

Hacker inventa una pellicola per rendere invisibile la propria auto a telecamere e radar. Come funziona di Andrea Paoletti

Negli Usa sono ormai centinaia di migliaia le telecamere con riconoscimento facciale, pensate per prevenire la criminalità ma usate in modo indiscriminato. La voce del dissenso passa anche soluzioni creative per confondere i computer. (Fonte: <https://www.corriere.it/> 15 agosto 2026)



Senza arrivare agli eccessi della Cina dove basta percorrere un'autostrada per essere accecati dal bagliore di centinaia di flash e sentirsi puntati addosso gli obiettivi di una foresta di telecamere, anche negli USA sono ormai numerosissimi i dispositivi che leggono le targhe e riconoscono i volti dei conducenti. Servono alle forze dell'ordine per controllare il territorio e individuare potenziali malviventi, ma l'immenso database di immagini ed informazioni che ne scaturisce pone questioni importanti legate alla privacy, ma anche alla sicurezza in caso di errore. Questo è il motivo ufficiale della protesta di un gruppo di hacker, uno dei quali ha inventato un modo per rendere le automobili "invisibili".

La Yaris che manda in tilt i sensori

L'idea arriva dal ricercatore di cybersecurity Bill Swearingen, fondatore del progetto noRecognition, il cui obiettivo è combattere gli algoritmi dell'AI per impedire che riconoscano volti e oggetti, incluse le auto. La cosa più ironica è che per sviluppare i particolari pattern grafici che mandano in confusione i sistemi automatici di riconoscimento, Bill si è servito lui stesso dell'AI, in pratica mettendole una contro l'altra. La dimostrazione più spettacolare - dopo aver dimostrato il funzionamento su felpe e cappelli che facevano "sparire" le persone, è avvenuta

durante la conferenza DEF CON di Las Vegas, dove una Toyota Yaris è stata ricoperta con uno di questi disegni.



Come funziona

La telecamera in realtà continuava a vedere e registrare l'auto, ma il software faticava a riconoscerla come tale perché l'algoritmo giungeva a conclusioni sbagliate. Secondo i test effettuati da Swearingen, il pattern è riuscito a confondere tutti gli 11 algoritmi open source di riconoscimento utilizzati nella prova, oltre ai sistemi Flock per la lettura delle targhe e alle body camera di Axon. Qui non si tratta della leggenda metropolitana della pellicola riflettente capace di rendere illeggibile una targa, ma di un vero e proprio camouflaje digitale applicato fisicamente alla vettura.

Non è invisibilità, è confusione

La differenza è sostanziale. Invece di attaccare direttamente il software, la strategia è quella di ricoprire con questi disegni astratti l'oggetto che il software deve interpretare: siccome ci sono tantissime grafiche capaci di confondere gli algoritmi di analisi, impedendo loro di raggiungere la

percentuale minima di certezza su ciò che stanno vedendo, **secondo Bill sarà sempre più difficile neutralizzare un singolo disegno.**

Il rischio di errore

Flock Safety è il nome della gigantesca rete di telecamere capaci non solo di leggere le targhe, ma di identificare caratteristiche delle vetture, creando una sorta di “impronta digitale” dell'automobile. Il sistema viene utilizzato dalle forze dell'ordine statunitensi per ricostruire gli spostamenti e collegare veicoli e luoghi, **con una percentuale di accuratezza tra il 93 e il 99 per cento**, ma quando si parla di miliardi di scansioni, anche una percentuale apparentemente eccellente genera un numero di errori impressionanti. Secondo i calcoli, sono **20 miliardi di targhe al mese** e anche ipotizzando un'accuratezza del **99%**, significherebbe potenzialmente **200 milioni di pericolose imprecisioni.** Un falso riconoscimento segnalato dal software può trasformarsi in un controllo di polizia, in una detenzione illegittima e, nei casi peggiori, in una situazione pericolosa. Il punto debole, dunque, non è necessariamente una singola telecamera che confonde la lettera “O” e il numero “0”, ma l'intera catena: **dati inseriti male, riconoscimento automatico imperfetto e operatori che scelgono di fidarsi della tecnologia senza verificare adeguatamente.**



La guerra delle macchine

E così nasce una sfida degna di un film di fantascienza, ma assolutamente reale: l'intelligenza artificiale utilizzata per sorvegliare le automobili viene sfidata da un'altra intelligenza artificiale che studia come renderle difficili da riconoscere. Flock può addestrare i propri sistemi

per reagire ai nuovi pattern, mentre noRecognition può generare grafiche sempre differenti, in **una partita a scacchi tra algoritmi**. Quello che a prima vista può sembrare un wrapping curioso, oppure le livree con cui le Case automobilistiche nascondono le forme dei prototipi durante i test, è a tutti gli effetti **un vestito pensato per non farsi riconoscere**. La Yaris ricoperta di strani disegni alla fine non è altro che **il tentativo di sfuggire a un'epoca in cui le automobili sono diventate oggetti digitalmente tracciabili e dove la carrozzeria può trasformarsi in uno strumento di privacy**.