19 Marzo 2024

Smart city o modelli di sorveglianza integrata? Il caso eclatante di Trento

Di Enrico Pelino

Abstract

Raccolta di dati acquisiti da microfoni, telecamere, piattaforme di condivisione video, social network, trattati con processi di intelligenza artificiale. Il recentissimo caso dei dispositivi di controllo installati nella città di Trento per finalità di ricerca costituisce l'espressione più visibile, e per molti versi più stupefacente, di una tendenza che si manifesta diffusamente altrove in Italia in forme più miti e più carsiche, ma non meno insidiose, quella cioè di leggere l'attuale ampia disponibilità di tecnologia in chiave prevalente di presidio di pubblica sicurezza, e concepire quest'ultima in termini di sorveglianza generalizzata. In tal modo, la "smart city", da luogo di cittadinanza rafforzata, si trasforma in un contesto distopico, nel quale i diritti sono minorati. Come si arriva a questi modelli, quanto conta la leggerezza e qual è il ruolo fondamentale dei consulenti per prevenire o correggere le derive? L'articolo muoverà dalla recente ordinanza-ingiunzione del Garante per la protezione dei dati personali nei confronti del comune di Trento, assunta come case study per tracciare un'analisi di raggio più ampio sui temi della sorveglianza, della consapevolezza giuridica, dell'assetto delle tutele.

Indice

Microfoni in città

> Partiamo da un caso eclatante, perché vicino a noi, emotivamente e geograficamente, ossia dove non ci attenderemmo di trovarlo. Dimentichiamo per un attimo il programma cinese Skynet, la rete statale di videosorveglianza capillare che individua attraverso sistemi automatizzati determinati pattern comportamentali. Eccoci invece in Italia, a Trento. È qui che il Comune attiva due sistemi di intelligenza artificiale, Marvel e Protector, alimentati da captazione di voci, immagini, post.

Il termine, *trendy*, per l'iniziativa è "*smart urban security*", ma l'ossatura di base appare più in stile vecchia DDR: Marvel, acronimo di "Multimodal Extreme Scale Data Analytics for Smart Cities Environments", necessita infatti di microfoni collocati in vari punti della città per intercettare le conversazioni dei passanti e di una rete di videocamere per raccogliere loro momenti di vita. L'idea è di applicare un sistema di intelligenza artificiale sui contenuti di conversazioni reali e su situazioni urbane di interazione sociale, al fine di ottenere il riconoscimento intelligente di scene audiovisive e il

rilevamento di eventi.

Il complesso di videocamere si trova già in loco, ma per una finalità diversa, ossia per ragioni ordinarie di sicurezza urbana, non viene tuttavia ritenuto necessario precisare nell'informativa di primo livello la nuova finalità. Non è un dettaglio giuridico marginale, e lo stesso Comune dovrà poi ammettere il "*possibile fraintendimento ingenerato nei cittadini conseguente al fatto che non sarebbe risultata chiara la finalità del trattamento dei dati*". Né gli interessati, osserva il Garante, "*sono stati messi in condizione di comprendere che anche il contenuto delle proprie conversazioni sarebbe stato acquisito e trattato*". Eppure, il punto è essenziale, considerato che "*la raccolta dei flussi audio e video necessari per lo sviluppo degli algoritmi non avviene*", come dichiarato dal Comune, "*unicamente in ambienti controllati e con il coinvolgimento di persone che hanno prestato il proprio consenso alla partecipazione al progetto, ma anche in ambiente urbano, ossia tramite le telecamere ed i microfoni installati in alcune piazze e vie della città*".

Protector, ossia "PROTECTing places of wORship", è similare, ma calibrato sul riconoscimento di situazioni di minaccia a luoghi di culto. Anche in questi casi vengono catturate immagini di videosorveglianza, elaborate poi da un sistema di intelligenza artificiale che si propone di individuare situazioni "anomale", espressioni di criminalità e presunte "devianze". Oltre alle immagini di videosorveglianza vengono acquisiti i contenuti di post pubblicati su social media (Twitter/X) e piattaforme di condivisione video (YouTube). I componenti automatici del sistema individuerebbero i messaggi di "odio religioso", analizzerebbero le emozioni suscitate e sarebbero in grado di rilevare la disinformazione legata a fake news religiose. "*Le componenti di analisi per i social media impiegano modelli di linguaggio basati su Transformer*". Un esperimento dunque assolutamente contemporaneo. I programmi fortunatamente non utilizzano sistemi di riconoscimento biometrico.

La responsabilità giuridica

Si tratta in definitiva di due ricerche molto avanzate, collocabili nell'area concettuale della "**polizia predittiva**" per l'evidente supporto a interventi anticipatori nella repressione di attività criminose. Ciò emerge sia dalla natura stessa dei progetti sia dalle dichiarazioni rese, come la seguente: "*Le funzionalità sviluppate tramite i progetti di ricerca saranno rese fruibili nell'utilizzo da parte del Corpo di polizia locale degli impianti di videosorveglianza di proprietà comunale*".

> Marvel e Protector registrano **pochi precedenti in un Paese dell'Europa occidentale** e incidono, evidentemente, su una serie di diritti fondamentali, quali la protezione della vita privata da ingerenze, la tutela delle comunicazioni interpersonali, la libertà di circolare liberamente, di esprimersi liberamente, di associarsi liberamente per strada. Paradossalmente (considerati gli obiettivi dei progetti), è proprio il diritto a camminare serenamente in città a risultare compresso.

I diritti fondamentali attinti compongono un'architettura di tutele che contribuiscono a definire alcuni connotati distintivi del nostro assetto di libertà individuali rispetto ad esperienze di altre aree geografiche che avvertiamo come lontane e non desiderabili. Ed è proprio questo che rende il caso di Trento così rilevante, la sensazione cioè, almeno in chi scrive, che abbia notevolmente accorciato certe distanze, pur essendo animato da ottime intenzioni.

Il Comune, che non sarebbe assolutamente dotato di strumenti tanto sofisticati di elaborazione, riceve gli appositi algoritmi di intelligenza artificiale e il necessario supporto di *know-how* da un istituto di ricerca privato, assai qualificato nell'analisi dei dati, la Fondazione Bruno Kessler. Di suo il Comune mette invece l'infrastruttura di videocamere **e la responsabilità giuridica**, assumendo su di sé la titolarità del trattamento, nonostante le complessità intrinseche di comprensione dell'impatto giuridico dei due esperimenti. L'analisi del Garante rivelerà infatti una profonda impreparazione o sottovalutazione di punti essenziali.

È importante evidenziare l'elemento di affidamento da parte del Comune al partner tecnologico e di ulteriore affidamento alla cornice europea delle iniziative. Marvel e Protector sono finanziati infatti dalla Commissione europea e si collocano perciò in un quadro percepito come istituzionale d'eccellenza.

Possiamo oggi parlare dell'intera vicenda al passato, perché il Garante vi ha posto sostanzialmente fine con un'ordinanza-ingiunzione dell'11 gennaio 2024 [9977020], vietando il trattamento dei dati essenziali di approvvigionamento dei due progetti, ossia registrazioni video o audio, messaggi/commenti ottenuti da reti sociali, informazioni relative alle reti di utenti sulla piattaforma Twitter/X, e disponendo anche la cancellazione di quelli acquisiti. Era un provvedimento atteso, è ben scritto ed è di grande interesse per articolazione e motivazioni. Un terzo esperimento predittivo, Precrisis, ossia "PRotECting public spaces thRough Integrated Smarter Innovative Security", non risulta ancora attivato.

La fascinazione dell'idea di *smart city*

> Che cosa è dunque emerso dalle verifiche del Garante? È risultata l'inidoneità delle informative specifiche sui due programmi (solo a titolo di esempio, rispetto al progetto Marvel, nell'informativa di primo livello "*gli interessati non sono stati messi in condizione di comprendere che anche il contenuto delle proprie conversazioni sarebbe stato acquisito e trattato ai fini del progetto*" e in quella di secondo livello, peraltro non agevolmente collegata con la prima, "*si omette di specificare che l'audio potrebbe riguardare anche le conversazioni intercorse tra le persone presenti sulla pubblica via, aspetto che è certamente da considerarsi uno degli impatti più consistenti del trattamento*").

È altresì risultato che la base giuridica era stata individuata in generici compiti di "sviluppo culturale, sociale ed economico della popolazione", che la DPIA, lungi dal descrivere Marvel e Protector e perfino dal menzionarli, non ha neppure toccato i temi essenziali della proporzionalità e della necessità del trattamento, vale a dire i presupposti essenziali dell'incombente (che non va ridotto a mera ricognizione di misure informatiche). Ma soprattutto, **è emerso che il Comune non credeva di trattare dati personali**, ed è certamente il punto più drammatico.

Il quadro restituito dall'istruttoria è dunque quello non solo di una radicale violazione dei fondamentali della normativa, nonostante la presenza di un DPO, ma anche di una radicale sottovalutazione. Il Garante ha comminato una sanzione tutto sommato assai blanda (50.000 euro, dimezzabili con definizione anticipata), rispetto al rilievo della vicenda e ai finanziamenti ottenuti dall'Ente. Non sembrerebbero essere stati emessi provvedimenti nei confronti del cervello tecnologico dei progetti, la Fondazione, che si trova del resto fuori traiettoria in virtù del suo ruolo di responsabile del trattamento e non parrebbe avere ricevuto contestazioni ai sensi dell'art. 32 GDPR in merito all'adozione delle tecniche di anonimizzazione, poi non risultate tali.

Ora, la circostanza che il Comune si sia dichiarato all'oscuro di trattare dati personali è quella che colpisce di più, perché ciò ha compromesso completamente la chiave essenziale di lettura giuridica dell'intera architettura posta in essere. Eppure, il trattamento di dati personali era palese, non solo perché costituisce il presupposto di una serie di attività, non da ultimo la qualificazione appunto della Fondazione come responsabile del trattamento, ma anche già per il fatto che i nomi, **in chiaro**, degli autori dei messaggi pubblicati sulla piattaforma Twitter (X) sono stati condivisi con la Polizia locale di Trento, con i colleghi di Anversa e con il Ministero dell'Interno della Bulgaria.

E, a parte questo, anche negli altri trattamenti in cui sono state utilizzate tecniche di offuscamento appare evidente il trattamento di dati personali e l'insufficienza della pretesa anonimizzazione. Non basta, infatti, oscurare un volto, alterare una voce o coprire un nome utente, come è stato fatto, se il resto delle immagini permette l'individuazione o se i contenuti di audio e post sono in chiaro. I contenuti di conversazioni possono contenere di tutto e rivelare di tutto: nomi, vicende, coordinate

identificative. Ugualmente, è elemento acquisito, dopo oltre un quarto di secolo di normativa sulla protezione dei dati personali, che, al di là di un volto oscurato, un filmato può contenere innumerevoli elementi che rendono riconoscibile un soggetto: corporatura, abbigliamento, gesti, camminata, posizione occupata nella scena, percorsi frequentati, solo per citarne alcuni.

La sensazione tuttavia non è tanto che queste nozioni di base fossero ignorate, ma che siano state sottovalutate, che abbia cioè prevalso la fascinazione del concetto di "*smart city*". Date a qualsiasi amministrazione fondi dell'Unione, il libero accesso alla tecnologia e il supporto di strutture di primo livello nella *data science* – amalgama davvero esplosivo – e accadrà probabilmente che esigenze di sicurezza diffuse, a torto o a ragione, nella cittadinanza saranno affrontate introducendo esperimenti di sorveglianza, prove tecniche di polizia predittiva, controllo su pattern interpretabili come precursori di tensioni sociali. È **la scelta più semplice e insieme quella che produce maggiore impressione sui soggetti amministrati**, perché intercetta le corde della paura e offre a problemi che derivano da cause complesse, quali le difficoltà di integrazione sociale, la marginalizzazione, il degrado urbano, una risposta pronta all'uso, la magia predittiva dell'algoritmo, che non affronta le cause ma promette reprimere in anticipo gli effetti.

Esiste alla base, in definitiva, una questione che potremmo definire "culturale", nel senso di un'alterazione percettiva del contesto giuridico avanzato in cui viviamo, dei rischi di allucinazioni e altre distorsioni degli strumenti di intelligenza artificiale, dei loro impatti sociali, della complessità e ricchezza delle interazioni umane e delle loro cause a monte. Guidati dalla fascinazione e dalla competenza tecnica di partner tecnologici, non ci si renderà nemmeno conto di sperimentare apparati securitari lontani dai nostri assetti democratici. Ecco, se non si affronta questo approccio semplicistico di fondo, le violazioni normative saranno sempre una conseguenza inevitabile, né è detto che si disponga sempre di un Garante per arginarle.

Il ruolo dei professionisti

In questo senso, il ruolo dei professionisti è fondamentale: dal DPO che dovrebbe impedire avventure securitarie in violazione della normativa, ai giuristi che hanno il dovere di innescare il pubblico dibattito e di svolgere opera di sensibilizzazione, smascherando la falsa equazione "maggiori controlli = maggiore sicurezza". È un'equazione che alimenta sé stessa, ricorsivamente. Pone cioè la premessa che vuole risolvere.

I professionisti della materia devono essere in grado di trasmettere alla collettività diffusa la percezione che la tutela dei dati personali, e della vita privata, non è un insieme di prescrizioni formalistiche e distaccate dalla realtà (e il recente provvedimento sui metadati davvero non agevola in questo), ma un valore, un arricchimento di umanità, il riconoscimento, in definitiva, che **prima dello Stato viene la persona**. È solo in questa chiave che l'esasperazione della sorveglianza potrà essere percepita nel sentire comune degli amministrati e degli amministratori come recessiva rispetto alla protezione dei dati. **Sono le persone, non i dati**, il vero obiettivo di tutela, e occorre cogliere il contenuto illuminista, progressista, di questo diritto, che costituisce un presidio **oggi indispensabile** nella società del controllo facile e diffuso. Quanto abbiamo bisogno di protezione dei dati personali nell'epoca di un'intelligenza artificiale diventata bene di consumo alla portata di tutti!

> Il punto chiave è proprio **il rapporto tra individuo e potere**: sta tutto in questo, e solo in questo, il GDPR. E quando il potere è quello pubblico, le garanzie giuridiche della persona trovano il loro significato più convincente ma anche il punto di maggiore fragilità. Il potere pubblico può infatti essere schiacciante, perché muove leve insuperabili in una prova di forza con l'individuo. La leva della paura, la leva del consenso collettivo, la leva dell'autorità. Senza un comune sentire, un diritto che si contrapponga al potere pubblico non ha nessuna realistica possibilità.

Un conto è il caso di Trento, un piccolo comune, altro quello dell'apparato centrale dello Stato, che può esercitare leve fortissime. Ne abbiamo avuta esperienza in occasione del green pass: un trattamento imposto politicamente, insostenibile giuridicamente. Eppure passato indenne da contrasto istituzionale. Ecco, in quel caso si è trasmesso alla collettività il senso di un fallimento delle tutele, l'impressione di un diritto che è tale solo occasionalmente, che vale solo talvolta e comunque solo tra privati. È stato un precedente pericoloso, anche in termini di percezione diffusa.

Il diritto di essere lasciati in pace

Come si anticipava, Trento è in realtà solo un *case study* di una rete più vasta, ed è proprio questo che lo rende un'esperienza interessante. Non ci troviamo cioè dinanzi a una singolarità, ma all'applicazione di un modello. Il progetto Marvel ha registrato la collaborazione prestigiosa del CNR e ha ricevuto finanziamenti non irrilevanti nell'ambito del progetto Horizon 2020 della Commissione europea. Protector ha ugualmente ricevuto il finanziamento della Commissione (Internal Security Fund for Police) e il supporto del G20 Inter Faith Forum e dell'UNICRI (United Nations Interregional Crime and Justice Research Institute) e vanta un consorzio europeo, che vede una forte partecipazione di autorità di polizia.

Il Garante, che ha affrontato la questione, ha ritenuto che non possono "*assumere rilevanza gli accordi contrattuali stipulati tra il Comune, gli altri partner dei progetti e la Commissione europea. Si osserva, infatti, a tal proposito, che tali accordi attribuiscono ai beneficiari delle sovvenzioni la responsabilità di assicurare il rispetto della normativa in materia di protezione dei dati (v. art. 39.2 del 'Grant Agreement' relativo al progetto Marvel e art. 23.2 del 'Grant Agreement' relativo al progetto 'Protector'; v. anche l'art. 4.4 del 'Consortium Agreement' relativo al progetto 'Marvel', ove si legge che 'ciascuna Parte è tenuta a garantire che la raccolta, il trattamento e la condivisione dei dati personali e/o di categorie particolari di dati personali siano conformi al Regolamento […] e ad altre normative […] in materia di dati personali. Le Parti garantiranno pertanto la sussistenza di una base giuridica […] in conformità con il GDPR prima di condividere qualsiasi dato personale e/o categorie speciali di dati personali*'".

E tuttavia, viene da domandarsi se, per le **caratteristiche intrinseche** dei due progetti, possa essere realisticamente garantita la cornice di rispetto della normativa o se quella citata non sia solo una clausola contrattuale di esonero di responsabilità. Da avvocato, propendo per la seconda opzione. Del resto, dal sito istituzionale di Horizon 2020 si legge che tra gli obiettivi di Marvel figura "***support new forms of monitoring*** *and managing of resources as well as to provide* ***situational awareness in decision-making***", sia pure asseritamente a beneficio dei cittadini, e che ciò è ottenuto "*via […] fusing large scale* ***distributed multi-modal audio-visual data in real-time***". I segnali c'erano già tutti. Si coglie, e non solo dalla vicenda qui ripercorsa, una tensione evidente, nel cuore dell'Unione, tra la rincorsa di tecnologie in cui siamo indietro rispetto ad altre aree del mondo e il mantenimento di alti livelli di tutela dei diritti. Quando si sperimentano sistemi come quelli visti a Trento, non privi di una forma di avallo della Commissione, almeno nell'impressione di chi scrive, **è lecito chiedersi per quale ragione vengano sperimentati, con quale intenzione applicativa futura di più ampia scala**.

Tornando appunto al senso profondo della tutela della vita privata, di cui il diritto alla protezione dei dati personali costituisce solo la filiazione, è interessante notare che non ci si sia posti nel caso esaminato una preoccupazione ancora più radicale di quella del trattamento di dati personali, ossia se, anche a prescindere da essi o dall'uso invece di informazioni anonime, un'attività di sorveglianza così invasiva e così poco evitabile per i cittadini come quella dei due progetti Marvel e Protector non potesse in ogni caso integrare quelle sproporzionate e non necessarie interferenze illecite nella vita privata, che l'art. 8 CEDU proibisce dal 1950. E le proibisce perché la Convenzione europea nasce esattamente dalla memoria di esperienze totalitarie allora appena concluse, almeno in una parte del mondo.

> Oggi, in un’epoca di travolgenti applicazioni di AI, si avverte particolarmente l’esigenza di essere lasciati in pace, ***to be let alone***, da sperimentazioni securitarie, dal riconoscimento di pattern di comportamento, dall’analisi di emozioni, dall’invasione degli spazi relazionali e addirittura mentali.

Alcuni di questi divieti li leggiamo all’art. 5 dell’AI Act, ma ancora una volta occorre costruire, innanzitutto, una consapevolezza collettiva affinché siano assimilati nell’agire comune. Anche in questo, sono fondamentali i professionisti, gli attivisti, i comunicatori. Possono tracciare la differenza tra il futuro che vogliamo e Skynet.