



Non solo Iran: le città intelligenti sono il nuovo campo di battaglia tecnologico

Descrizione

(Adnkronos) La morte della guida suprema iraniana Ali Khamenei in un attacco israeliano ha riportato al centro una questione spesso sottovalutata: le infrastrutture digitali delle città – telecamere, sensori, reti di gestione urbana – non sono solo strumenti per migliorare la mobilità o l'efficienza energetica. Possono diventare anche piattaforme di intelligence strategica.

Secondo Rosario Cerra, presidente del Centro economia digitale, il caso di Teheran dimostra come le smart city siano ormai parte integrante della competizione geopolitica e della sicurezza nazionale. In questa intervista con Adnkronos spiega perché le città intelligenti rappresentano un nuovo campo di battaglia tecnologico e perché l'Europa deve costruire una propria sovranità tecnologica.

Cosa rivela l'operazione che ha portato alla morte di Ali Khamenei?

Rivela qualcosa che gli esperti di sicurezza sanno da tempo: le infrastrutture digitali delle città sono anche strumenti di sorveglianza strategica. Nel caso di Teheran, non è stata sorprendente solo la precisione dei missili, capaci di colpire bersagli estremamente piccoli da oltre mille chilometri di distanza. La vera sorpresa è ci che era accaduto anni prima, in silenzio: quasi tutte le telecamere del traffico della capitale iraniana erano state violate e le loro immagini venivano trasmesse in tempo reale a server esterni.

Questo ha permesso di costruire quello che l'intelligence definisce pattern of life: una mappatura continua e granulare di come una città si muove, respira e si organizza. Quando si conosce una città come la strada in cui si è cresciuti, qualsiasi anomalia diventa immediatamente visibile.

Le smart city nascono con obiettivi molto diversi: mobilità, sostenibilità, servizi urbani.

Nessuno di quegli obiettivi è falso. Le smart city promettono semafori intelligenti, sistemi di sicurezza più efficaci, reti di sensori per l'energia e piattaforme integrate per i servizi pubblici. Il punto è che queste infrastrutture possono fare molto di più. Una telecamera a un incrocio non vede solo le

automobili: vede volti, comportamenti ricorrenti, anomalie. Se collegata a sistemi di riconoscimento facciale e analisi delle reti sociali, diventa un nodo di raccolta di intelligence. Moltiplichiamo questo per migliaia di dispositivi e otteniamo una piattaforma di sorveglianza persistente sull'intera popolazione urbana.

Lei sostiene che esiste un rischio ancora più insidioso di quello emerso a Teheran.

Il fatto che il rischio possa essere incorporato nel sistema stesso. A Teheran un attore esterno ha violato l'infrastruttura. Ma cosa accade quando il produttore dell'infrastruttura ha obblighi legali verso un governo straniero e i suoi apparati di intelligence?

Il caso più noto è quello della Cina. Dal 2017 una legge sull'intelligence nazionale impone alle aziende di sostenere e cooperare con le attività di intelligence dello Stato. Questo obbligo si applica a tutte le aziende soggette alla giurisdizione cinese, indipendentemente dal luogo in cui i loro prodotti vengono installati.

Parliamo di aziende come Huawei, Hikvision, ZTE o Dahua, che hanno installato infrastrutture di sicurezza urbana in oltre cento Paesi. In molti casi questi sistemi costituiscono la spina dorsale della videosorveglianza urbana e vengono gestiti anche da remoto.

Nel vostro rapporto sulla High-Tech Economy sostenete che la tecnologia è diventata una questione di potere geopolitico. In che modo le smart city rientrano in questo paradigma?

Nel nostro rapporto abbiamo sostenuto che la tecnologia non è solo un fattore produttivo o un servizio abilitante. È diventata il perno attorno al quale ruotano la sovranità e la rilevanza geopolitica delle nazioni.

La smart city rende questa dinamica molto concreta. L'infrastruttura urbana digitale è telecamere, sensori, reti di connettività e piattaforme di gestione dei dati non è semplicemente un servizio municipale. È il nodo fisico della High-Tech Economy: il punto in cui raccolta dati, algoritmi e controllo in tempo reale si fondono.

I dati generati da una smart city non sono dati municipali. Sono una rappresentazione dinamica di come funziona una nazione, di dove si trovano le sue vulnerabilità e di come si muovono i suoi decisori.

Questo ci porta al tema del dual use. Le città stanno diventando parte del perimetro della sicurezza nazionale?

Esattamente. Il concetto di dual use è tecnologie civili utilizzabili anche in ambito militare o di sicurezza esiste da tempo. Pensiamo all'aerospazio o alla crittografia. La differenza oggi è la scala. Le tecnologie dual use non sono più confinate a settori industriali altamente specializzati. Sono nei semafori, nelle stazioni, negli ospedali, nei parcheggi.

Di conseguenza il perimetro della sicurezza nazionale si è spostato dentro le città. Non alle frontiere o nelle basi militari, ma nelle infrastrutture urbane quotidiane.

Le amministrazioni locali sono consapevoli di questa dimensione?

Spesso no. Quando un comune acquista sistemi di videosorveglianza o piattaforme di gestione urbana pensa di prendere una decisione tecnica o di bilancio. In realtà sta prendendo una decisione di sicurezza nazionale.

Il problema è che molte amministrazioni locali non hanno né le competenze né i quadri normativi necessari per valutare il rischio geopolitico di queste scelte.

Negli ultimi anni diversi Paesi hanno iniziato a vietare alcune tecnologie.

È un passo necessario, ma non sufficiente. Gli Stati Uniti hanno vietato gli acquisti federali di prodotti Hikvision e Dahua. L'Australia ha rimosso queste telecamere dagli edifici governativi sensibili. Il Regno Unito ha imposto l'uscita di Huawei dalle reti 5G. Anche l'India sta rafforzando i controlli sulle telecamere importate.

Il problema è che queste misure spesso arrivano tardi: le infrastrutture sono già installate e continuano a funzionare. E molti enti locali non rientrano nelle categorie coperte dai divieti.

Qual è allora la vera sfida per l'Europa?

La sfida non è solo difensiva. Non basta vietare o rimuovere tecnologie rischiose. Bisogna costruire un ecosistema alternativo solido e competitivo, basato su alleanze con partner affidabili.

L'Europa deve smettere di essere solo un mercato per tecnologie sviluppate altrove e diventare protagonista della loro progettazione, con architetture aperte, audit indipendenti e governance trasparente.

Investire in un'industria europea della sicurezza urbana non è solo una questione economica: è un posizionamento geopolitico.

In concreto, cosa dovrebbero fare oggi i governi europei?

Servono interventi su tre livelli.

Il primo è normativo: le gare pubbliche per infrastrutture di sorveglianza urbana devono includere criteri di rischio geopolitico simili a quelli adottati per il 5G.

Il secondo è architeturale: i sistemi di smart city devono essere progettati secondo principi di security by design, con cifratura end-to-end, separazione delle reti e localizzazione dei dati.

Il terzo è strategico: l'Europa deve investire nella costruzione di capacità tecnologiche proprie, invece di limitarsi a escludere i competitor. La sovranità tecnologica proattiva significa avere alternative credibili da offrire.

Siamo entrati nel paradosso delle smart city?

Più una città diventa intelligente, connessa e integrata, più diventa trasparente. E in un contesto geopolitico ostile la trasparenza può diventare vulnerabilità. A Teheran le telecamere erano anche occhi altrui. In qualche altra città del mondo potrebbe accadere la stessa cosa, senza neppure bisogno di un attacco informatico. Perché la porta potrebbe essere già aperta dall'interno. (di Giorgio Rutelli)

??

economia

webinfo@adnkronos.com (Web Info)

Categoria

1. Comunicati

Tag

1. Ultimora

Data di creazione

Marzo 5, 2026

Autore

redazione

default watermark