Università degli Studi di Padova

Dipartimento di Diritto Pubblico, Internazionale e Comunitario

Corso di Laurea in Diritto e Tecnologia

a.a. 2022/2023

Smart cities, videosorveglianza e protezione dati: l'esperienza dei Paesi Bassi

Relatore: Chiar.mo Prof. Andrea Pin

Studente: Manuel Corosiniti

Matricola 2001751

INDICE

INTRODUZIONE

Le città cambiano, si evolvono giorno dopo giorno. Il 50% della popolazione mondiale vive nelle città[1] e ci si aspetta un ulteriore incremento nei prossimi anni. Le città sono al centro di una rivoluzione tecnologica senza precedenti che vede nell' "Information and Communication Technology" (ICT) un mezzo per trasformare problemi in opportunità. Mai come in questo momento è disponibile una mole di informazioni e dati in tempo reale, che sfruttate nel modo giusto possono migliorare la qualità della vita dei cittadini. Iniziative di città intelligenti, che in generale si riferiscono all'ampia integrazione di tecnologie abilitate da software negli ambienti urbani, sono ormai una vista comune nelle grandi città di tutto il mondo. Sembrano ormai una caratteristica quasi obbligatoria in qualsiasi città (o paese) nel mondo sviluppato, compresa l'Europa, dove la Commissione europea incentiva tali progetti attraverso consistenti opportunità di finanziamento[2]. L'uso dei servizi moderni offerti dalla città offre molte opportunità interessanti ed attraenti a molte entità. Tuttavia, nell'ambiente delle città intelligenti, ci sono molte minacce che influiscono sulla privacy degli individui. Le soluzioni tecniche progettate o già implementate devono servire la popolazione, soddisfare le sue esigenze, migliorare la qualità della vita o semplicemente fornire comfort. Pertanto molte di esse devono, per ovvie ragioni, interagire specificamente con le persone, ad esempio l'identificazione, la scansione, il controllo della posizione attuale, compreso il tempo e la direzione del movimento per poi elaborare queste informazioni e archiviarle correttamente per un possibile uso successivo. I sistemi di videosorveglianza sono una componente chiave dell'infrastruttura delle città intelligenti in quanto comportano l'installazione di telecamere in posizioni strategiche in tutta la città per il monitoraggio degli spazi pubblici e la fornitura in tempo reale di registrazioni di sorveglianza alle forze dell'ordine e ad altri rappresentanti della città. Senza adeguate protezioni della privacy del cittadino, i dati raccolti possono essere utilizzati impropriamente o gestiti in modo errato, causando gravi violazioni. I Paesi Bassi non fanno eccezione e possono essere descritti come un paese totalmente impegnato in progetti di città intelligente e "living

[1] United Nations World Urbanization Prospects
[2] Commissione Europea, Smart cities. https:// ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/cityinitiatives/smart-cities_en;

labs". Di conseguenza, diventa sempre più difficile camminare per le strade di una città olandese (grande o piccola) senza essere monitorati, tracciati e talvolta influenzati attraverso una varietà di sofisticate tecnologie digitali.

Nel primo capitolo viene affrontato il concetto di smart city assieme alle nuove tecnologie che contribuiscono ad offrire servizi più efficaci ed accessibili ai cittadini. Viene introdotto il tema della videosorveglianza (anche smart) e dell'uso dei dati raccolti dal punto di vista della protezione dei dati personali con focus sul Regolamento n. 2016/679 (GDPR).

Nel secondo capitolo vengono analizzati due casi studio: le città di Eindhoven ed Amsterdam nei Paesi Bassi. Entrambe risultano essere le città olandesi più attive nella sperimentazione di tecnologie di sorveglianza. Questo grazie a "living labs" e sistemi informatici creati per scopi prevalentemente di sicurezza pubblica.

Il terzo capitolo si concentra sulle principali implicazioni legate all'uso della tecnologie nelle smart cities con particolare enfasi sul fenomeno del "nudging". Si discute dell'influenza del GDPR sull'innovazione delle smart cities. In fine si una menziona la nuova proposta di regolamento con finalità di stabilire regole armonizzate sugli strumenti di intelligenza artificiale ("AI ACT").

CAPITOLO I

VIDEOSORVEGLIANZA SMART E PROTEZIONE DATI

1. Smart city: nozione e caratteristiche

La prima teorizzazione della relazione esistente tra urbanizzazione e processi di innovazione tecnologica si può rivenire nel concetto dei *"distretti industriali sviluppatosi a metà del 1970, un paradigma che si è poi evoluto nella teoria dei cluster industriali"*[3]. Ma il termine *smart city* venne introdotto per la prima volta all'inizio degli anni '90, per indicare la trasformazione urbana frutto della rivoluzione tecnologica e per descrivere l'impatto delle innovazioni in ICT[4] sulle problematiche delle grandi metropoli. Le città tradizionali con il tempo cominciarono a configurarsi come laboratori urbani tecnologico-digitali, vere e proprie "digital city", con il preciso intento di offrire ai cittadini servizi più efficaci e accessibili. Ancor oggi non vi è unanimità nella definizione del termine, anche a causa della complessità della materia oggetto di trattazione, fermo restando che una delle tante esplicazioni si può trovare nella raccomandazione *ITU-T Y.4900* dell'*Unione internazionale delle telecomunicazioni*, in cui: "*Una città intelligente e sostenibile è una città innovativa che utilizza le tecnologie dell'informazione e della comunicazione (ICT) e altri mezzi per migliorare la qualità della vita, l'efficienza delle operazioni e dei servizi urbani e la competitività, garantendo nel contempo che soddisfi le esigenze delle generazioni presenti e future rispetto agli aspetti economici, sociali, ambientali e culturali*"[5]. Da questa affermazione si evince che si fa riferimento sì, a una città intelligente, ma soprattutto a una città sostenibile, efficiente e innovativa, una città in grado di garantire un'elevata qualità di vita ai suoi cittadini grazie all'utilizzo di soluzioni e sistemi tecnologici connessi e integrati tra loro. Lo spazio pubblico al giorno d'oggi è sempre più soggetto all'uso della tecnologia. Pensiamo al tracciamento Wi-Fi e

[3] R. De Santis, A. Fasano, N. Mignolli, A. Villa Il Fenomeno smart cities, in Rivista Italiana di Economia Demografica e Statistica, 2014.
[4] Information and Communication Technologies: tecnologie riguardanti i sistemi integrati di telecomunicazione, i computer, le tecnologie audio-video e relativi software, che permettono agli utenti di creare, immagazzinare e scambiare informazioni.
[3] Raccomandazione ITU-T /.4900, International Telecommunication Union, https://www.itu.int.int/itu-t/recommendations/rec.aspx?rec=12627

Bluetooth, alle telecamere (mobili o corporee) o ai sensori che raccolgono dati sul traffico o sul suono. I comuni stanno sempre più utilizzando queste tecnologie per avere una migliore comprensione dello spazio pubblico al fine di ottimizzarlo, influenzarlo o gestirlo meglio. La tecnologia è quindi indispensabile, ma non è sufficiente, dunque "smart city" come città digitalizzata, ma in cui tutti gli elementi fondanti sono correlati.

Le tecnologie di cui parliamo e che risultano determinanti per facilitare i processi di trasformazione delle suddette città sono: *Tecnologie e infrastruttura dell'informazione e della comunicazione (come il 5G), analisi dei "big data", internet of things, sensori e attuatori, sistemi di riduzione e gestione del consumo energetico e di monitoraggio energetico, sistemi di produzione e distribuzione dell'energia, nuovi materiali e soluzioni per una edilizia sostenibile, nuovi veicoli ibridi ed elettrici, modelli di pianificazione urbana, supporto alle decisioni e gestione a livello amministrativo, gestione del ciclo dei rifiuti, intelligenza artificiale.* La maggior parte delle applicazioni si concentra sulla mobilità e sulla sicurezza (del traffico), dalla misurazione dei flussi di visitatori e traffico al monitoraggio delle aree di intrattenimento. Queste reti intelligenti che si vengono a creare mediante ai dispositivi e sensori che raccolgono dati prodotti dalla città e dai cittadini, analizzando informazioni sull'ambiente, sulle persone e sui consumi, offrono un supporto strategico alle azioni di miglioramento sia in termini di quantità di risorse che di distribuzione intelligente, permettendo, inoltre, comunicazione tra utente-cittadino e PA/ente e di fruire al meglio dei servizi offerti dalla città. La smart city sarebbe, quindi un territorio con alta capacità di apprendimento e innovazione, costruito sulla base delle creatività delle sue comunità, delle sue istituzioni e della sua infrastruttura digitale per la comunicazione e la gestione della conoscenza[6].

Per R. Hollands[7], una città "smart" può trovare quattro distinte definizioni, a seconda dell'interesse preminente perseguito, e così città che possono dare priorità: all'innovazione, al mondo degli affari, alle politiche di inclusione, alla sostenibilità sociale ed ambientale. A questa visione si contrappone la proposta dell'Unione Europea che predilige un approccio che permette di valutare più concretamente la *smartness* di una città intelligente in "6 dimensioni":

[6] https://www.forumpa.it/citta-territori/nicos-komnios-la-smart-city-nasce-dallintelligenza-collettiva/.
[7] R.G. Hollands, Will the Real Smart City Please Stand Up? Intelligent, Progressive or Entrepreneurial?, in City, 12-3-2008, pp. 303-320

- Smart People: partecipazione dei cittadini, coinvolgimento e fiducia nelle istituzioni.

- Smart Governance: le istituzioni devono implementare i servizi, renderli fruibili e comunicarli.

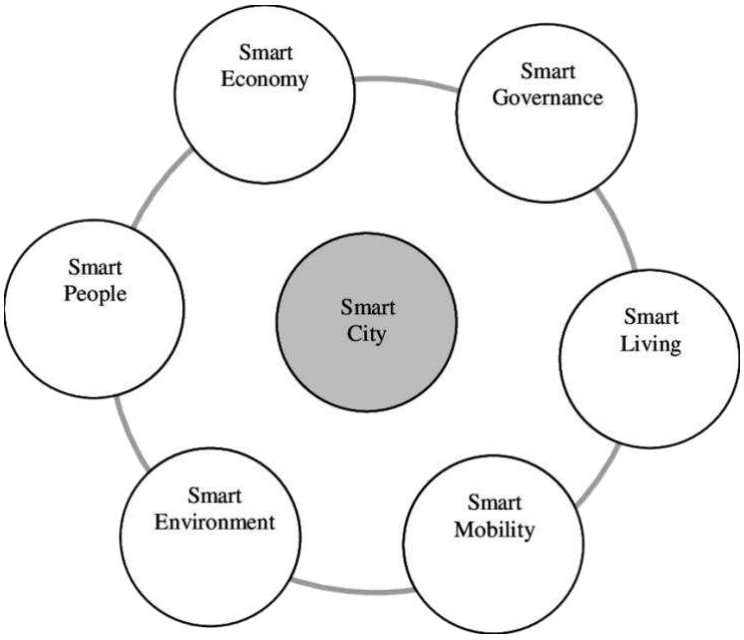
- Smart Living: la gestione di 4 principali *driver* quali salute, educazione, sicurezza, cultura.

- Smart Economy: crescita economica dei territori.

- Smart Mobility: mobilità individuale e collettiva hanno un impatto su salute e stile di vita.

- Smart Environment: migliorare l'impatto ambientale delle attività umane.

Queste sei dimensioni lavorano e collaborano in sinergia le une con le altre: in tal modo ciascuna è funzionale alla definizione delle altre, con il fine del raggiungimento dei così detti "traguardi smart", ed è per questo che vanno pensate all'interno di un modello olistico.



Fonte: A. ANDRONICENAU, M IVAN[8]

2. Intelligenza artificiale, videosorveglianza e sicurezza (dei dati personali).

Le tecnologie a supporto dell'evoluzione e dello sviluppo delle smart cities si fondano su due pilastri di fondo: Big data e intelligenza artificiale. Analizzando il primo, il concetto di Big data viene definito da Gartner come "un patrimonio informativo caratterizzato da velocità, volume e varietà elevati, che richiede forme innovative di analisi e gestione finalizzate a ottenere "insight" nei processi decisionali"[9] .

Questo binomio, attraverso modelli e algoritmi, ha potere predittivo ed è in grado di ipotizzare eventuali scenari futuri. Si è evidenziato come da almeno una quindicina di anni la videosorveglianza sia lo strumento tecnologico di prevenzione a cui più frequentemente fanno ricorso i comuni di tutto il mondo.[10]

Il crescente bisogno di sicurezza urbana, l'implementazione di servizi pubblici e di diffusione delle informazioni, nonché l'attenzione rivolta sempre di più alle tematiche ambientali, hanno fatto sì che le grandi città più industrializzate prendessero come *benchmark*[11] i più moderni canoni della smart city.

I sistemi di sorveglianza rappresentano un aspetto chiave delle future iniziative delle città intelligenti, aiutando le amministrazioni comunali, le agenzie statali e le società di servizi a svolgere le loro funzioni in modo più efficiente e con un impatto ambientale inferiore.

I benefici per i cittadini includono meno congestione del traffico, livelli inferiori di inquinamento e maggiore sostenibilità e sicurezza, affermandosi quindi, in una delle risposte alle nuove esigenze delle più evolute aree urbane.

In tale contesto, l'introduzione di una "sorveglianza partecipativa"[12] oggi

[8] A. ANDRONICEANU, M. IVAN, Smart City – A Challenge for The Development of The Cooperation Mechanism Between European Cities, Proceedings of Administration and Public Management International Conference, 2012, pp.337

[9] L. Camiciotti, C. Racca, Creare valore con i Big data. Gli strumenti, i processi, le applicazioni pratiche, Edizioni LSWR, Milano, 2015.

[10] Paliotta A.P. (2020), Le politiche innovative di sicurezza nelle città tra tecnologie di riconoscimento e smart cities, Sinappsi, X, n.2, pp.98-119

[11] "Parametro di riferimento".

[12] Si richiama il concetto di *crowdsourcing,* ossia quel fenomeno in cui il contributo individuale a fornire dati e informazioni, attraverso dinamiche automatizzate o manuali per il tramite di device, è diventato ormai una componente della vita espressa nella *dimensione digitale.*

consente di procedere, grazie ad applicazioni che lavorano su larga scala, all'identificazione e alla classificazione digitale, utilizzando la combinazione di intelligenza artificiale, algoritmi, caratteristiche biometriche e reti neurali. Si evince quindi che sì, un'articolata sorveglianza all'interno del contesto urbano contrasta comportamenti pericolosi e criminosi, ma allo stesso tempo l'accesso all'enorme mole di dati raccolti è altrettanto massiccio e necessita di essere regolato. Il tema in questione è sempre attuale: si discute già da tempo su come vengano utilizzate le informazioni che lasciamo a social network e app in generale.

La raccolta di informazioni di tutti gli individui che entrano nel raggio di azione (si pensi ad una videocamera installata in una piazza molto frequentata di una città) grazie alle informazioni raccolte ed alla tecnologia utilizzata comporta l'identificazione e successivamente profilazione[13] dei comportamenti dei cittadini. Il rischio di un uso improprio di questi dati cresce in relazione alla dimensione dello spazio monitorato, al numero di persone che frequentano una determinata area ed alla tipologia ed uso dei dati trattati.

Le tecniche utilizzate possono essere più intrusive (ad es. tecnologie biometriche che identificano i soggetti) o meno intrusive (ad es. semplici algoritmi di conteggio non identificativi dei soggetti): conseguentemente, i problemi legati alla protezione dei dati differiscono a seconda della tecnologia utilizzata.

Nelle "Raccomandazioni dell'Autorità Garante Privacy olandese sulle Smart Cities (luglio 2021)[14] da parte di Monique Verdier[15] si evince come: "La tecnologia può aiutarci a risolvere i nostri problemi e a rendere le città più abitabili e sicure. Ma dobbiamo organizzarla in modo che non crei nuovi problemi e un senso di insicurezza. Gli amministratori e i funzionari devono trattare i diritti e le libertà dei cittadini con il massimo rispetto. Ciò significa tenere conto della loro privacy in ogni fase dello sviluppo di una smart city. La privacy deve essere il punto di partenza dell'innovazione, non il punto di arrivo".

[13] Art. 4, Regolamento 2016/679/UE: "Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica".
[14] https://www.autoriteitpersoongegevens.nl/en/news/dutch-dpa-issues-recommendations-smart-cities.
[15] Vice Presidente Garante Privacy olandese.

2.1 Confini normativi: privacy e protezione dati della *videosorveglianza (smart)*.

Il tema della videosorveglianza (smart e non), come si è visto, si è trovato ad essere impattato dalla normativa privacy. E' inimmaginabile, infatti, una smart city priva del trattamento dei dati (anche) personali.

Si parte ancora una volta dal principio generale sancito dall'articolo 8[16] della Carta dei diritti fondamentali dell'Unione Europea[17], ossia il diritto di chiunque alla protezione dei dati personali che lo riguardano.

Con l'entrata in vigore del Regolamento 2016/679/UE[18] (o "GDPR") si entra in una nuova era del mondo privacy, permeato da un approccio sistematico ed una visione innovativa; al fine di contestualizzare i principi della protezione dei dati nel perimetro della videosorveglianza di una città intelligente, grazie all'introduzione delle novità apportate dal GDPR, si elencano quali sono i punti cardine della disciplina della protezione dati:

1. Accountability[19];
2. Privacy by Design[20];
3. Privacy by Default[21];
4. Principio di limitazione delle finalità[22];
5. Principio di minimizzazione;[23]
6. Limitazione della conservazione;[24]
7. Principio di integrità e riservatezza[25]
8. Basi di liceità.[26]

[16] "1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente."
[17] Si veda 2000/C 365/01
[18] Il Regolamento generale sulla protezione dei dati è un regolamento dell'Unione Europea in materia di *trattamento dei dati personali* e di *privacy*, adottato il 27 aprile 2016.
[19] Art. 5, comma 2, e articolo 24, Regolamento 2016/679/UE
[20] Art. 25, comma 1, Regolamento 2016/679/UE
[21] Art. 25, comma 2, Regolamento 2016/679/UE
[22] Art. 5, comma 1, Regolamento 2016/679/UE
[23] Art. 5, comma 1, Regolamento 2016/679/UE
[24] Art. 5, comma 1, Regolamento 2016/679/UE
[25] Art. 5, comma 1, Regolamento 2016/679/UE
[26] Art. 6, comma 1, Regolamento 2016/679/UE

9. Informativa (trasparenza);[27]
10. Misure di sicurezza[28];
11. DPIA (valutazione di impatto e rischio del trattamento)[29];
12. Data breach[30].

A fronte di questo utilizzo sempre più profondo delle tecniche di videosorveglianza urbana, con l'applicazione di nuove tecnologie, oltre alla suddetta disciplina prevista dal GDPR si è resa necessaria da parte del EDPB[31] l'adozione, il 29 gennaio 2020, delle "*Linee Guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video*" il cui scopo è quello di fornire indicazioni su come applicare il GDPR in relazione a questo tipo di trattamento: si tratta di un punto di riferimento in materia su territorio europeo, in cui i punti più importanti in relazione al tema si suddividono in tre macroaree.

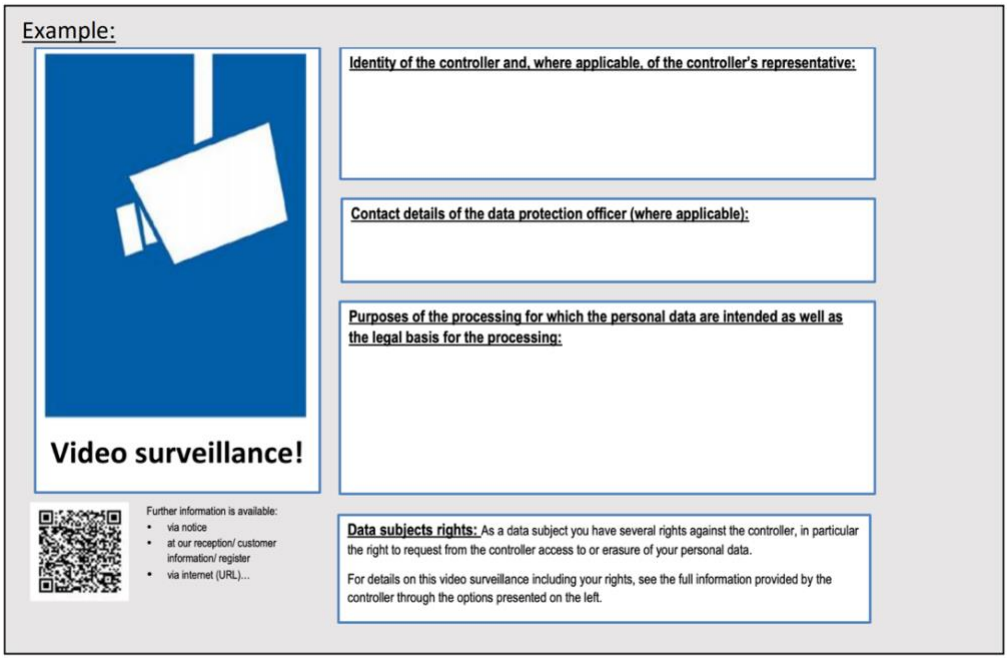
Partendo dalla prima, il trattamento dei dati personali attraverso dispositivi video deve essere improntato in primis al rispetto dei principi fondamentali di riferimento, previsti dall'art. 5 del GDPR, ossia: liceità, correttezza, trasparenza e limitazione della finalità.

Per quanto riguarda le basi giuridiche, si ritengono valide tutte quelle espresse nell'articolo 6, paragrafo 1 del GDPR[32] anche se in pratica le più usate si ritengono essere: *il legittimo interesse* e *l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*. Successivamente rientra il bisogno di individuare i casi di non applicazione del GDPR, sanciti all'interno dell'articolo 2 del citato regolamento ed infine l'individuazione ed il rispetto di alcuni adempimenti

[27] Art. 5, comma 1, Regolamento 2016/679/UE
[28] Art. 32, Regolamento 2016/679/UE
[29] Art. 35, Regolamento 2016/679/UE
[30] Art. 33 e 34, regolamento 2016/679/UE
[31] Il Comitato europeo per la Protezione dei Dati è un organismo indipendente dell'Unione europea il cui scopo è garantire un'applicazione coerente del Regolamento generale sulla Protezione dei Dati e promuovere la cooperazione tra le autorità di protezione dei dati dell' UE.
[32] 1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

specifici, ad esempio: il trattamento deve essere effettuato per finalità determinate, esplicite e legittime; in caso di trattamento di dati particolari – quali ad es. i dati biometrici – i titolari del trattamento sono tenuti a procedere ad una valutazione d'impatto sulla protezione dei dati personali (DPIA), così come in tutti i casi in cui vi sia una sorveglianza sistematica su larga scala di una zona accessibile al pubblico, ex art. 35, par. 3, lettera c) del GDPR; andrà definito con esattezza il periodo di conservazione dei dati raccolti, e andranno garantite misure tecniche ed organizzative di sicurezza elevate.

Le linee guida inoltre riportano anche il seguente esempio di cartello informativo semplificato:



FONTE: Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video. Pagina 29.

Il seguente esempio di cartello informativo semplificato si riconduce all'obbligo di trasparenza ed informazione. Si tratta delle informazioni di primo livello, ovvero la segnaletica di avvertimento, e riguarda la modalità con cui avviene la prima interazione fra il titolare del trattamento e l'interessato. Questo deve essere posizionato in modo da permettere facilmente le circostanze della sorveglianza. Non è necessaria l'indicazione dell'ubicazione della telecamera, in quanto l'interessato deve poter stimare quale zona sia

coperta da una telecamera in modo da evitare la sorveglianza o adeguare il proprio comportamento, ove necessario.

Molte persone potrebbero essere a proprio agio con videosorveglianza installata, ad esempio, per una determinata finalità di sicurezza, ma occorre assicurare che non ne venga fatto un uso improprio per scopi totalmente diversi e inaspettati per l'interessato come nei casi di riconoscimento facciale e trattamento dei dati biometrici. Attualmente si utilizzano molti strumenti per sfruttare le immagini acquisite e trasformare le telecamere tradizionali in telecamere intelligenti. La quantità di dati generati da video, unitamente a questi strumenti e tecniche, aumenta i rischi di un uso secondario (correlato o meno allo scopo al quale viene inizialmente destinato il sistema) o persino improprio. Il tema è di importanza odierna: l'ultima frontiera tecnologica nel campo della videosorveglianza cittadina è costituita dal riconoscimento facciale, ossia un sistema che è in grado di identificare una persona partendo da un'immagine digitale o da un fotogramma. Proprio il tema dei sistemi di riconoscimento attraverso dati biometrici in tempo reale collocati negli spazi accessibili al pubblico è al centro di un ampio spazio nella proposta di Regolamento presentata il 21 aprile scorso dalla Commissione Europea sull'armonizzazione delle norme sull'Intelligenza Artificiale all'interno degli Stati membri (AI Act).

I sensori biometrici stanno diventando una parte integrante della sicurezza delle città intelligenti. Questi possono essere utilizzati per autenticare l'accesso a edifici, veicoli e altre aree soggette a restrizione. I sensori possono anche essere utilizzati per rilevare e tracciare individui in spazi pubblici, consentendo alle autorità di monitorare e rispondere a potenziali minacce. Questi dati biometrici, ai sensi dell'articolo 4 del GDPR possono essere definiti come quei dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici. Questi dati, rientrano nella categoria dei "dati particolari", su cui vige il divieto di diffusione e di norma che di trattamento, fatte salve le eccezioni espressamente previste dall'articolo 9 del GDPR.

Si deduce un tema di vero e proprio asset, quali trattamento di informazioni e di dati, da tutelare, sia dal punto di vista economico che sotto il profilo di sicurezza dei sistemi e infrastrutture utilizzate.

Si evince da un report effettuato da "Statista"[33] come i vari settori e servizi che permeano le caratteristiche di una Smart Cities siano maggiormente esposti a rischi e *cyberattacchi,* quali risultano essere:

- Reti Wi-fi pubbliche
- Smart grid (insieme di reti di informazioni e di reti di distribuzione dell'energia elettrica)
- Il mondo dei trasporti
- *Il mondo delle telecamere per la sicurezza*
- Iniziative open data

In un'ottica di una possibile installazione di un impianto di videosorveglianza pubblica, questo si traduce nella verifica che questi progetti debbano adottare fin dall'origine l'ottica della protezione dati e quindi adottando i principi di *privacy by design* e *privacy by default.* Inoltre, sarà necessario ex ante al trattamento dei dati una valutazione d'impatto come disposto dall'articolo 35 del GDPR. Si intende la DPIA, una "procedura finalizzata a descrivere il trattamento, valutarne la necessità e proporzionalità, e facilitarne la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali", che "permette di realizzare e dimostrare la conformità alle norme"[34]. Lo stesso Garante Privacy inglese[35] ha elaborato nel 2020 una guida per lo svolgimento della DPIA sui sistemi di videosorveglianza urbana. Si chiarisce un'idea dei ruoli e delle responsabilità del soggetto e della normativa privacy che risulti necessaria quando si attua l'installazione di telecamere con fine di sorveglianza. Esempi di domande volte ad aiutare il processo di descrizione e valutazione proposte per l'impiego di suddette telecamere sono:

- Le telecamere sono la giusta soluzione al vostro problema?
- Quali sono i rischi per i soggetti interessati?
- L'impatto sui diritti e sulle libertà degli individui è proporzionato al problema che state affrontando?
- I rischi possono essere ridotti ad un livello accettabile?

[33] https://www.statista.com/statistics/723090/smart-city-services-most-at-risk-for-cyberattacks/.
[34] Linee guida WP29 del 4 Aprile 2017, par.1
[35] https://www.gov.uk/government/publications/data-protection-impact-assessments-forsurveillance-cameras.

Nei sistemi di videosorveglianza urbana, si evidenzia come le principali finalità vengano ricondotte al tema della sicurezza, riduzione e prevenzione della criminalità ma anche alla gestione delle situazioni di rischio e di emergenza, con conseguente intervento e soccorso da parte delle Forza dell'Ordine.

CAPITOLO II

CASI STUDIO

1. I Paesi Bassi: uno stato videosorvegliato?

I Paesi Bassi sono uno dei principali paesi europei impegnati a sperimentare nello sviluppo di città intelligenti[36]. Intere città o parti di esse quali strade, campus universitari o distretti sono diventati veri e propri laboratori in condizioni reali, godendo della libertà di innovare e testare, in gran parte senza essere ostacolati da regolamentazioni pubbliche. Diventa quindi sempre più difficile camminare per le strade di una città olandese (grande o piccola) senza essere monitorati, rintracciati e talvolta influenzati attraverso una varietà di sofisticate tecnologie digitali.

L'Autorità Garante della protezione dei dati personali olandese (Autoriteit Persoonsgegevens) si è espressa sul tema smart city affermando che l'implementazione di soluzioni negli spazi pubblici influisce innegabilmente su diversi diritti fondamentali con l'uso dei dati per classificare o escludere (gruppi di) persone e che ci sia il pericolo di dirigersi verso una società sorvegliata in cui non si può camminare liberamente per strada[37]. Per questo motivo il vice-presidente si è espresso affermando di voler richiedere il divieto di riconoscimento facciale negli spazi pubblici, affermando che con l'aumentare di ogni telecamera installata per strada, parco, treno o autobus avvicini sempre di più i cittadini verso una società di sorveglianza[38].

I comuni, la polizia olandese e alcune entità private sperimentano collettivamente la tecnologia di sorveglianza attraverso i cosiddetti "living labs", un termine che è stato assegnato forse dalle autorità di applicazione della legge per enfatizzare la loro presunta esistenza temporanea. Questi laboratori tendono ad essere concentrati in una città o in un

[36] NL smart city strategy: the future of living. (2017). March 19, 2019, from https:// instituteforfutureofliving.org/wp-content/uploads/NL_Smart_City_Strategie_EN_LR.pdf.
[37] https://www.autoriteitpersoongegevens.nl/en/news/dutch-dpa-issues-recommendations-smart-cities.
[38] https://autoriteitpersoonsgegevens.nl/actueel/privacytoezichthouders-pleiten-voor-verbod-op-gezichtsherkenning

quartiere. Spesso i cittadini non sono informati del progetto e dei suoi possibili effetti sulla loro privacy e su altri diritti fondamentali[39].
Eindhoven ed *Amsterdam* sono le due principali città olandesi che verranno analizzate.

2. Eindhoven e "Stratumseind Living Lab"

Eindhoven è una città di 227 100 abitanti nella provincia del Brabante Settentrionale. Si tratta della città al centro nel campo della tecnologia nei Paesi Bassi, si pensa che un terzo del denaro destinato alla ricerca ed allo sviluppo in questo stato si concentra proprio nella città[40] grazie alla presenza estremamente elevata di aziende ad alta tecnologia e startup innovative[41]. Sensori e telecamere appaiono sparsi per la città senza molte informazioni su chi li possiede e a cosa servono: questo comporta che i cittadini di Eindhoven sono soggetti a vari sistemi di raccolta dati e "living labs" senza la loro conoscenza o consenso.

Il progetto più noto e controverso della città di Eindhoven, che fa discutere molto nei Paesi Bassi in merito al tema della sorveglianza pubblica è l'iniziativa "*Stratumseind Living Lab*".

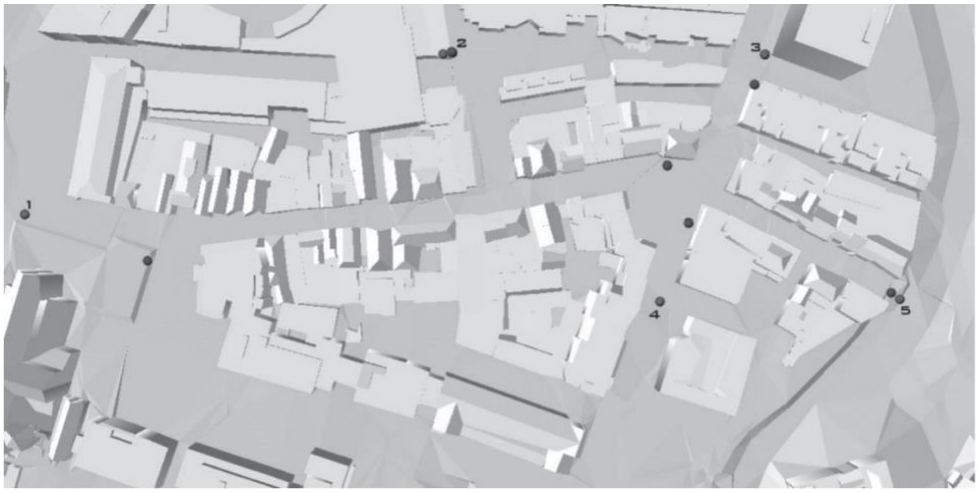
Facendo un passo indietro, la Stratumseind è la via della vita notturna più lunga nei Paesi Bassi (circa 400 metri); ospita circa 50 locali, tra cui caffè, pub, snack bar, una discoteca e un "coffee shop"[42]. In questa via vengono testate ed applicate tutti i nuovi tipi di tecnologie nella vita reale, infatti, troviamo sensori acustici e telecamere video con funzionalità integrate (tra cui il conteggio delle persone, il rilevamento dell'umore e dei modelli di camminata) allo scopo di individuare comportamenti potenzialmente pericolosi e di avvisare la polizia, oltre a lampade stradali dotate di una tecnologia speciale di illuminazione destinata a influenzare l'umore dei passanti[43].

---

[39] Luca Montag, Rory Mcleod, Lara De Mets, Meghan Gauld, Fraser Rodger, and Mateusz Pełka. "The Rise and Rise of Biometric Mass Surveillance in the Eu – a legal analysis of Biometric Mass Surveillance practices in Germany, The Netherlands and Poland" (2021)
[40] https://it.wikipedia.org/wiki/Eindhoven#Tecnologia
[41] Sengers, F. (2016) Smart-Eco Cities in the Netherlands: Trends and City Profiles 2016. Exeter: University of Exeter (SMART-ECO Project).
[42] Maša Galič, 'Surveillance and Privacy in Smart Cities and Living Labs' (PhD, Tilburg University 2020.
[43] Non è presente un sito ufficiale per il progetto, chiamato "Stratumseind Living Lab". Si veda, ad esempio: van Dijk, M. (2018). Stratumseind: de datastraat van Eindhoven. Da https:// innovationorigins.com/nl/stratumseind-de-datastraat-van-eindhoven/.

Con “living lab” si fa riferimento allo sviluppo fuori dal laboratorio, quindi nel mondo reale, coinvolgendo stakeholder, cittadini e utenti finali nella progettazione collaborativa di nuovi servizi. I benefici immediati dell'approccio di questo tipo di laboratorio derivano da questa relazione creata tra le persone e tecnologia[44]. Questo progetto si concentra proprio sulla missione di ridurre la violenza ed arginare i comportamenti criminali, infatti questa via è molto nota per un’incidenza relativamente elevata di violenza, in parte causata da elevati livelli di consumo di alcol.

L’obbiettivo dello Stratumseind Living Lab è proprio quello di creare una città vibrante con cittadini attivi e sani, un buon clima economico e reti sociali solide, nonché una città sostenibile con ricchezza sociale, attenzione all'ambiente e un'economia sostenibile.[45]



Posizioni delle videocamere e audio-sensiori sulla Stratumseind.
FONTE: Comune di Eindhoven

All’interno del progetto dello Stratumeseind Living Lab, ci sono stati numerosi sotto-progetti con attori e obbiettivi diversificati ma comunque interconnessi. Tra i vari, quello più grande e duraturo fu “CityPulse” in cui le due compagnie Atos (creato da IBM) ed Intel ne facevano parte insieme al comune di Eindhoven, le forze della

[44] Innovations in designing Smart Cities as Living Labs (1), di Dr. A. N. Sarkar. www.thesmartcityjournal.com/en/articles/innovations-designing-smart-cities-as-living-labs-1#:~:text=In%20essence%2C%20a%20Living%20Lab,collaborative%20design%20of%20new%20services.
[45] Tinus Kanters, ‘Living Lab Stratumseind’ (2016) www.midpointcsi.nl/powered-bysocialinnovation/wp-content/uploads/2016/07/LLTrillion2015.pdf

polizia ed altre piccole aziende nel campo della tecnologia. Questo progetto impiegava telecamere video (con volti sfocati), sensori audio e telecamere audio con capacità analitiche incorporate, oltre ai dati creati da altri sensori, come temperatura, velocità del vento e pioggia e dati raccolti dalle statistiche settimanali. Raccogliendo dati da una serie di fonti esistenti, tra cui il numero di visitatori e i livelli sonori, queste informazioni "sul campo" venivano combinate con dati raccolti da fonti di social media per creare un quadro potente della strada e aiutare le autorità a prevedere meglio le situazioni ed a reagire ad esse in modo da de-escalare situazioni di possibile pericolo prima che si sviluppino.[46]
Il sistema "CityPulse" sapeva quindi presumibilmente quante persone camminavano o andavano in bicicletta in giro per la Stratumseind in qualsiasi momento della giornata, quale bar era più affollato, quanto velocemente si muovevano le persone e chi aveva un andamento sospetto nella camminata.

2.1 Analisi giuridica dei dati.

All'interno dello Stratumseind living lab, molti dei dati che vengono acquisiti e processati si rifanno ai così detti "dati ambientali" e cioè dati relativi in questo caso al clima, alla quantità dei beni venduti dagli esercenti, livello di suono e affollamento e non quindi a dati che cadono nella definizione di "dati personali" sanciti dall'Art. 4 comma 1 del GDPR.[47]

L'EDPB afferma che la nozione di dati personali è molto ampia e comprende tutte le informazioni che possono essere collegate ad un individuo in termini di contenuto, scopo e risultato[48]. Questo perché se una particolare informazione si riferisce o meno a un individuo è specifico del particolare contesto in cui si trova. Lo stesso dato può essere considerato come riferito ad una persona in un determinato caso e non riferito a una persona in un altro a seconda di una serie di fattori (ad esempio, l'entità dei dati in

[46] Atos, 'CityPulse - Using Big Data for Real Time Incident Response Management' (2015) - https://atos.net/wp-content/uploads/2016/06/atos-ph-eindhoven-city-pulse-case-study.pdf
[47] 1. «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
[48] European Data Protection Board, Opinion 2007. Nowak, para. 34. Visto anche Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González (2014)

possesso, gli scopi del trattamento, il contesto tecnologico e organizzativo attuale e futuro del trattamento). Questa analisi di "relatività" può essere considerata essere stata confermata nella sentenza Nowak della CJEU[49].

Si pensi al tentativo di individuare un ladro ed avvisare gli agenti di polizia all'interno dello Stratumseind living lab, in cui i dati su modelli di camminata degli individui e fotogrammi (con i volti sfocati) provenienti dalle registrazioni video verranno sicuramente analizzati. Bisogna considerare che la sorveglianza all'interno della strada è rivolta a tutti i visitatori, di cui la maggior parte non saranno impegnati in attività criminose o illecite. La seconda parte chiave della definizione di dati personali all'interno dell'Art. 4 comma 1 del GDPR è la nozione di "identificato o identificabile": mentre "identificato" si riferisce ad una persona conosciuta, quindi distinta in un gruppo, "identificabile" si riferisce ad una persona che non è ancora identificata ma che risulta possibile. Inoltre un individuo può essere identificato "direttamente", per esempio con il riferimento a nome e cognome ed "indirettamente" con combinazioni di informazioni che consentono di individuare l'individuo nel gruppo.[50]

Il Considerando 26 del GDPR[51] adotta un test di ragionevole probabilità di identificazione da parte del titolare del trattamento o da un'altra persona, facendo riferimento a fattori oggettivi, come i costi e la quantità di tempo necessari per l'identificazione e tenendo conto dello stato dell'arte della tecnologia al momento del trattamento. Il punto cruciale però all'interno dello Stratumseind living lab è che l'identificabilità non è necessaria ai suoi scopi: gran parte dei dati raccolti non forniscono informazioni sulla persona ma riguarda l'ambiente spaziale. Inoltre, i pochi dati che effettivamente si riferiscono alle persone, vengono anonimizzati per garantire che non possano essere rintracciati.[52] A titolo di esempio, le telecamere utilizzate per conteggiare il numero di persone presenti "salvavano un'immagine sfocata di ciò che stava accadendo in strada"[53]. Tenendo conto che le persone in tali immagini possono comunque essere

[49] Nella sentenza "Nowak", la CJEU ha dichiarato che la nozione di "dati personali" potenzialmente comprende qualsiasi informazione, purché si riferisca all'interessato, cioè quando le informazioni sono collegate a una persona specifica "in ragione del suo contenuto, scopo o effetto". La posizione giuridicamente vincolante della CJEU è quindi in linea con la posizione dell'EDPB.
[50] EDPB,Opinione 4/2007, pagina 13-14.
[51] https://gdpr-text.com/it/read/recital-26/
[52] Willianne Korteweg, 'Smart Urban Governance & Good Governance Principles' (Master Thesis, Utrecht University 2019)
[53] Iris van de Kerk, 'Data Use Versus Privacy Protection in Public Safety in Smart Cities' (Master thesis, University of Utrecht 2015)

riconosciute, il comune di Eindhoven aveva optato per non utilizzare tali immagini e registrare invece il numero di persone, infatti, le videocamere mostrano ogni persona come un "grande punto" e contano per metro quadro il numero di persone che visitano la via grazie ad un software sviluppato da "ViNotion" [54]

La presente figura[55] mostra come il software di ViNotion acquisisce e conta il numero di persone che camminano all'interno della via.

Un'ulteriore valutazione può essere effettuata con una situazione di rischio quale una rissa che sta per scoppiare e che giustificherebbe l'intervento della polizia sulla strada. Lo scopo del progetto "CityPulse" descritto precedentemente, in questo caso, sarà quello di rilevare la situazione rischiosa che altrimenti rimarrebbe inosservata tramite il normale sistema di videosorveglianza operato dalla polizia. L'obbiettivo qui però, è di rilevare una possibile "situazione di pericolo" in modo che il sistema possa avvisare le forze di polizia in anticipo, un obbiettivo che non richiede nessun tipo di identificazione.

[54] Linda Vlassenrood, 'Becoming a Smart Society' (DATAstudio), https://destaatvaneindhoven.hetnieuweinstituut.nl/sites/default/files/datastudio_becoming_a_smart_society_def.pdf

[55] Tinus Kanters, 'Living Lab, Onderdeel Van Stratumseind 2.0, Smart Sensors, Smart Interfaces, Smart Actors, Smart Lights, Smart Data, Smart Design, Augmented Reality, Gaming' (Eindhoven, 2013) pagina 8.

La situazione sarebbe diversa se i responsabili non fossero fermati immediatamente, quindi la polizia ricorrerebbe al flusso video (non sfocato), potendo eventualmente pubblicare immagini sulle notizie e social media, situazione che va al di fuori degli scopi del progetto in questione. Si può affermare che in generale gli obbiettivi dello Stratumseind living lab non consistono nell'identificare individui specifici. Emerge però la discussione se la profilazione costituisce una forma di trattamento dei dati personali per via della sua finalità di influenzare gli individui, una questione che non è stata ancora risolta e che detiene sostenitori ed oppositori. Discussa è anche quella che si potrebbe chiamare "profilazione atmosferica" che cerca di influenzare indirettamente una molteplicità di persone anziché un individuo ma sembra non costituire un tipo di trattamento dei dati personali. Questo potrebbe spiegare perché nella pratica, molti attori dei progetti inerenti alle smart cities considerano che le loro operazioni di trattamento dei dati coinvolgono dati, in realtà, non personali, creando così un vuoto legale. Una soluzione potrebbe essere quella di impiegare strumenti di autoregolamentazione che vanno oltre i limiti della legge sulla protezione dei dati e quindi possono valutare l'accettabilità di questi tipi di progetti senza essere vincolati dalla distinzione tra dati "personali" e "non personali". Tuttavia, i rischi di iniziative di autoregolamentazione sono stati a lungo sottolineati, soprattutto per quanto riguarda la grande quantità di discrezionalità che concedono.

3. Amsterdam ed il "crowd management".

Amsterdam è la capitale e la maggiore città dei Paesi Bassi. Si trova nella provincia dell'Olanda Settentrionale e con i suoi 921402 residenti (nel 2022) di oltre 170 nazionalità[56] si è posizionata come un attore di rilievo quando si tratta di attuare progetti a favore dello sviluppo economico sostenibile. Amsterdam è attiva sul tema smart cities già da tempo: la città ha promosso una partnership tra più di 70 soggetti pubblici e privati per creare i servizi e le infrastrutture adibiti al raggiungimento di questi scopi.[57]

Nel 2009, avviato dall'*Amsterdam Economic Board*[58] e l'operatore di

[56] https://it.wikipedia.org/wiki/Amsterdam
[57] Stefania Carulli, "Amsterdam, l'avanguardia europea delle smart city" (2014), https://www.techeconomy2030.it/2014/05/05/amsterdam-lavanguardia-europea-delle-smart-city/
[58] L'Amsterdam Economic Board è un'organizzazione non profit con sede ad Amsterdam. Stimola le partnership che lavorano sulla metropoli intelligente, verde e sostenibile del domani e si concentra su

elettricità “Liander”, in stretta collaborazione con il comune, nasce “Amsterdam Smart City”: si tratta della prima città europea a lanciare un progetto del genere. “Amsterdam Smart City” è una piattaforma aperta che riunisce professionisti dell'innovazione provenienti da governi, aziende, istituzioni di conoscenza e organizzazioni della società civile per plasmare la città e la regione del futuro. Aziende, istituti di conoscenza, governi e residenti attivi si riuniscono, interagiscono e collaborano per la città.[59] Si sostanzia quindi in una piattaforma indipendente pensata per lavorare su due piani: il primo quello della partnership tra pubblico e privato al cui centro si pongono i rapporti con le aziende e il secondo quello della community che si rivolge direttamente ai cittadini.

3.1 The “Public Eye” e privacy-by-design.

La città di Amsterdam è una realtà molto affollata con alti numeri di turisti che creano agglomerati nelle vie più trafficate, situazione che può portare a situazioni pericolose e molte volte non sicure, con rischio di violenza, lesioni e possibili cadute nei canali, come afferma Boen Groothoff (responsabile del progetto per la “smart mobility” nell’Ufficio Tecnologico della città di Amsterdam). Questo ha portato il comune a sviluppare quello che si definisce il primo sistema di monitoraggio della folla *privacy-by-design*[60], chiamato “Crowd Monitoring System Amsterdam (CMSA)”. Si tratta di un sistema di monitoraggio composto da telecamere di conteggio e sensori Wi-Fi per fornire una comprensione dei numeri e delle densità dei pedoni. Questi dati vengono utilizzati per scopi strategici e operativi. Il progetto pilota “Public Eye”, un sistema innovativo ed open-source, parte del CMSA, viene utilizzato per mappare le folle in alcuni luoghi ad Amsterdam. In questi luoghi sono presenti telecamere collegate a un server del comune. Sul server, un algoritmo analizza quanti individui sono presenti nelle immagini. L’algoritmo converte immediatamente le immagini in numeri anonimi, dopo di che questi

argomenti importanti per i residenti della metropoli: l'uso responsabile dei dati e della tecnologia, un ambiente di vita sostenibile e salutare e un lavoro significativo per tutti. - https://amsterdameconomicboard.com/en/faq/

[59] https://amsterdamsmartcity.com/about

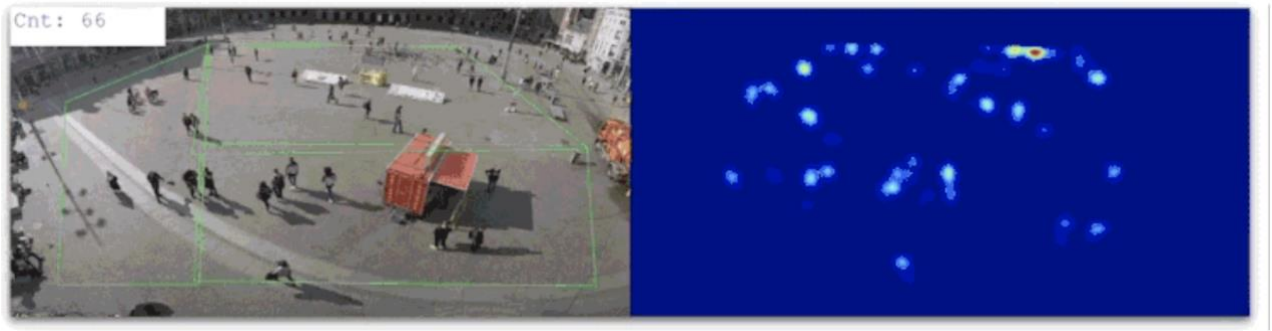
[60] Il principio della privacy-by-design richiede che la tutela dei diritti e delle libertà degli interessati con riguardo al trattamento dei dati personali comporti l'attuazione di adeguate misure tecniche e organizzative al momento sia della progettazione che dell'esecuzione del trattamento stesso, onde garantire il rispetto delle disposizioni del Regolamento UE 2016/679.

vengono inviati al CMSA[61]. In particolare questo tipo di tecnologia intelligente è presente in tre posizioni nella città: Arena Boulevard, Marineterrein e Piazza Dam. Le informazioni sul numero di persone presenti vengono inviate agli addetti comunali che possono utilizzare il conteggio per regolare meglio il traffico. I dati vengono anche utilizzati per supportare un'app e un sito web del comune[62], oltre a messaggi su chioschi digitali sparsi per la città per aiutare i cittadini a pianificare il loro percorso e evitare invece percorsi possibilmente affollati. Ad esempio, durante la pandemia quando le palestre erano chiuse, Amsterdam ha utilizzato "Public Eye" in una popolare area fitness all'aperto nel Marineterrein. Se l'algoritmo rilevava che le persone erano troppo vicine l'una all'altra, le strisce LED si accendevano di blu e poi di rosso se c'erano troppe persone nell'area[63]. L'algoritmo permette che le immagini degli individui non vengano mostrate o memorizzate: vengano immediatamente eliminate non appena quest'ultimo abbia contato il numero di presenti[64]. Dall'informativa sulla privacy[65] redatta dall'autorità locale di Amsterdam in riferimento all'iniziativa "Public Eye" si evince che il comune raccoglie e utilizza diverse categorie di dati personali dai suoi residenti ma dipenderà dal trattamento specifico quali dati personali verranno elaborati esattamente e per quale scopo. Viene affermato come la finalità del trattamento dei dati personali per "Public Eye" sia monitorare e, se necessario, influenzare o intervenire nei flussi di traffico nel contesto di:

- Accessibilità e flusso del traffico.
- Qualità e comfort.
- Sicurezza del traffico.
- Contribuire a fornire informazioni valide agli utenti della strada.
- Sviluppare ed addestrare un algoritmo che determina il numero di persone in una determinata area.

[61] Autorità locale di Amsterdam, https://www.amsterdam.nl/innovatie/mobiliteit/public-eye-oplossing-crowdmanagement/
[62] Il sito in questione è: https://druktebeeld.amsterdam.nl/. I residenti e i visitatori della città possono visualizzare le informazioni sul numero di persone presenti nei punti di sorveglianza.
[63] Sarah Wray, Why the City of Amsterdam developed its own crowd monitoring technology. (2021), https://cities-today.com/why-the-city-of-amsterdam-developed-its-own-crowd-monitoring-technology/
[64] Autorità locale di Amsterdam, https://algoritmeregister.amsterdam.nl/public-eye/
[65] https://www.amsterdam.nl/privacy/specifieke/privacyverklaring-parkeren-verkeer-bouw/public-eye/

Il comune di Amsterdam elabora i dati personali per l'esecuzione di un compito di interesse pubblico. Viene specificato come le basi giuridiche in questione siano rispettivamente: l'articolo 2 della "Legge sulla Circolazione Stradale del 1994"[66] e dell'articolo 174[67], comma 1, comma 2 e comma 6 del libro 6 del codice civile olandese. I dati in questione non vengono inoltre elaborati al di fuori dello Spazio Economico Europeo e non vengono profilati. Importante tema che viene affrontato è il "retention period" in quanto viene dichiarato che non vi è un periodo di conservazione (legale). Questo perché l'implementazione del "Public Eye" si basa sui requisiti di privacy-by-design e di minimizzazione dei dati[68]; i dati personali vengono anonimizzati quasi immediatamente sui server trasformandosi in "heatmap" da cui non è possibile recuperare alcun tipo di dato personale. Da questa operazione, solo alcune schermate delle immagini verranno utilizzate casualmente per un altro anno per testare e addestrare l'algoritmo.



Nella seguente figura[69] viene mostrato come le immagini catturate dalle videocamere vengono anonimizzate.

[66] https://www.global-regulation.com/translation/netherlands/3074644/road-traffic-act-1994.html
[67] 1. "Il possessore di una cosa immobile costruita che causa pericolo per le persone o altre proprietà perché non soddisfa gli standard che nelle circostanze date possono essere stabiliti per tali cose, è responsabile se questo pericolo potenziale si realizza, a meno che non sarebbe stato responsabile ai sensi della precedente Sezione se avesse avuto conoscenza del pericolo al momento in cui è occorso."
2. "Quando una cosa immobile costruita come previsto nel paragrafo precedente è gravata da un diritto di enfiteusi a lungo termine, la responsabilità ricade sul possessore del diritto di enfiteusi a lungo termine. Per quanto riguarda le strade pubbliche pericolose, la responsabilità ricade sull'autorità pubblica che deve garantire che la strada sia in buone condizioni. Per quanto riguarda le condotte pericolose, la responsabilità ricade sulla direzione responsabile della manutenzione, tranne per quanto riguarda le condotte situate in un edificio o una costruzione e destinate all'approvvigionamento o alla scarico di fluidi o altre sostanze per conto di tale edificio o costruzione."
6. "Ai fini del presente articolo, una strada pubblica comprende la fondazione e la superficie della strada e i suoi arredi stradali."
[68] Il principio di minimizzazione dei dati fa parte dei principi in base ai quali si effettua il trattamento dei dati. Esso parte dall'idea che, salvo poche eccezioni, un titolare deve trattare solo i dati di cui ha realmente bisogno per raggiungere le finalità del trattamento.
[69] Ivi. 61

Inoltre, il comune di Amsterdam di recente ha implementato in collaborazione con l'Amsterdam Institute of Advanced Metropolitan Solution il progetto "Shuttercam", in cui la città sta sperimentando telecamere con una sorta di tenda che si aprono e si chiudono per mostrare alle persone quando i sensori sono effettivamente attivi e quindi sono in funzione. Nel "Marineterrein Amsterdam Living Lab" sono in fase di sperimentazione tre telecamere prototipo: una con un oscurante che funziona secondo un programma orario prestabilito, un'altra che i residenti possono spegnere temporaneamente o dalla quale possono optare per non essere monitorati e una terza che deve essere "avvolta" e quindi oscurata manualmente una volta alla settimana come una barriera fisica[70].

Un sistema di monitoraggio delle folle funziona con una telecamera dotata di un algoritmo in grado di leggere ed analizzare le immagini video. Oltre a misurare le folle e visualizzarle in numeri utilizzabili, l'algoritmo può anche determinare se le persone mantengono una distanza di 1,5 metri. Tutto ciò avviene in modo anonimo e conforme alle norme di protezione dati: le immagini video non vengono visualizzate da un essere umano, ma vengono elaborate automaticamente dove viene salvato solo un numero limitato di fotogrammi con volti di persone irriconoscibili e sfocati. Questi fotogrammi aiutano a "addestrare" l'algoritmo. Inoltre, queste immagini non vengono conservate.[71]
In conclusione, le telecamere che rientrano in questo esperimento sono elencate nella scheda "Elaborazione dei dati personali in spazi pubblici"[72]: si tratta di una mappa interattiva della città dove viene mostrato nello spazio pubblico dove effettivamente vengono elaborati dati personali da parte del comune e a quale scopo[73].

[70] The UN specialized Agency for ICT; https://www.itu.int/hub/2021/10/why-the-city-of-amsterdam-developed-its-own-crowd-monitoring-technology/
[71] Amsterdam Institute of Advanced Metropolitan Institute; https://www.ams-institute.org/urban-challenges/urban-data-intelligence/shuttercam-would-cameras-equipped-with-shutters-contribute-to-a-responsible-smart-city/
[72] https://maps.amsterdam.nl/privacy/
[73] https://www.amsterdam.nl/innovatie/digitalisering-technologie/digitale-veiligheid/sensoren-openbare-ruimte/shuttercam-project/

CAPITOLO III

RIFLESSIONI ED OSSERVAZIONI CONCLUSIVE

1. Il rischio del "nudging"

Come si è dimostrato nei precedenti capitoli, rimane impensabile immaginare una smart city scevra dal trattamento di dati (anche) personali. Evidenza che viene sottolineata anche dallo stesso Garante italiano[74] nella comunicazione a commento dello studio "Artificial Intelligence and Urban Development"[75], condotto dal Parlamento Europeo in cui si afferma come l'applicazione delle tecnologie di intelligenza artificiale allo sviluppo delle smart cities può comportare seri rischi, potendosi altresì creare un divario di sviluppo e opportunità sociali ed economiche tra singole zone della città che si aggiunge alla problematica centrale del lecito trattamento e l'individuazione delle corrette finalità dell'elaborazione. La raccolta dei dati è ciò che alimenta le città intelligenti e le comunità, ma è anche la fonte di preoccupazioni sulla privacy, alcune legittime e altre basate su cupi scenari improbabili.

Come si è visto in relazione alla sorveglianza per scopi di sicurezza urbana, uno dei principali rischi è legato alla questione della spinta manipolativa (o "nudging"), uno degli argomenti chiave per cui valorizziamo la privacy. Si tratta di misure non regolamentari che mirano a influenzare un individuo a cambiare il suo comportamento attraverso modifiche sottili ed economicamente convenienti nel suo ambiente[76]. Da questa prospettiva, il fenomeno *smart city* sta trasformando le città in grandi laboratori, dove una domanda chiave posta è: come rendere prevedibile e esternamente controllabile il comportamento delle persone? In questo senso, il sistema di videosorveglianza pubblica (anche automatizzata) può essere visto come una manipolazione dell'ambiente al fine di scoprire e influenzare il comportamento delle persone per rendere il luogo più sicuro e attraente per i visitatori. Si è visto come molte tecnologie delle città intelligenti non

[74] Garante per la Protezione dei Dati Personali, Newsletter del 6-10-2021, doc.web. 9705786, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9705786#3
[75]https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690882/IPOL_STU(2021)690882_EN.pdf
[76] Oliver, Adam. 2013. "From Nudging to Budging: Using Behavioural Economics to Inform Public Sector Policy." Journal of Social Politics pagine 685–700.

raccolgono dati sul comportamento o sulle attività individuali dei residenti, ma sull'infrastruttura locale, sull'ambiente o sul comportamento collettivo dei residenti, il che comporta rischi minimi o nulli per la privacy. Tuttavia preoccupazioni sorgono anche dalle sfide tecnologiche connesse alla separazione tra dati urbani e dati personali. Si pensi all'uso sempre più dettagliato dei metodi di profilazione e dalle carenze nelle attuali strumentazioni di anonimizzazione, che potrebbero agevolare la "ri-identificazione" delle persone dai dati aggregati e anonimizzati[77]. Si può affermare come nonostante le telecamere e i microfoni vengano utilizzati principalmente per la gestione delle folle, e dunque le informazioni vengono anonimizzate, il rischio di profilazione è sempre presente. I quesiti che sorgono alla luce di queste informazioni sono: è necessario e legittimo raccogliere dati per manipolare il comportamento dei cittadini? Viene effettivamente raccolto il minimo indispensabile dei dati? Ed infine, se la smart city collabora con una società privata per raccogliere e elaborare i dati (come nel caso dello "Stratumseind Living Lab"), chi possiede i dati e che tipo di contratti hanno queste entità con gli enti pubblici? La risposta si trova anzitutto nell'Articolo 5 del GDPR, dove vengono esplicati i principi applicabili al trattamento di dati personali, infatti, le tecnologie di raccolta dei dati devono operare in modo aperto e verificabile, con documentazione chiara sula gestione delle informazioni[78]. Risulta chiaro allo stesso tempo come i dati raccolti dalle tecnologie all'interno delle smart cities siano originariamente rivolte a gestire l'efficienza dei servizi pubblici invece che influenzare e manipolare le decisioni dei cittadini.

Le "spinte" basate sui dati dei cittadini tendono a funzionare meglio quando questi ultimi non sono consapevoli della loro esistenza: operando in modo "non trasparente" difficilmente possono conformarsi ai requisiti del GDPR relativi alla trasparenza della raccolta e dell'elaborazione dei dati, poiché i cittadini dovrebbero essere informati di questo uso secondario e potenzialmente non correlato dei dati al fine che vi siano autorizzati a revocare eventualmente il loro consenso.

Il GDPR richiede anche che enti pubblici e privati debbano garantire la raccolta

[77] van Zoonen, Liesbeth. 2016. "Privacy Concerns in Smart Cities." Government Information Quarterly, pagine 472–480.
[78] Privacy International. 2017. "Smart cities: Utopian vision, Dystopian Reality." https://privacyinternational.org/sites/default/files/2017-12/Smart%20Cities-Utopian%20Vision%2C%20Dystopian%20Reality.pdf

e l'elaborazione dei dati entro i limiti della necessaria esecuzione di un compito di interesse pubblico definito dalla legge come espresso dagli articoli 5 e 6 comma 1 del GDPR[79]. Come si è visto, le smart cities lavorano spesso insieme ad attori privati per raccogliere ed elaborare dati attraverso diverse tecnologie; tuttavia, l'uso di dispositivi e reti interconnesse gestiti da parti pubbliche e private è problematico. Le città intelligenti si affidano a società tecnologiche private (ad esempio, IBM, Alphabet) come forma di riduzione dei costi, a causa della mancanza di competenze nei loro dipartimenti IT locali. La crescente dipendenza di una governance ibrida ed estese reti pubblico-private solleva ulteriori preoccupazioni, come la mancanza di trasparenza dei dati, la responsabilità dei loro custodi, la delega non giustificata di compiti pubblici a attori privati e la protezione dell'interesse pubblico[80]. Si potrebbe pensare che queste stesse "spinte" manipolative basate sui dati sviluppate dalle tecnologie gestite in parte da società private potrebbero non essere solo un riflesso dell'interesse pubblico in un determinato momento, ma potrebbero anche essere influenzate dagli interessi delle società orientate al profitto.

2. Il GDPR rallenta l'innovazione delle smart cities?

La privacy è stata a lungo vista come un ostacolo all'innovazione. È stata considerata come un elemento che aumenta i costi per la gestione dei dati senza fornire benefici reali. Con l'entrata in vigore del GDPR il 25 Maggio 2018, questo è stato e continua a essere oggetto di discussioni in tema di innovazione tecnologica. L'obiettivo del GDPR è proteggere tutti i cittadini dell'UE da violazioni della privacy e delle informazioni in un mondo, come si è visto, sempre più basato sui dati, molto diverso dall'epoca in cui è stata istituita la direttiva del 1995[81].

Non tutti i sistemi collegati alla Smart City saranno direttamente correlati ai dati di base, specialmente quelli che non sono di natura ad alta tecnologia. Si pensi a sistemi di irrigazione o smaltimento dei rifiuti: questi risultano non essere direttamente collegati alle persone. Tuttavia, ci sono attività in cui questa divisione non è così semplice. Ad esempio, una rete di piste ciclabili; se non è sotto sorveglianza video, non ha alcuna

[79] Blume, Peter. 2015. "The Public Sector and the Forthcoming EU Data Protection Regulation." European Data Protection Law, pagine 567–591.
[80] Maher, Imelda. 2007. "Economic Governance: Hybridity, Accountability and Control." Columbia Journal of European Law, pagine 679–703.
[81] Direttiva 95/46/CE

connessione con i dati personali. Tuttavia, se la città dispone di un sistema di condivisione delle biciclette (sistema di biciclette pubbliche), quando si utilizzano le biciclette della città, di solito autorizzate e pagate con carte di credito, inevitabilmente verranno raccolti dati personali. I più moderni modelli di smart city utilizzano le tecnologie dell'"Internet of things" (IoT): in questo caso, è necessario raccogliere, accedere e gestire i dati personali in modo appropriato[82].

La domanda che ci si pone in questo contesto è: cosa succede nei sistemi in cui ci sono diversi livelli di automazione e in cui una persona fisica non segnala volontariamente i propri dati? Con l'art. 5 del regolamento si può affermare come la raccolta di dati personali a fini di sviluppo delle smart city deve essere precisamente definita, con adeguate norme legali, e deve essere prestata particolare attenzione alla conservazione dei dati che consentono l'identificazione di una persona fisica, che non dovrebbe durare più del necessario. Certamente, i dati possono poi essere conservati per scopi statistici e altri, come la creazione di un modello del traffico, ma come si è visto, dovrebbero essere anonimi. L'articolo 6 del regolamento stabilisce inoltre che il trattamento dei dati personali è legittimo se sono soddisfatte determinate condizioni, come l'esecuzione di un compito di interesse pubblico e si menziona esplicitamente la questione della sicurezza del trattamento dei dati personali, come affermato esplicitamente nell'articolo 32. Come si è visto, le definizioni di base dei dati personali, secondo l'articolo 4, significa qualsiasi informazione relativa a una persona fisica identificata o identificabile; una persona fisica identificabile è una persona che può essere identificata, direttamente o indirettamente, in particolare facendo riferimento a un identificatore come un nome, un numero di identificazione, dati di localizzazione, un identificatore online o a uno o più fattori specifici dell'identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale di tale persona fisica. La persona fisica potrebbe essere identificata anche dal veicolo che guida, anche in una città con decine di migliaia di persone; il veicolo potrebbe essere individuato dal colore e dal tipo di veicolo, anche quando guidato da un singolo individuo - quindi potrebbe essere riconosciuto anche senza conoscere le targhe. In determinati casi, se le riprese di sorveglianza finiscono in mano a una persona malintenzionata, potrebbe verificarsi una violazione molto grave della privacy. Da quest'analisi si può notare come l'applicazione del GDPR influenza in

[82] Surdean, R., Secure Connections for a Smarter World, MIPRO 2017 Proceedings, Opatija, Croatia, pagina 5.

maniera notevole l'implementazione del modello smart city, dove la raccolta dei dati personali diviene inevitabile dal punto di vista dell'individuo nel contesto urbano dell'individuo. Nel contesto urbano, il GDPR può contribuire a costruire un modello smart city di alta qualità. Tuttavia, è lecito affermare come la mancanza di un approccio sistematico ed una strategia di sviluppo potrebbero portare a delle difficoltà: impostare male un sistema di videosorveglianza è sufficiente per far sì che i dati personali possano essere soggetti ad un abuso in una piccola città. Il GDPR ha senza dubbio rafforzato enormemente i poteri e i compiti delle autorità di controllo privacy nei vari stati. I poteri sanzionatori e di intervento ex post sono poi estremamente estesi ed incisivi, tanto da avere effetti dissuasivi e preventivi anche nei confronti di grandi colossi digitali e non[83]. Il GDPR ha quindi contribuito in maniera massiccia ad una migliore tutela dei dati contro le minacce tecnologiche, grazie a diverse misure come l'applicazione simultanea delle stesse regole in tutti i Paesi dell'UE, sanzioni uniformi, obbligatorietà in moltissimi casi della nomina del Responsabile della protezione dei dati, fine della centralità assoluta del consenso ed emersione paritetica di altri presupposti di liceità di trattamento, obbligo di notifica al garante e della comunicazione degli interessati delle violazioni di dati personali, i principi di "privacy by design" e "privacy by default", e così via[84]. In breve, il GDPR non dovrebbe essere visto come un "pericolo" per le smart city, ma come una serie di condizioni che possono essere utili nello sviluppo dei modelli di smart city. Inoltre, i cittadini accetteranno più volentieri una smart city che non li faccia pensare a una forma di "Grande Fratello" o di controllo totalitario sulle loro libertà personali. Pertanto, il GDPR può anche contribuire allo sviluppo dei modelli di smart city, poiché la sua attuazione garantisce un livello più elevato di protezione dei dati personali, riducendo così la paura di possibili abusi delle funzioni di controllo della città intelligente.

3. AI act

La Commissione europea ha presentato nel 2021 una proposta di regolamento con

[83] https://www.istitutoitalianoprivacy.it/2019/04/01/il-garante-privacy-del-futuro-idee-per-il-prossimo-collegio-2019-2026/
[84] https://www.agendadigitale.eu/sicurezza/privacy/il-gdpr-compie-un-anno-il-valore-del-dato-delinea-il-futuro-delle-authority-antitrust-agcom-privacy/

finalità di stabilire regole armonizzate sugli strumenti di intelligenza artificiale[85]. Approvato il 14 giugno 2023, ora sarà soggetto ad ulteriori modifiche ad opere delle altre istituzioni dell'Unione Europea. Il Parlamento Europeo ha adottato la sua posizione sul così detto "AI Act" votando non solo di mantenere, ma anche estendere il divieto proposto inizialmente dalla Commissione Europea sull'identificazione biometrica in tempo reale. Il Consiglio dell'Unione Europea, d'altra parte, ha concordato di estendere gli utilizzi consentiti dei sistemi di identificazione biometrica remota da parte delle forze dell'ordine e l'utilizzo dell'identificazione facciale e biometrica "in tempo reale" con finalità di indagare e perseguire i reati[86]. Si tratta di due posizioni che dimostrano quanto il tema sia estremamente rilevante ai giorni d'oggi. Mentre la sorveglianza biometrica di massa sembra andare nella direzione del divenire vietata, altri utilizzi della sorveglianza biometrica possono anche costituire un grave rischio per i diritti umani e dovrebbero essere consentiti solo in base a un solido regime normativo che garantisca trasparenza, proporzionalità, controllo e rimedio.

[85] Commissione europea, *Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale* (doc. 52021PC0206), 2021

[86] Iverna McGowan, "Iverna McGowan, "CDT Europe Calls on EU Leaders to Prohibit Mass Surveillance Through Indiscriminate and Arbitrary Uses Of Biometric Technologies In the EU's AI Act", https://cdt.org/insights/cdt-europe-calls-on-eu-leaders-to-prohibit-mass-surveillance-through-indiscriminate-and-arbitrary-uses-of-biometric-technologies-in-the-eus-ai-act/ 2023

CONCLUSIONI

Il tema della privacy negli spazi pubblici nel contesto della sorveglianza nelle smart cities ha portato la stesura dell'elaborato su di un piano interdisciplinare di importanza odierna. Nelle città più grandi (e più nuove) si assiste giorno dopo giorno a delle trasformazioni, dei cambiamenti attraverso l'introduzione di sensori e tecnologie di sorveglianza come telecamere intelligenti e microfoni ma anche sistemi di tracciamento wi-fi. Ottenere la privacy negli spazi pubblici può diventare difficoltoso ed al tempo stesso rischioso.

Quello che è emerso dai casi studio analizzati è come l'attenzione di tale sorveglianza sia rivolta all' "atmosfera" della strada e le persone sono governate come una molteplicità piuttosto che come individui. Di conseguenza, il principio è in qualche modo inclusivo: le trasgressioni minori sono trascurate finché l'atmosfera sulla strada non viene compromessa. I "rischi legati alla privacy" includono rischi più ampi derivanti dalla sorveglianza, come può essere la profilazione di gruppo. Di conseguenza, le persone non devono essere identificate individualmente, ma possono comunque essere soggetti a previsioni e "spinte" conseguenti basate su questo presupposto[87]. La protezione della privacy nello spazio pubblico deve essere bilanciata con altri interessi legittimi, come la sicurezza pubblica e la prevenzione della criminalità. Tuttavia, questo bilanciamento deve essere fatto in modo proporzionato e conforme ai diritti umani e dovrebbe includere un coinvolgimento dei cittadini nelle decisioni riguardanti la sorveglianza nello spazio pubblico.

In conclusione, una città intelligente non deve essere così "orwelliana" come sembra: non c'è motivo per cui ciò che sembra invasivo in astratto non possa rivoluzionare il modo in cui le persone vivono meglio, offrendo servizi che anticipano le loro esigenze. La comprensione e la protezione della privacy nello spazio pubblico sono fondamentali per la salvaguardia della socialità e della partecipazione attiva negli ambienti urbani del presente e del futuro.

[87] Barocas, S., & Nissenbaum, H. (2014). Big Data's end run around anonymity and consent. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), Privacy, Big Data, and the public good: frameworks for engagement (pagine. 44–75). Cambridge: Cambridge University Press.

BIBLIOGRAFIA

A. Andronicenau, M. Ivan, *Smart City – A Challenge for The Development of The Cooperation Mechanism Between European Cities, Proceedings of Administration and Public Management International Conference*, 2012

A. Capoluogo, Smart cities tra intelligenza artificiale, videosorveglianza e data protection. Aspetti legali, casi di studio, soluzioni operative. Edizioni giuridiche Simone, 2023

A. Capoluongo, Videosorveglianza: the Game Changer – Data protection, norme e applicazioni, Edizioni Themis, 2021

Atos, CityPulse - *Using Big Data for Real Time Incident Response Management*, 2015 - https://atos.net/wp-content/uploads/2016/06/atos-ph-eindhoven-city-pulse-case-study.pdf

Barocas, S., & Nissenbaum, H., 2014. *Big Data's end run around anonymity and consent. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum* (Eds.), Privacy, Big Data, and the public good: frameworks for engagement, Cambridge: Cambridge University Press.

Blume, Peter, T*he Public Sector and the Forthcoming EU Data Protection Regulation.* European Data Protection Law , 2017

Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González (2014)

Commissione Europea, *Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale* (doc. 52021PC0206), 2021

Commissione Europea, Smart cities. https:// ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/cityinitiatives/smart-cities_en

European Data Protection Board, Opinion 2007. Nowak.

Iris van de Kerk, *Data Use Versus Privacy Protection in Public Safety in Smart Cities* (Master thesis, University of Utrecht 2015)

L. Camiciotti, C. Racca, *Creare valore con i Big data. Gli strumenti, i processi, le applicazioni pratiche*, Edizioni LSWR, Milano, 2015.

Linda Vlassenrood, *Becoming a Smart Society* (DATAstudio) https://destaatvaneindhoven.hetnieuweinstituut.nl/sites/default/files/datastudio_becoming_a_smart_society_def.pdf

Luca Montag, Rory Mcleod, Lara De Mets, Meghan Gauld, Fraser Rodger, and Mateusz Pełka. *The Rise and Rise of Biometric Mass Surveillance in the Eu – a legal analysis of Biometric Mass Surveillance practices in Germany, The Netherlands and Poland* 2021

Maher, Imelda, *Economic Governance: Hybridity, Accountability and Control*, 2007 Columbia Journal of European Law

Maša Galič, *Surveillance and Privacy in Smart Cities and Living Labs* (PhD, Tilburg University) 2020.

NL smart city strategy: the future of living.. Marzo 19, 2019, https://instituteforfutureofliving.org/wpcontent/uploads/NL_Smart_City_Strategie_EN_LR.pdf.

Oliver, Adam. *From Nudging to Budging: Using Behavioural Economics to Inform Public Sector Policy*, 2013, Journal of Social Politics

Paliotta A.P., *Le politiche innovative di sicurezza nelle città tra*

tecnologie di riconoscimento e smart cities, Sinappsi, 2020

Privacy International, *Smart cities: Utopian vision, Dystopian Reality*, 2017 https://privacyinternational.org/sites/default/files/2017-12/Smart%20Cities-Utopian%20Vision%2C% 20Dystopian%20Reality.pdf

R. De Santis, A. fasano, N. mignolli, A. villa, *Il Fenomeno smart cities, in Rivista Italiana di Economia Demografica e Statistica*, 2014.

R.G. Hollands, *Will the Real Smart City Please Stand Up? Intelligent, Progressive or Entrepreneurial?,* in City, 12-3-2008

Sarah Wray, *Why the City of Amsterdam developed its own crowd monitoring technology,* 2021, https://cities-today.com/why-the-city-of-amsterdam-developed-its-own-crowd-monitoring-technology/

Sengers, F. *Smart-Eco Cities in the Netherlands: Trends and City Profiles* 2016. Exeter: University of Exeter (SMART-ECO Project).

Stefania Carulli, "*Amsterdam, l'avanguardia europea delle smart city"*, 2014, https://www.techeconomy2030.it/2014/05/05/amsterdam-lavanguardia-europea-delle-smart-city/

Surdean, R., *Secure Connections for a Smarter World*, MIPRO 2017 Proceedings, Opatija, Croatia

Tinus Kanters, '*Living Lab Stratumseind*', 2016, www.midpointcsi.nl/ powered-bysocialinnovation/wp-content/uploads/2016/07/LLTrillion2015.pdf

Tinus Kanters, *Living Lab, Onderdeel Van Stratumseind 2.0, Smart Sensors, Smart Interfaces, Smart Actors, Smart Lights, Smart Data, Smart Design, Augmented Reality, Gaming* , Eindhoven, 2013

Van Zoonen, Liesbeth,, *Privacy Concerns in Smart Cities*, Government Information Quarterly, 2013

Willianne Korteweg, *Smart Urban Governance & Good Governance Principles* (Master Thesis, Utrecht University 2019)

RINGRAZIAMENTI

Al termine di questo lavoro ritengo doveroso ringraziare in primis il Prof. Andrea Pin, presidente del corso di laurea, per l'estrema disponibilità ed attenzione verso noi studenti e per aver accolto e seguito la stesura di quest'elaborato.

Il ringraziamento più grande va alla mia famiglia che mi ha supportato durante questi tre anni accademici. Grazie per avermi sempre permesso, fin da quando ero bambino, di essere aperto al mondo e di dare spazio alle mie idee ed ai miei sogni.

Un sentito ringraziamento va a tutte le persone che si sono fermate durante questo percorso. Dalla Calabria, passando dal Veneto fino ai Paesi Bassi. Se state sentendo o leggendo queste parole significa che mi avete lasciato qualcosa. Ogni momento passato insieme ha reso la persona che sono oggi e per questo vi sono grato. Anche se non sappiamo cosa ci riserverà il futuro, so che potrò trovare ciascuno di voi in una frase, una canzone o un ricordo.