La macchina che sa se menti

Il doppio uso dell'intelligenza artificiale capace di leggere la sincerità: controllo totale, o la fine della menzogna di chi comanda.

CONTROPOTERE

un libro di Alessio Farinella

La macchina che sa se menti

Il doppio uso dell'intelligenza artificiale capace di leggere la sincerità: lo strumento di controllo più potente mai creato, o la fine della menzogna di chi comanda

Alessio Farinella

Indice

Prefazione

Immagina una tecnologia capace di dire, con affidabilità quasi totale, se una persona sta mentendo. Ora immagina due mondi diversi in cui quella tecnologia esiste. Nel primo, un governo la usa per verificare la lealtà assoluta di ogni funzionario, di ogni oppositore, di ogni cittadino qualunque — un livello di controllo che nessun regime della storia ha mai avuto a disposizione. Nel secondo, sono i cittadini a usarla per verificare, in tempo reale, se chi li governa sta dicendo la verità — la fine di ogni menzogna politica impunita.

È la stessa identica tecnologia. Cambia solo chi la controlla, e con quali regole viene distribuita.

Questo libro parte da un punto di onestà che raramente viene fatto in questo tipo di discussioni: quella tecnologia, oggi, non esiste ancora con l'affidabilità necessaria a reggere nessuno dei due scenari — i sistemi di intelligenza artificiale più avanzati per il rilevamento della menzogna restano, allo stato attuale della ricerca, inaffidabili in modo significativo, a volte peggio del caso. Ma la sorveglianza di massa che raccontano i capitoli centrali di questo libro non ha bisogno di aspettare quella tecnologia per essere

già, oggi, una realtà concreta e documentata: riconoscimento facciale su database di decine di miliardi di volti, sistemi di controllo sociale già operativi su intere popolazioni, spyware venduto da aziende private a governi di ogni tipo.

Questo libro racconta cosa è già realtà, cosa resta ancora ipotesi tecnica, e perché la domanda su chi controllerà questa tecnologia quando diventerà più affidabile — non se arriverà, ma quando — è una delle più urgenti di tutta questa serie sull'intelligenza artificiale.

Capitolo 1 — Come funziona (e non funziona ancora) il rilevamento IA della sincerità

Cosa può incrociare un sistema che nessun essere umano riesce a incrociare

Un sistema di intelligenza artificiale può analizzare insieme, nello stesso istante, decine di segnali diversi da un testo o da una registrazione vocale: la scelta delle parole, il tono, la coerenza di una versione dei fatti raccontata più volte nel tempo, i tempi di risposta, persino minuscole variazioni nella voce. Nessun essere umano, per quanto addestrato, riesce a incrociare così tanti segnali contemporaneamente con la stessa costanza — è il motivo per cui l'idea di un'intelligenza

artificiale capace di riconoscere la menzogna sembra, a prima vista, plausibile e già a portata di mano.

Cosa dice davvero la ricerca scientifica, oggi

Ed è qui che questo libro deve essere onesto fin dal primo capitolo, prima ancora di raccontare gli scenari inquietanti dei capitoli successivi: **la scienza del rilevamento della menzogna, con o senza intelligenza artificiale, non ha ancora trovato un segnale affidabile e universale**. Decenni di ricerca psicologica non hanno mai identificato un comportamento — evitare lo sguardo, esitare, muoversi in un certo modo — che distingua in modo affidabile chi mente da chi dice la verità. Non esiste, allo stato delle conoscenze attuali, nemmeno un segnale fisiologico o neurale univocamente attribuibile all'atto di mentire.

Gli studi più recenti sui sistemi di intelligenza artificiale applicati a questo compito confermano che il problema resta irrisolto, e in alcuni casi mostrano risultati peggiori di quanto ci si aspetterebbe: uno studio ha misurato un sistema capace di riconoscere correttamente le bugie nell'85,8% dei casi, ma di riconoscere correttamente le verità solo nel 19,5% dei casi — un sistema, cioè, che tende a giudicare bugiardo quasi chiunque, comprese le persone sincere. In condizioni più vicine alla vita reale, dove la maggior parte delle persone testate dice effettivamente la verità, l'accuratezza di alcuni sistemi crolla fino al 15,9% —

un risultato peggiore di quanto si otterrebbe tirando a indovinare.

Perché questo capitolo non chiude il discorso, lo apre

Chi si aspettava, aprendo questo libro, la descrizione di una tecnologia già matura e pronta all'uso, potrebbe restare sorpreso da questa premessa cauta. Ma è una premessa necessaria: i ricercatori che studiano questo campo dicono esplicitamente «non ci siamo ancora», e servono miglioramenti sostanziali prima che un sistema del genere possa essere usato su larga scala con un'affidabilità reale.

Questo non significa che il resto di questo libro sia campato in aria. Significa due cose, entrambe importanti: primo, che la traiettoria generale di miglioramento dell'intelligenza artificiale raccontata nel resto di questa serie rende plausibile che, nei prossimi anni, l'affidabilità di questi sistemi migliori in modo significativo — la domanda su chi li controllerà, quando succederà, resta urgente da porsi già oggi. Secondo, e più importante per i capitoli che seguono: **la sorveglianza di massa non ha bisogno di aspettare un rilevatore di menzogne perfetto per essere già una realtà**. I prossimi capitoli raccontano cosa è già operativo, oggi, senza bisogno di quella tecnologia specifica — riconoscimento facciale, analisi comportamentale, controllo sociale su scala di intere popolazioni.

Capitolo 2 — La sorveglianza di massa già in corso

Non serve aspettare il futuro: è già qui

Il capitolo precedente ha chiarito che il rilevamento IA della menzogna resta, per ora, immaturo. Ma sarebbe un errore concludere che la sorveglianza di massa raccontata in questo libro sia ancora fantascienza. Gli strumenti descritti in questo capitolo — riconoscimento facciale su scala enorme, analisi comportamentale, punteggi di rischio individuali calcolati da un algoritmo — sono già pienamente operativi, oggi, non in un futuro ipotetico.

Un database più grande di quanto sembri possibile

L'azienda privata statunitense **Clearview AI** gestisce un database proprietario di oltre **50 miliardi di immagini facciali**, raccolte in gran parte da internet — social media, siti pubblici, qualunque fotografia accessibile online. Il servizio doganale statunitense (Customs and Border Protection) accede, tramite un proprio contratto con l'azienda, a un database ancora più ampio: oltre **60 miliardi di immagini** pubblicamente disponibili. Per dare un'idea della scala: sono numeri diverse volte superiori alla popolazione mondiale, perché ogni persona reale può comparire in decine di fotografie diverse raccolte dal sistema.

Cosa significa, in pratica, un punteggio di rischio automatico

Il caso più documentato e su scala più ampia di controllo sociale automatizzato si trova nella regione cinese dello **Xinjiang**, raccontato nel dettaglio nel prossimo capitolo. Ma il principio di fondo — assegnare a ogni persona un punteggio di rischio calcolato da un algoritmo, sulla base di dati raccolti senza che la persona ne sia pienamente consapevole — non è confinato a un solo paese: è un modello che, con intensità e garanzie diverse, si sta diffondendo in molte parti del mondo, incluse le democrazie occidentali, come racconta il Capitolo 4.

La differenza tra «poter fare qualcosa» e «avere il consenso per farlo»

Quello che rende questi strumenti particolarmente delicati non è solo la loro potenza tecnica, ma la velocità con cui si sono diffusi senza un dibattito pubblico proporzionato alla loro portata. Un database di miliardi di volti raccolti da internet, usato per identificare persone in tempo reale attraverso telecamere di sorveglianza, è un cambiamento enorme nel rapporto tra Stato e cittadino — ma è avvenuto, nella maggior parte dei paesi, attraverso contratti tra agenzie governative e aziende private, non attraverso leggi discusse e votate pubblicamente con la piena consapevolezza dei cittadini coinvolti.

Perché questo capitolo è il fondamento di tutto il resto del libro

I prossimi capitoli raccontano casi specifici — Cina, ma anche democrazie occidentali — e il mercato delle aziende private che vendono questi strumenti ai governi. Prima di entrare nei dettagli, questo capitolo pone la domanda di fondo che accompagna l'intero libro: se questi strumenti di sorveglianza sono già così diffusi oggi, con un rilevatore di menzogne ancora immaturo come mostrato nel Capitolo 1, cosa succederà quando quella tecnologia mancante verrà perfezionata e aggiunta a un sistema di controllo già esteso e già operativo?

Capitolo 3 — I regimi che usano l'IA per il controllo sociale

Il caso più documentato al mondo

Tra tutti i casi di uso dell'intelligenza artificiale per il controllo di una popolazione, quello della regione cinese dello **Xinjiang** è il più ampiamente documentato da organizzazioni indipendenti per i diritti umani, con anni di ricerche, testimonianze e analisi tecniche pubblicate. Vale la pena raccontarlo con precisione, perché mostra concretamente cosa succede quando gli strumenti descritti nel capitolo precedente vengono applicati senza alcun limite legale reale al controllo di un'intera popolazione.

Come funziona il sistema, nel dettaglio

Al centro del sistema di sorveglianza dello Xinjiang c'è una piattaforma chiamata **Integrated Joint Operations Platform (IJOP)**, descritta da Human Rights Watch come il «cervello» che coordina diversi sistemi di raccolta dati sul territorio: decine di milioni di telecamere a circuito chiuso, potenziate da riconoscimento facciale, analisi dell'andatura (il modo in cui una persona cammina, un dato biometrico difficile da nascondere) e riconoscimento vocale. La piattaforma profila fino a **1,8 milioni di residenti ogni giorno**, incrociando dati di localizzazione, cronologia degli acquisti e persino i consumi elettrici delle abitazioni, per assegnare a ciascuna persona un «livello di rischio» calcolato automaticamente.

Le conseguenze per le persone coinvolte

Secondo Human Rights Watch, gli uiguri — la minoranza musulmana turcofona che vive prevalentemente in questa regione — passano costantemente attraverso posti di controllo dotati di riconoscimento facciale. Diverse centinaia di migliaia di persone restano detenute nella regione, senza che, secondo la stessa organizzazione, vi sia stata alcuna assunzione di responsabilità per crimini contro l'umanità documentati da più fonti indipendenti nel corso degli anni.

Il rapporto sui diritti umani nel mondo pubblicato nel 2026 segnala un ulteriore rafforzamento di questo sistema nel corso dell'anno, con nuove politiche statali

che includono la raccolta di dati biometrici senza consenso, punteggi di rischio calcolati dall'intelligenza artificiale, e il monitoraggio continuo, ventiquattr'ore su ventiquattro, delle moschee della regione.

Perché questo caso conta per tutto il resto del libro

Il caso dello Xinjiang non è importante solo in sé, per la gravità di quanto documentato. È importante perché rappresenta, oggi, il punto più avanzato di quello che gli altri capitoli di questo libro descrivono come una possibilità più ampia: cosa succede quando gli strumenti di sorveglianza IA vengono applicati senza limiti legali reali, senza un potere giudiziario indipendente capace di fare da contrappeso, e senza libertà di stampa capace di documentarne gli abusi dall'interno. È il punto di riferimento — l'esempio più estremo e meglio documentato — rispetto a cui il prossimo capitolo misura quanto le democrazie occidentali si stiano, con intensità diverse, muovendo nella stessa direzione tecnologica.

Capitolo 4 — Le democrazie e la sorveglianza «per la sicurezza»

Non è solo una storia che riguarda i regimi autoritari

Sarebbe comodo, per chi vive in una democrazia occidentale, leggere il capitolo precedente e pensare che quella storia riguardi solo un altro tipo di paese, lontano e diverso. I dati raccontati in questo capitolo mostrano che non è così: anche i governi democratici stanno espandendo, rapidamente, gli stessi strumenti tecnologici — con garanzie diverse, ma con una direzione di marcia simile.

Il caso Clearview AI negli Stati Uniti

Negli Stati Uniti, diverse agenzie federali hanno stretto contratti con **Clearview AI**, l'azienda privata descritta nel Capitolo 2 che gestisce un database di oltre 50 miliardi di immagini facciali. L'agenzia per l'immigrazione e le dogane (**ICE**) utilizza il servizio tramite un contratto da **9,2 milioni di dollari**; il servizio doganale (**CBP**) ha firmato, nel febbraio 2026, un contratto per attività di «targeting tattico» e analisi delle reti; l'esercito statunitense ha rinnovato, a inizio 2026, un contratto specifico per le forze speciali. In totale, FBI, esercito, US Marshals Service e Dipartimento della Sicurezza Interna detengono insieme contratti con Clearview per quasi **10 milioni di dollari**.

Un dettaglio che pesa più delle cifre

Nel giugno 2026, ICE ha firmato il proprio contratto più grande di sempre con Clearview AI, da **3,75 milioni di dollari** — nello stesso periodo in cui il Dipartimento della Sicurezza Interna ha eliminato una propria policy interna che regolava la supervisione sull'uso dello strumento. È un dettaglio che vale più di qualunque cifra da solo: mentre l'uso dello strumento si espande, il meccanismo di controllo interno pensato per vigilare su quell'uso si riduce, non si rafforza.

Perché nelle democrazie il dibattito resta comunque diverso

Va detto con onestà, per non appiattire situazioni molto diverse tra loro: nelle democrazie occidentali questi contratti sono, almeno in parte, documentabili tramite richieste di accesso agli atti, inchieste giornalistiche, interrogazioni parlamentari — gli stessi strumenti che hanno permesso di ricostruire i dati citati in questo capitolo. Nello Xinjiang raccontato nel capitolo precedente, un simile livello di documentazione indipendente è, di fatto, impossibile da ottenere dall'interno. La differenza tra i due contesti è reale e importante.

Ma la direzione preoccupa comunque

Detto questo, il punto centrale di questo capitolo resta: la direzione di marcia — più contratti, più dati raccolti, meno supervisione interna dichiarata — è la stessa in entrambi i contesti, anche se la velocità e le garanzie

legali sono diverse. La domanda che il resto di questo libro pone non è «le democrazie diventeranno come lo Xinjiang» — sarebbe una semplificazione ingiusta. La domanda è: quali garanzie concrete, verificabili, e non semplicemente dichiarate, impediscono che la stessa traiettoria tecnologica produca, nel tempo, risultati sempre più simili, indipendentemente dalle intenzioni dichiarate all'inizio?

Capitolo 5 — Il lato opposto: la fine della menzogna di chi comanda

La stessa tecnologia, capovolta

Fin qui, questo libro ha raccontato solo un lato della storia — quello più documentato, perché già in gran parte realtà. Ma il titolo di questo libro parla di un doppio uso, e questo capitolo racconta l'altro lato: cosa succederebbe se gli stessi strumenti descritti finora — analisi del linguaggio, riconoscimento di pattern, verifica incrociata di informazioni — venissero usati non per controllare i cittadini, ma per verificare la sincerità di chi li governa.

Un potere che oggi non esiste, in nessuna democrazia

Nessuna democrazia, per quanto avanzata, ha mai avuto a disposizione uno strumento capace di verificare, con affidabilità reale e in tempi rapidi, se una dichiarazione pubblica di un politico corrisponde al

vero. Il fact-checking esiste, ma è lento, costoso, dipende dal lavoro umano di giornalisti e ricercatori, e arriva quasi sempre dopo che la dichiarazione ha già raggiunto il proprio pubblico e prodotto il proprio effetto. Un sistema di intelligenza artificiale capace di incrociare, in tempo reale, una dichiarazione pubblica con l'insieme dei dati disponibili — documenti, dichiarazioni precedenti, dati economici verificabili — potrebbe, in teoria, ridurre drasticamente quel ritardo.

Perché conta più della tecnologia in sé

Il Capitolo 1 ha già chiarito che questa tecnologia, nella sua forma più ambiziosa, non è ancora matura. Ma vale la pena immaginare lo scenario in cui lo diventi, perché aiuta a capire meglio la posta in gioco descritta nel resto del libro. Un sistema del genere, se reso disponibile ai cittadini in modo aperto e verificabile — non controllato da un singolo governo o da una singola azienda — potrebbe rappresentare uno degli strumenti di responsabilizzazione del potere più potenti mai esistiti: la possibilità, per chiunque, di verificare la sincerità di chi lo governa con la stessa facilità con cui oggi si verifica un dato su un motore di ricerca.

Il rischio di un potere ancora più concentrato

Ma lo stesso identico strumento, se sviluppato e controllato da chi già oggi detiene il potere — un governo,

un'azienda alleata a un governo — non produce automaticamente questo effetto liberatorio. Anzi: potrebbe diventare un ulteriore strumento nelle mani di chi comanda, usato selettivamente per accusare gli avversari politici di menzogna mentre si proteggono le proprie dichiarazioni da un controllo equivalente. La tecnologia, da sola, non decide quale dei due scenari si realizzerà.

Cosa determina davvero l'esito

Il prossimo capitolo affronta esattamente questo punto: perché la proprietà e le regole di accesso a questi sistemi contano più della loro capacità tecnica. Un sistema di verifica della sincerità aperto, verificabile da chiunque nel proprio funzionamento, distribuito su più attori indipendenti, produce un effetto molto diverso da un sistema chiuso, proprietario, controllato da un singolo governo o da una manciata di aziende. È la stessa domanda che attraversa l'intera serie «Intelligenza Artificiale» di questa collana, applicata qui a uno degli usi più delicati immaginabili per questa tecnologia.

Capitolo 6 — Chi controlla l'algoritmo controlla la narrazione

Una domanda più importante della tecnologia stessa

I capitoli precedenti hanno raccontato due scenari opposti prodotti dalla stessa tecnologia: controllo totale o trasparenza radicale. Questo capitolo spiega perché la variabile decisiva non è quanto la tecnologia sia avanzata, ma chi la possiede e con quali regole di accesso viene distribuita.

Un esempio concreto per capirlo

Immagina un sistema capace di verificare la sincerità di una dichiarazione pubblica, sviluppato e gestito da un'unica azienda privata, con un accordo esclusivo con un solo governo. Quel sistema potrebbe tecnicamente funzionare alla perfezione — e comunque produrre un risultato pericoloso, perché chi lo controlla decide quali dichiarazioni sottoporre a verifica, quali risultati rendere pubblici, e quali lasciare nell'ombra. Un algoritmo «neutro» sulla carta diventa, nella pratica, uno strumento di parte nelle mani di chi decide come e quando utilizzarlo.

Il parallelo con il resto di questa collana

Questo principio non è nuovo, ed è il filo conduttore di gran parte della collana Contropotere: il potere raramente si esercita vietando apertamente qualcosa.

Si esercita più spesso controllando l'infrastruttura attraverso cui l'informazione passa — chi possiede i media, chi controlla le agenzie di rating, chi decide le condizioni di un prestito internazionale. La tecnologia raccontata in questo libro aggiunge un nuovo livello a questo stesso meccanismo: non solo chi controlla cosa viene detto, ma chi controlla la capacità stessa di verificare se quello che viene detto è vero.

Il caso di un sistema distribuito, come alternativa

Il Capitolo 10 di [[Libro_Ultima_Invenzione]] descrive, tra gli elementi del «Piano A» per una transizione gestita verso la superintelligenza, il principio della trasparenza totale della ricerca e della distribuzione del potere su più aziende e più paesi, invece che la concentrazione in un solo laboratorio o in un solo governo. Lo stesso principio, applicato alla tecnologia specifica raccontata in questo libro, indicherebbe una strada diversa da quella oggi prevalente: un sistema di verifica della sincerità sviluppato con codice aperto, verificabile da più organizzazioni indipendenti in più paesi, con dati di addestramento pubblici e controllabili — invece di un sistema chiuso, proprietario, nelle mani di un solo attore.

Perché, oggi, siamo lontani da questo scenario

I capitoli precedenti hanno mostrato che gli strumenti di sorveglianza già operativi oggi — da Clearview AI alle piattaforme di controllo sociale — seguono quasi ovunque il modello opposto: aziende private, spesso senza obblighi di trasparenza pubblica sul proprio funzionamento interno, che vendono i propri strumenti a governi tramite contratti la cui esistenza stessa, in molti casi, emerge solo grazie a inchieste giornalistiche indipendenti. È la stessa dinamica di concentrazione di potere raccontata nel resto di questa serie — applicata qui a una delle tecnologie potenzialmente più delicate mai sviluppate.

Capitolo 7 — La privacy come diritto in via di sparizione

Un diritto che si erode senza un momento preciso di rottura

A differenza di altri diritti, la cui violazione è spesso un evento riconoscibile — un arresto ingiusto, una censura esplicita — l'erosione della privacy raccontata in questo libro avviene per accumulo, senza un singolo momento in cui qualcuno possa dire con certezza «da qui la mia privacy è finita». Ogni singolo contratto tra un'agenzia governativa e un'azienda di sorveglianza, ogni nuova telecamera con riconoscimento facciale

installata, ogni database di volti che cresce di qualche milione di immagini, sembra, preso da solo, un piccolo passo. Sommati insieme, come mostrano i capitoli precedenti, disegnano un cambiamento enorme.

Cosa significa, concretamente, vivere dentro questo sistema

Prova a immaginare la tua giornata attraverso gli strumenti descritti in questo libro. Le telecamere che incontri camminando per strada, in molte città, possono già oggi essere collegate a sistemi di riconoscimento facciale simili a quelli descritti nei capitoli precedenti. Le tue comunicazioni digitali — messaggi, email, chiamate — potrebbero, in linea di principio tecnico, essere già oggi analizzabili su larga scala dagli stessi tipi di sistemi linguistici descritti nel Capitolo 1, anche se con l'affidabilità ancora limitata di cui parla quel capitolo. Non significa che ogni tuo messaggio venga davvero letto da un funzionario — significa che l'infrastruttura tecnica per farlo, se qualcuno decidesse di usarla in quel modo, esiste già, in gran parte, oggi.

Il problema del consenso che non è mai stato dato

Nessun cittadino ha mai votato esplicitamente per l'esistenza di un database da 50 miliardi di immagini facciali raccolte da internet, descritto nel Capitolo 2. Nessuno ha firmato un consenso specifico perché le proprie fotografie pubbliche sui social media finissero

in un archivio consultabile da agenzie governative attraverso un contratto commerciale. Questo è, forse, il problema più profondo raccontato in questo capitolo: la tecnologia si è diffusa più in fretta della capacità delle istituzioni democratiche di regolarla, e il consenso dei cittadini — quando esiste — è quasi sempre implicito, dedotto da termini di servizio che quasi nessuno legge per intero, non liberamente e consapevolmente espresso.

Perché questo non è un discorso astratto sui «diritti»

È facile liquidare le preoccupazioni sulla privacy come un discorso astratto, lontano dalla vita quotidiana concreta delle persone. Ma la privacy, storicamente, non è mai stata solo una questione di comodità personale: è stata, in molti momenti della storia, la condizione minima necessaria perché un'opposizione politica potesse organizzarsi, un giornalista potesse proteggere una fonte, un cittadino potesse dissentire senza rischiare conseguenze immediate. Un mondo dove ogni comunicazione può essere analizzata, anche solo in linea di principio tecnico, cambia il calcolo di rischio di chiunque voglia esprimere un'opinione scomoda — anche se quella capacità di analisi non viene mai effettivamente esercitata contro di lui.

Capitolo 8 — Le aziende private che vendono sorveglianza agli Stati

Un mercato che pochi conoscono, che riguarda tutti

Dietro gran parte degli strumenti di sorveglianza descritti in questo libro non ci sono agenzie governative che sviluppano tecnologia in proprio, ma aziende private che la progettano, la vendono, e la aggiornano su base commerciale — spesso a più governi contemporaneamente, incluso a paesi con storici di diritti umani molto diversi tra loro. È un mercato con poca trasparenza pubblica, regolato in modo debole rispetto alla sua reale portata.

Il caso NSO Group e lo spyware Pegasus

L'esempio più documentato è quello dell'azienda israeliana **NSO Group**, produttrice dello spyware **Pegasus** — un software capace di infiltrarsi in un telefono e accedere a messaggi, chiamate, foto, posizione, spesso senza che il proprietario del dispositivo debba compiere alcuna azione per attivarlo. NSO Group dichiara di vendere il proprio prodotto esclusivamente ad agenzie governative, per finalità dichiarate di contrasto al crimine e al terrorismo.

Almeno **11 governi** risultano clienti documentati di NSO, tra cui Azerbaigian, Bahrein, Kazakistan, Messico, Marocco, Ruanda, Arabia Saudita, Ungheria, India,

Togo ed Emirati Arabi Uniti — un elenco che comprende sia democrazie che regimi autoritari. Secondo altre stime, circa **40 paesi** hanno avuto accesso allo strumento nel corso degli anni, con persone bersaglio identificate in oltre **50 paesi** nel mondo.

Chi è stato colpito, secondo le inchieste indipendenti

L'inchiesta giornalistica internazionale nota come «Pegasus Project», pubblicata nel 2021, ha rivelato l'uso dello spyware contro giornalisti, avvocati, attivisti per i diritti umani e politici in decine di paesi — non solo sospetti di reati gravi, come dichiarato dall'azienda, ma anche voci critiche verso i governi che avevano acquistato lo strumento. Un nuovo filone di inchiesta, avviato più di recente, ha continuato ad ampliare queste rivelazioni, confermando che l'uso improprio dello strumento non è stato un episodio isolato nel tempo.

Un settore che cambia proprietà, non natura

Nell'autunno del **2025**, un gruppo privato di investitori statunitensi ha acquisito NSO Group. Il cambio di proprietà non ha, di per sé, alcun effetto automatico sulle pratiche commerciali dell'azienda o sui controlli — reali o dichiarati — sulla vendita del proprio prodotto a governi con un track record documentato di abusi.

Perché questo mercato dovrebbe preoccupare anche chi non ha nulla da nascondere

L'obiezione più comune a questo tipo di preoccupazioni è «chi non ha nulla da nascondere non ha nulla da temere». Ma le persone colpite dallo spyware Pegasus, secondo le inchieste citate, non erano criminali: erano giornalisti che facevano il proprio lavoro, avvocati che difendevano i propri clienti, attivisti che esercitavano un diritto di dissenso legittimo in molte democrazie. Un mercato che vende strumenti di sorveglianza di questa potenza a chiunque possa permetterseli, con controlli deboli su come vengono effettivamente utilizzati, riguarda direttamente la libertà di stampa e il dissenso politico — pilastri che, storicamente, hanno beneficiato anche chi non li ha mai esercitati direttamente, semplicemente vivendo in una società dove altri potevano farlo per conto di tutti.

Capitolo 9 — Le obiezioni, trattate con onestà

«Questi strumenti servono davvero a fermare crimini gravi»

È l'obiezione più forte, e va riconosciuta con onestà: strumenti come il riconoscimento facciale e l'analisi dei dati hanno contribuito, in casi documentati, a identificare autori di reati gravi, a prevenire attacchi

terroristici, a ritrovare persone scomparse. Le stesse agenzie citate nel Capitolo 4 — FBI, servizio doganale, esercito — hanno compiti legittimi di sicurezza pubblica che nessuno, in questo libro, mette in discussione in linea di principio. Il problema non è l'esistenza di questi strumenti in assoluto, ma l'assenza di controlli proporzionati alla loro potenza — un punto diverso, e più preciso, di un generico «questi strumenti sono un male».

«Chi non ha nulla da nascondere non ha nulla da temere»

È probabilmente l'obiezione più diffusa nel dibattito pubblico, e merita una risposta precisa piuttosto che un rifiuto sbrigativo. Il problema di questo argomento, come mostra il Capitolo 8 a proposito dei bersagli reali dello spyware Pegasus, è che presuppone che il potere che detiene questi strumenti li userà sempre in modo giusto e proporzionato. La storia, incluse le inchieste citate in questo libro, mostra ripetutamente il contrario: giornalisti, avvocati e attivisti — persone che esercitavano diritti legittimi, non criminali — sono stati bersaglio di questi stessi strumenti. «Non avere nulla da nascondere» protegge solo se chi detiene il potere di sorveglianza lo esercita sempre con giustizia — una condizione che nessun sistema politico, storicamente, ha mai garantito in modo permanente e senza eccezioni.

«Le aziende occidentali sono comunque più controllate di quelle di altri paesi»

È un'obiezione parzialmente fondata: le democrazie occidentali dispongono, come mostra il Capitolo 4, di strumenti di controllo — accesso agli atti, stampa libera, tribunali indipendenti — che permettono almeno di documentare pubblicamente contratti come quelli di Clearview AI con le agenzie federali statunitensi. Questo è un vantaggio reale rispetto al caso dello Xinjiang raccontato nel Capitolo 3. Ma la stessa scelta, documentata nel Capitolo 4, di eliminare una policy di supervisione interna proprio mentre un contratto di sorveglianza raggiungeva il proprio valore più alto, mostra che questo vantaggio strutturale non è una garanzia automatica: va difeso attivamente, non dato per scontato in eterno.

«Se non sviluppiamo noi questi strumenti, lo faranno altri comunque»

È lo stesso argomento, applicato qui alla sorveglianza, che il Capitolo 3 di [[Libro_Ultima_Invenzione]] descrive a proposito della corsa generale all'intelligenza artificiale: la competizione tra paesi rende difficile per un singolo governo rinunciare unilateralmente a una tecnologia, per timore che i rivali la sviluppino comunque, ottenendo un vantaggio. È un argomento reale, che spiega perché la rinuncia unilaterale sia poco realistica — ma non risponde alla domanda su quali regole e controlli dovrebbero comunque accompagna-

re lo sviluppo di questi strumenti, indipendentemente da chi li costruisce per primo.

Cosa resta, dopo aver ascoltato queste obiezioni

Riconoscere queste obiezioni non significa concludere che la sorveglianza descritta in questo libro sia priva di rischi. Significa evitare la scorciatoia opposta: dipingere ogni singolo strumento di sicurezza pubblica come un passo verso un regime totalitario. La realtà, più scomoda e più utile da tenere a mente, è quella descritta nel Capitolo 6: la tecnologia in sé non decide l'esito. Lo decidono le regole, i controlli, e chi ha il potere reale di farli rispettare — il tema del prossimo capitolo.

Capitolo 10 — Cosa si potrebbe cambiare

Obblighi di trasparenza sui contratti di sorveglianza

Una prima misura concreta, già proposta da diverse organizzazioni per i diritti digitali, è imporre per legge la pubblicazione obbligatoria di ogni contratto tra agenzie governative e aziende private di sorveglianza — inclusi valore economico, finalità dichiarate, e meccanismi di controllo previsti. Oggi, come mostra il Capitolo 4, gran parte di questa informazione emerge

solo grazie a inchieste giornalistiche indipendenti, non da un obbligo sistematico di trasparenza.

Supervisione giudiziaria indipendente, non solo interna

Il dettaglio più preoccupante raccontato nel Capitolo 4 — l'eliminazione di una policy di supervisione interna proprio mentre un contratto di sorveglianza cresceva di valore — mostra il limite dei controlli lasciati alla stessa agenzia che utilizza lo strumento. Una proposta più solida, sostenuta da giuristi specializzati in diritti digitali, prevede l'obbligo di un'autorizzazione giudiziaria indipendente prima di ogni utilizzo su larga scala di strumenti di riconoscimento facciale o analisi comportamentale da parte di agenzie governative — sul modello delle autorizzazioni già richieste per altre forme invasive di sorveglianza in molti sistemi legali.

Regole internazionali sulla vendita di spyware

Il Capitolo 8 ha mostrato come lo spyware Pegasus sia arrivato, secondo le stime più ampie, in circa 40 paesi, con bersagli documentati che includevano giornalisti e attivisti oltre ai criminali dichiarati come target ufficiale. Diverse organizzazioni internazionali propongono un regime di controllo delle esportazioni per questo tipo di software, simile a quello già esistente per le armi convenzionali — con l'obbligo di verificare il rispetto dei diritti umani del paese acquirente prima

di autorizzare la vendita, e sanzioni reali per le aziende che vendono comunque a governi con un track record documentato di abusi.

Un «diritto all'oblio algoritmico» per i database biometrici

Il Capitolo 2 ha mostrato la scala enorme dei database di volti raccolti da aziende come Clearview AI, spesso da fotografie pubbliche online senza consenso esplicito. Alcune proposte legislative, già discusse in diverse giurisdizioni, prevedono il diritto per ogni cittadino di richiedere la rimozione della propria immagine da questi database privati — un principio simile a quello già esistente per altri tipi di dati personali in alcune normative sulla privacy, ma non ancora applicato in modo sistematico ai database biometrici commerciali.

Standard aperti per i sistemi di verifica della sincerità

Il Capitolo 6 ha spiegato perché la proprietà e le regole di accesso a un futuro sistema di verifica della sincerità conterebbero più della sua capacità tecnica. Alcuni ricercatori propongono, fin da ora, di stabilire standard tecnici aperti per questo tipo di sistemi — codice verificabile pubblicamente, dati di addestramento controllabili da più organizzazioni indipendenti — prima che la tecnologia raggiunga la maturità descritta come possibile nel Capitolo 1, invece di aspettare che il mer-

cato si consolidi attorno a sistemi chiusi e proprietari difficili da correggere in un secondo momento.

Il filo comune

Come per gli altri titoli di questa serie, nessuna di queste misure risolve da sola il problema descritto in questo libro. Ma condividono lo stesso principio: la tecnologia della sorveglianza si sta sviluppando più in fretta delle regole pensate per governarla, e recuperare quel ritardo richiede scelte deliberate, non l'attesa che il problema si risolva da solo.

Capitolo 11 — Cosa puoi fare tu, adesso

Verificare la propria impronta digitale pubblica

Un primo passo concreto, alla portata di chiunque, è verificare quali proprie fotografie sono pubblicamente accessibili online — social media, siti professionali, articoli di giornale — perché sono esattamente il tipo di materiale che alimenta database come quello descritto nel Capitolo 2. Non è possibile eliminare del tutto la propria presenza online in un mondo connesso, ma ridurre consapevolmente quello che è pubblicamente accessibile, quando possibile, riduce la quantità di materiale disponibile per questo tipo di raccolta.

Informarsi sui contratti di sorveglianza della propria area

Molte richieste di accesso agli atti relative a contratti di sorveglianza locale — polizia municipale, sistemi di videosorveglianza cittadina — sono già oggi possibili in diversi paesi attraverso normative sulla trasparenza amministrativa. Organizzazioni per i diritti digitali pubblicano spesso guide pratiche su come effettuare queste richieste, anche per chi non ha competenze legali specifiche.

Sostenere il giornalismo investigativo indipendente

Gran parte di quello che sappiamo sui temi raccontati in questo libro — dal Pegasus Project alle inchieste sui contratti Clearview AI — esiste grazie al lavoro di consorzi giornalistici indipendenti che hanno investito anni di ricerca per documentare pratiche che nessun governo o azienda coinvolta avrebbe reso pubbliche volontariamente. Seguire, condividere e sostenere economicamente questo tipo di giornalismo, spesso pubblicato in accesso aperto, è un modo concreto per mantenere questo tipo di controllo indipendente attivo nel tempo.

Fare pressione politica sulle proposte del capitolo precedente

Le misure discusse nel Capitolo 10 — trasparenza sui contratti, supervisione giudiziaria indipendente,

regole sull'export di spyware — richiedono attenzione politica continua, non un singolo momento di indignazione pubblica. Chiedere esplicitamente a chi ci rappresenta quale posizione ha su questi temi specifici, e seguire nel tempo come votano su proposte di legge concrete quando vengono discusse, è un modo per mantenere la pressione anche dopo che la notizia del momento è passata.

Condividere questo libro

Se questo libro ti ha aiutato a distinguere cosa è già realtà da cosa resta ancora ipotesi tecnica in questo campo, condividilo con chi, nella tua vita, ne parla senza questa distinzione — sia chi minimizza il problema perché «quella tecnologia non esiste ancora davvero», sia chi lo esagera oltre quanto i fatti oggi permettono di sostenere. In entrambi i casi, la precisione sui fatti resta lo strumento più utile per formarsi un giudizio solido, invece che basato sulla paura o sulla rassicurazione di comodo.

Nota sulla trasparenza nell'uso dell'intelligenza artificiale

Questo libro è stato scritto con il supporto di strumenti di intelligenza artificiale, usati per la ricerca preliminare delle fonti, la prima stesura dei testi a partire da una scaletta e da indicazioni editoriali definite dall'autore, e la revisione linguistica e strutturale.

Restano interamente umane: la scelta del tema e la tesi del libro, la verifica di ogni fatto, cifra e citazione contro una fonte primaria o istituzionale prima della pubblicazione, la decisione editoriale finale su cosa viene pubblicato o corretto, e la responsabilità editoriale dei contenuti — che resta in capo all'autore, mai allo strumento di intelligenza artificiale utilizzato.

Questa nota risponde agli obblighi di trasparenza previsti dall'art. 50 del Regolamento (UE) 2024/1689 (AI Act), applicabile dal 2 agosto 2026.

Se trovi un errore, una fonte imprecisa o un'affermazione che ritieni non verificata correttamente, scrivi a redazione@contropotere.com — ogni segnalazione fondata porta a una correzione pubblica del testo. Questo libro fa parte della collana **Contropotere**: gli altri titoli sono disponibili gratuitamente su **contropotere.com**.