dossier

Privacy o sicurezza?

La videosorveglianza nell'era degli algoritmi

Andrea Carobene
Giornalista, Head of Digital and Data Management di United Risk Management
<a.carobene@unitedrisk.eu>

La videosorveglianza, ormai presente in maniera capillare negli spazi pubblici e privati, riceve nuove possibilità di applicazione dall'intelligenza artificiale: i nuovi dispositivi non si limitano a registrare, ma sono anche in grado di interpretare ciò che osservano e di riconoscere oggetti e persone. Questo offre nuove opportunità in termini di tutela della sicurezza e della legalità, ma una riflessione più attenta individua anche rischi per la tutela della privacy, in particolare sul luogo di lavoro. A quale scopo e a vantaggio di chi vengono impiegate le informazioni che le telecamere intelligenti consentono di raccogliere? Occorre trovare un bilanciamento tra opposte esigenze, attraverso la definizione di standard e di vincoli operativi per gli apparati di videosorveglianza.

Facciamo un piccolo esperimento: quante sono le telecamere che ogni giorno ci inquadrano? Probabilmente sono decine e decine le apparecchiature che, spesso senza che noi ne abbiamo piena consapevolezza, riprendono i nostri movimenti. Incontriamo telecamere nei negozi, sui mezzi di trasporto pubblico, in banca, agli incroci e su molti semafori, lungo i marciapiedi e le strade, all'ingresso delle zone a traffico limitato, ai caselli autostradali e ai distributori. Telecamere inquadrano i nostri volti allo stadio, nei luoghi di lavoro, negli aeroporti, nei grandi magazzini.

Il fenomeno è globale e si si stima che quest'anno nel mondo si supererà il miliardo di telecamere installate[1]. Appartiene ormai all'esperienza comune l'impressione di sentirsi osservati da questi occhi elettronici; ma in quale misura noi siamo realmente "visti" o "guardati"? Più precisamente: **qual è la capacità dei dispositivi di sorveglianza di interpretare la realtà che registrano, ricavandone informazioni utili?** Per fare questo, occorre che l'"occhio" sia collegato a un "cervello": in tal caso, abbiamo a che fare con una intelligenza artificiale (AI), cioè un computer in grado di svolgere questa funzione di interpretazione. Nelle prossime pagine, vedremo in che modo l'AI modifica la funzione e i termini di impiego della videosorveglianza e ne estende gli ambiti di applicazione. Questa disamina ci permetterà di evidenziare una prima serie di opportunità e di rischi connessi alle nuove tecnologie, che una analisi più approfondita dei singoli casi renderebbe molto più corposa.

La tutela della sicurezza

Gli utilizzi di questi apparecchi sono diversi, ma sicuramente quello più noto è il loro impiego per la sicurezza, spesso indicato con il termine inglese *security*. In questo ambito, quando si parla di videosorveglianza si intende una tecnologia che permette di visualizzare un'area o un edificio da proteggere, con l'obiettivo di rilevare eventuali accessi non autorizzati. **L'utilizzo con funzione di *security* può essere affiancato a quello a scopo di prevenzione di incidenti e infortuni**, ad esempio vigilando sul rispetto delle norme della sicurezza sul lavoro (in questo caso si intende sicurezza nel senso del termine inglese *safety*). Un esempio è quello della gestione di cantieri complessi, dove una centrale operativa remota può monitorare da lontano l'attività svolta, verificando che tutti gli operai indossino i dispositivi di sicurezza individuali come caschi e scarpe antinfortunistiche, che i mezzi di lavoro seguano esattamente i percorsi predefiniti, che i luoghi a rischio siano correttamente recintati e così via.

Un ulteriore utilizzo estremamente diffuso delle telecamere è il controllo del traffico stradale. Anche in questo caso le immagini sono veicolate verso centrali operative che possono seguire in tempo reale il flusso dei veicoli, disponendo eventuali interventi in caso di necessità e sanzionando le trasgressioni per mezzo del controllo delle targhe. Ancora: le videocamere possono essere usate per il monitoraggio di parchi o aree protette, per la verifica di

[1] IHS Markit (2019), *Video Surveillance Installed Base Report*, dicembre, <https://technology.ihs.com/607069/video-surveillance-installed-base-report-2019>.

fenomeni naturali che necessitano di un'attenzione costante, come una frana non stabilizzata, o ancora per la rilevazione di profili altimetrici. In realtà, **l'utilizzo delle telecamere si amplia sempre più**. Telecamere termiche (termocamere) possono essere montate su droni per valutare l'efficienza degli impianti fotovoltaici installati sui tetti, altri sistemi consentono invece la creazione di modelli tridimensionali (detti *digital twins*, cioè gemelli digitali) di vaste aree edificate o edificabili per progettarne e seguirne lo sviluppo urbanistico.

Diverse sono le tecnologie impiegate per il funzionamento degli apparecchi di videosorveglianza e la raccolta dei dati, che vanno al di là della "semplice" cattura di immagini, anche se digitali. Le telecamere possono essere fisse, oppure possono essere ruotate da remoto sul piano verticale e orizzontale aggiustando la messa a fuoco, e, grazie alla tecnologia basata sui raggi infrarossi, possono operare anche al buio. Le termocamere rilevano infatti le differenze di temperatura e consentono, ad esempio, di individuare una persona che si introduce al buio all'interno di un sito protetto, o di misurare l'isolamento termico di un edificio. Per aumentare la sicurezza si usano anche veri e propri radar che, una volta segnalata una possibile intrusione, allertano una telecamera mobile che automaticamente cambia il proprio orientamento, puntando verso il luogo da cui proviene l'allarme e mettendosi automaticamente a fuoco. In alcuni casi è possibile organizzare veri e propri pattugliamenti da remoto, accendendo e orientando le telecamere su orari e percorsi prefissati. Infine, le telecamere possono essere programmate per non "vedere" alcune zone, che vengono automaticamente oscurate, come l'interno delle finestre di un edificio privato che confina con il sito da sorvegliare.

Le immagini possono essere viste in diretta o raccolte in un registratore che, nel rispetto delle regole definite dal garante della privacy (cfr Carobene e Mastrangelo 2019), le cancella periodicamente sovrascrivendone la traccia. Le registrazioni possono essere crittografate con una chiave di accesso messa a disposizione unicamente delle persone che hanno diritto alla visione e che possono consegnarle alle autorità competenti, qualora ne facciano richiesta.

Una sola tecnologia non basta

Col tempo ci si è resi conto che la semplice raccolta delle immagini non è sufficiente per realizzare una piena politica di *security* e di *safety*. In altre parole, **non è possibile garantire un livello di sicurezza adeguato se i filmati sono semplicemente rimandati**

ai monitor di una centrale operativa dove gli addetti li visionano in diretta. **Il motivo è legato alla soglia di attenzione umana**: anche un professionista esperto non può guardare per otto ore di fila una decina di monitor prestando costantemente la necessaria attenzione; dopo un certo periodo la concentrazione inevitabilmente cala e il rischio di non percepire anche eventi gravi o macroscopici è elevato.

Inoltre, la concentrazione umana è fortemente selettiva, come ha dimostrato un celebre test eseguito da Daniel Simons (Università dell'Illinois a Urbana-Champaign) e Christopher Chabris (Università di Harvard). I due ricercatori hanno chiesto a un gruppo di volontari di osservare un filmato di pochi minuti nei quali un gruppo di ragazzi si scambia una palla giocando a basket e di contare con attenzione i passaggi effettuati dai giocatori con maglia bianca. Nel bel mezzo del filmato, un uomo vestito da gorilla entra in campo, saluta ed esce dalla scena. Ebbene: circa metà dei volontari, impegnati nel contare i passaggi, non si sono accorti della strana intrusione che, pur essendo stata formalmente "vista", non era stata registrata dal cervello e quindi non si era trasformata in informazione conscia (Simons e Chabris 1999).

Esperimenti di questo tipo dimostrano che, anche quando una persona è estremamente attenta, può non percepire un evento particolare, se questo è inatteso. Così in una centrale operativa, certi accadimenti, anche se inquadrati dalle telecamere, possono non essere effettivamente "visti" dagli operatori, non solo per il calo fisiologico di attenzione. È per questo motivo che le telecamere di sorveglianza, da oggetti "stupidi" si sono dovute trasformare progressivamente in "intelligenti". Il rischio era che, all'aumentare del numero delle telecamere di sorveglianza, non aumentasse in maniera altrettanto significativa la sicurezza reale dei luoghi monitorati.

Telecamere e intelligenza artificiale

La soluzione più praticata per sopperire a questo limite delle telecamere è realizzare **sistemi di sorveglianza che in automatico lancino un allarme al verificarsi di determinate condizioni** o eventi, ad esempio tramite l'invio di un segnale sonoro o di una mail, o con altri mezzi.

Un esempio è dato dai sistemi di *geofencing*, che realizzano barriere virtuali di protezione di determinate aree (ad esempio scuole, aree edificabili, ecc.). Si tratta di barriere di luce invisibile che, quando sono attraversate da un oggetto, fanno scattare un allarme, richiamando così l'attenzione dell'operatore, ad esempio in caso di violazione di una recinzione perimetrale. **Sistemi di questo tipo,**

tuttavia, non sono ancora sufficienti a garantire un'elevata sicurezza, **in quanto è difficile discriminare tra veri e falsi allarmi**. Un tipico caso è il superamento della barriera da parte di un piccolo animale, che genera un allarme inutile. Segnali di questo tipo, chiamati falsi positivi, possono essere causati da molteplici fattori, come la crescita della vegetazione con foglie che si muovono al vento, o un ragno che tesse la sua tela sull'occhio di una telecamera. Anche in questo caso il rischio è di abbassare la soglia di attenzione degli operatori, che si assuefanno progressivamente agli allarmi a causa di un eccesso di falsi positivi. In un'ottica di sicurezza, occorre trovare un bilanciamento tra il rischio di falsi positivi e quello di falsi negativi. Annullare i primi, cioè fare sì che l'allarme scatti solo in presenza di un pericolo reale, richiede un innalzamento della soglia di sensibilità dell'apparato, aumentando così la probabilità che pericoli reali, ma caratterizzati da segnali più deboli, non vengano riconosciuti (i cosiddetti falsi negativi) e di conseguenza non producano alcun segnale di allarme. Si finirebbe così per non individuare alcuni eventi che richiedono un intervento.

In questo contesto, **un aiuto è offerto da sistemi di videoanalisi che eseguono, grazie all'AI e alle reti neurali, un processo di classificazione automatica delle immagini** e permettono così di distinguere la sagoma di un animale da quella di un essere umano. Sistemi di questo tipo, associati alle telecamere a infrarossi, aiutano a individuare con maggiore efficacia le minacce reali. Si tratta di una tecnologia di *deep learning*, che discrimina tra diverse tipologie di immagini paragonandole a quelle con le quali la macchina è stata "allenata" per distinguere tra forme differenti, separando quelle rilevanti da quelle prive di interesse.

Una **rete neurale artificiale** (*Artificial Neural Network*, ANN) è un modello matematico che imita il funzionamento di una rete neurale biologica, cioè di un gruppo di neuroni che svolgono una specifica funzione. È questo tipo di funzionamento che permette al computer di imparare a interpretare i dati che riceve.

L'AI è utilizzata anche nei sistemi di lettura delle targhe, per collegare un veicolo al suo proprietario, e negli algoritmi di riconoscimento facciale. In quest'ultimo caso le telecamere riconoscono i volti delle persone, individuando ad esempio chi ha un determinato diritto, come quello di accedere a un'area riservata (*white list*), oppure identificando soggetti che richiedono una particolare attenzione, come persone ricercate dalla magistratura (*black list*). Le *black list* del riconoscimento facciale possono essere costruite scansionando le foto segnaletiche della polizia, ma anche in questo caso è necessario trovare il giusto equilibrio tra falsi positivi e falsi negativi.

Anche nel caso della prevenzione e della sicurezza sul lavoro l'AI può fornire un aiuto prezioso, permettendo ad esempio una

gestione remota dei cantieri. Un sistema di questo tipo funziona con un algoritmo di classificazione supervisionato: **la rete neurale viene addestrata tramite la somministrazione di una serie di immagini** di lavoratrici e lavoratori che indossano un casco o ne sono privi, accompagnate dalla corretta etichetta ("casco" / "non casco"). Alla macchina vengono dati due tipi diversi di input: positivo in caso di situazione conforme ("casco") e negativo in caso contrario ("non casco"). Accanto a questa metodologia, esistono anche algoritmi di apprendimento non supervisionato, dove il sistema impara autonomamente a classificare oggetti e riconoscere ciò che merita attenzione.

Opportunità e rischi

Come per qualunque tecnologia, anche l'utilizzo delle videocamere abbinato all'AI presenta rischi e opportunità.

Sul piano delle opportunità, oltre a quella già segnalata sul versante della sicurezza, un capitolo importante merita **il rispetto della legalità sui luoghi di lavoro**. L'AI, abbinata all'utilizzo delle telecamere, permette infatti di "vedere" irregolarità che altrimenti rimarrebbero nascoste. L'esempio tipico, già citato, è quello delle telecamere che avvisano immediatamente quando gli operai in un cantiere non indossano i dispositivi di protezione previsti dalle norme. Si tratta di programmi che adottano algoritmi di *machine learning* per la classificazione delle immagini, distinguendo così fra situazioni "normali" e "critiche".

Un utilizzo di questo tipo è stato proposto dalla Regione Lombardia con la recente *Legge regionale 26 novembre 2019, n. 18, Misure di semplificazione e incentivazione per la rigenerazione urbana e territoriale*. Questa norma vuole favorire il recupero dei circa 3.500 edifici e aree abbandonate censiti in Lombardia, introducendo benefici sul piano dell'indice di edificabilità o della variazione della destinazione d'uso. Tali benefici sono concessi, tra l'altro, a chi adotta «processi di gestione dei rischi dei cantieri, basati sulla tracciabilità e sulle attività di controllo […], che si basino su tecnologie avanzate, utilizzando strumenti come la geolocalizzazione, la videosorveglianza» (art. 3, c. 1, lett. p). In questo caso la videosorveglianza intelligente diventa uno strumento per garantire la legalità e il rispetto delle norme nei cantieri, con l'obiettivo di ridurre gli infortuni sul lavoro. Un utilizzo per la legalità che in Lombardia diventa funzionale al progetto di recupero delle aree dismesse.

L'esempio dei cantieri ci introduce alla questione del monitoraggio dei luoghi di lavoro. Infatti, **l'utilizzo di telecamere "intelligenti" costituisce un ulteriore strumento per il controllo**

da remoto dei lavoratori, una pratica che non è permessa, fatte salve le esigenze organizzative, di tutela del patrimonio aziendale e di sicurezza dei lavoratori, o ancora un previo accordo con si sindacati o con l'autorizzazione amministrativa della Direzione territoriale del lavoro.

Il senso di questa normativa è **conciliare due diritti tra loro apparentemente contrastanti: il diritto del lavoratore alla riservatezza e quello del datore di lavoro alla tutela dei beni aziendali**, senza trascurare l'aspetto della sicurezza del lavoro. La conciliazione viene realizzata imponendo al datore di lavoro il rispetto dei principi che tutelano i dati personali, tra cui spicca quello della proporzionalità, ossia l'utilizzo di strumenti che non siano eccedenti lo scopo della verifica. Ci si può chiedere se l'uso massivo dell'AI nel controllo dei lavoratori non rischi di infrangere questo principio, permettendo una individuazione "sproporzionata" della persona, la ricostruzione di tutti i suoi movimenti, la classificazione delle sue azioni, ecc.

Da questo punto di vista ci si scontra con uno dei problemi caratteristici dell'utilizzo dell'AI, ossia la facilità con il quale questi strumenti riescono a penetrare nella sfera privata, portando alla luce anche aspetti estremamente riservati. Nulla esclude che, con il miglioramento degli algoritmi, in un prossimo futuro si possa capire se una persona si trova in un particolare stato emotivo, come stress, stanchezza o eccessivo nervosismo. Un uso diffuso di telecamere intelligenti sui luoghi di lavoro, realizzato a fini di sicurezza, si potrebbe tradurre nella classificazione degli stati mentali dei lavoratori, che potrebbero essere eventualmente collegati alla loro produttività. Non si tratta di un'ipotesi remota: l'AI, avendo la possibilità di analizzare milioni e milioni di dati, può rivelare anche gli atteggiamenti più privati. Chi scrive ha testato un programma che individua, con il 91% di precisione, se una persona che naviga tra le pagine di un sito effettuerà un acquisto o meno semplicemente analizzando il tempo trascorso su ogni pagina, i click effettuati e il percorso seguito. L'analisi dei movimenti del corpo umano fornisce molti più dati dei click di un mouse, ed è quindi potenzialmente capace di fare emergere informazioni ben più private della decisione di acquistare o meno un prodotto.

Queste riflessioni si accompagnano alla convinzione che **oggi non è possibile pensare la nostra società senza le telecamere**. Tramite questa tecnologia garantiamo la sicurezza di alcuni ambienti, viaggiamo con più tranquillità sulle strade, controlliamo fenomeni naturali ed eseguiamo la diagnosi energetica degli edifici.

Le telecamere intelligenti costituiscono un'occasione straordinaria per migliorare la nostra vita quotidiana, ma al contempo è necessario che il loro uso massivo venga regolato da norme precise, basate sugli stessi principi che tutelano i dati individuali. Allo stesso tempo è necessario che gli algoritmi alla base del loro funzionamento siano trasparenti e comprensibili, ossia che si possa sempre conoscere il criterio con il quale queste telecamere classificano gli eventi. Solamente così si potrà **trovare un giusto bilanciamento tra sicurezza, legalità e rispetto del diritto alla riservatezza di ogni persona**. Un bilanciamento necessario perché questi algoritmi, da strumento prezioso per la sicurezza e la legalità, non si trasformino invece nell'incubo del Grande Fratello.

Benanti P. (2020), «L'algoritmo: un nuovo attore nel mondo del lavoro?», in *Aggiornamenti Sociali*, 1, 12-19.

Biasiotti A. (2019), *Gli impianti di videosorveglianza. Progettazione, gestione, manutenzione, protezione dei dati*, EPC, Roma.

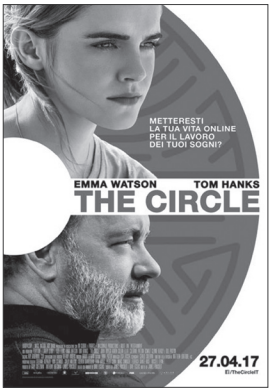
Carobene A. – Mastrangelo M. (2019), «La tutela dei dati personali in un mondo digitale. Il Regolamento europeo sulla privacy», in *Aggiornamenti Sociali*, 6-7, 465-473.

Manzelli S. – Sivieri G. (2019), *Videosorveglianza urbana integrata. Città più sicure con il D.L. 14/2017 e il D.L. 113/2018*, Edizioni Giuridiche Simone, Napoli.

Simons D. – Chabris C. (1999), «Gorillas in our midst: sustained inattentional blindness for dynamic events», in *Perception*, 28, 1059-1074.

Soro A. (2019), «Apertura dei lavori,» in *I confini del digitale. Nuovi scenari per la protezione dei dati. Atti del convegno, 29 gennaio 2019, Roma*, Garante per la protezione dei dati personali, 3-12, <www.garanteprivacy.it/documents/10160/0/I+confini+del+digitale.+Nuovi+scenari+per+la+protezione+dei+dati+-+Atti+del+Convegno.pdf/89efdb61-c0c3-cc6f-8037-f0b283bad2b4?version=1.0>.

Uni Global Union (2018), *Top 10 Principles for Workers' Data Privacy and Protection*, Uni Global Union, Nyon (CH) <www.thefutureworldofwork.org/media/35421/uni_workers_data_protection.pdf>.



Stati Uniti – Emirati Arabi Uniti 2017,
Thriller, Drammatico,
110 minuti

Mae entra a far parte dell'esclusivo mondo che dà vita a The Circle, il social network più diffuso al mondo.
Ma è tutto oro quel che luccica?

James Ponsoldt

The Circle

Mae Holland (Emma Watson) è una ragazza semplice, pochi grilli per la testa, un padre malato di SLA accudito dalla mamma, troppo poveri per pagarsi cure adeguate. Lavora nel call center della società idrica della sua città, quando inaspettatamente le si offre la possibilità di un colloquio per entrare nell'esclusiva realtà di The Circle, la società di software che sviluppa il social network più diffuso al mondo.
Dopo un periodo di ambientamento, Mae viene avviluppata dalla rete per cui lavora, in cui tutti sono sempre connessi e dove non sembra esserci spazio per nessun tipo di privacy. In un estremo tentativo di sottrarsi all'essere perennemente on line, la giovane rischia di morire affogata durante una escursione notturna in solitaria, dopo aver rubato un kayak, ma viene salvata grazie a un servizio di geolocalizzazione posizionato su una boa, che però rivela anche il suo furto. Consapevole di aver violato la legge e di essersi salvata solo grazie alla tecnologia di The Circle, Mae stringe un accordo con il proprietario della società di software, Eamon Bailey (Tom Hanks) e si sottopone all'esperimento di vivere perennemente connessa e on line sul social network, sposando l'idea che la totale trasparenza sia il modo migliore per comportarsi in modo onesto, sempre.
Ben presto però la vita di Mae, esposta all'interazione con i follower di tutto il mondo, si complica e la ragazza si rende conto di non essere libera come aveva pensato: qualunque spazio personale viene letteralmente azzerato, a scapito anche dei genitori e dei più cari amici, che finiscono loro malgrado nelle maglie di una rete troppo invasiva che non guarda in faccia a nessuno, ma che desidera solo scrutare e vivisezionare la vita degli altri, in nome di una trasparenza che in realtà si rivela piena di ombre.
Mae scopre infatti che tutti i dati che The Circle raccoglie da tutti i suoi milioni di utenti, tra cui politici, governanti, persone famose ecc., vengono conservati gelosamente per poter essere riutilizzati in futuro in un sistema totalizzante che potrebbe consentire a The Circle di controllare il mondo. La mente geniale di Eamon Bailey punta proprio a questo, ma sarà Mae a sconfiggerlo con le sue stesse armi, sfidandolo a esporsi a sua volta alla "trasparenza totale" pretesa dagli utenti del social network.
Il film si chiude in modo brusco, lasciando una sensazione di incompletezza, per tutte le domande che suscita sull'abuso della vita virtuale, a cui però non fornisce – forse volutamente – alcuna risposta, se non quella che emerge dalla scena finale: non possiamo più sottrarci a una vita sempre connessa, ma abbiamo il dovere di imparare a gestirla.

Francesca Ceccotti