individuare minacce potenziali prima che si concretizzino, aumentando così la capacità di risposta preventiva.

Un altro punto chiave è rappresentato dalla regolamentazione dell'intelligenza artificiale: l'UE, con l'AI Act, ha già avviato un percorso pionieristico per assicurare che le applicazioni di IA siano trasparenti, responsabili ed eticamente allineate. Tuttavia, il rapporto evidenzia come siano necessari ulteriori sforzi per garantire un uso corretto e sicuro di queste tecnologie nei settori sensibili come la sicurezza e l'ordine pubblico.

Fondamentale sarà anche rafforzare la collaborazione tra settore pubblico e privato: molte delle tecnologie più avanzate, infatti, sono sviluppate dall'industria, e una sinergia strutturata tra imprese, forze dell'ordine e istituzioni europee potrà garantire che l'innovazione tecnologica sia sempre più orientata alla tutela dei cittadini e della legalità.

Infine, il rapporto evidenzia la necessità urgente di potenziare le infrastrutture digitali e la sicurezza informatica, con particolare attenzione alla crittografia post-quantistica e alla cooperazione transfrontaliera.

FONTE e LINK al testo originale:

Fonte: Commissione Europea

LINK alla Notizia: https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/how-will-emerging-technologies-reshape-eu-internal-security-2025-04-01_en?prefLang=it

ProtectEU: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_920