HITACHI
Inspire the Next

CONNECTED CITIES

Smart Safety

come le nuove tecnologie digitali possono rendere le nostre città più sicure

The European House
Ambrosetti

The European House – AMBROSETTI

The European House - Ambrosetti è un Gruppo professionale, attivo dal 1965, che supporta le aziende nella gestione integrata e sinergica dei quattro aspetti critici dei processi di creazione di valore: Vedere, Pianificare, Raggiungere e Ottimizzare.

Da oltre 50 anni The European House - Ambrosetti affianca le imprese italiane e fornisce ogni anno consulenza a circa 1.000 clienti, realizzando più di cento scenari strategici e studi rivolti a istituzioni e aziende italiane ed europee.

Per il sesto anno consecutivo, The European House - Ambrosetti è stata nominata - nella categoria “Best Private Think Tanks” - 1° Think Tank in Italia, tra i primi 10 in Europa e nei primi 100 indipendenti su 6.846 a livello globale nell’edizione 2018 del “Global Go To Think Tanks Report” della University of Pennsylvania.

Hitachi Social Innovation

L’Internet of Things (IoT) sta creando nuove opportunità per integrare gli ecosistemi industriali e sociali combinando infrastrutture operative e soluzioni informatiche sofisticate. I principali settori e utilities – come i trasporti, la sicurezza, l’energia e la salute – stanno affrontando trasformazioni che porteranno miglioramenti per tutti gli attori coinvolti. Tali miglioramenti riguarderanno sia le imprese che le amministrazioni pubbliche, e promettono di generare benefici fondamentali per clienti e cittadini.

In Hitachi, l’attività nel campo della trasformazione digitale è definita come “Social Innovation” e consiste nell’uso della tecnologia e di nuovi modelli di business per apportare cambiamenti positivi nella vita delle persone e nella società, creando valore condiviso.

L’obiettivo del Social Innovation Business di Hitachi è quello di sviluppare soluzioni innovative tramite una combinazione di IT e OT (Operational Technology) e un processo di creazione collaborativa con imprese, municipalità, mondo universitario e altri attori pubblici e privati.

Tale impatto positivo può avere una risonanza particolarmente significativa all’interno degli spazi urbani. I servizi delle città e le infrastrutture stanno già sperimentando cambiamenti e trasformazioni che porteranno miglioramenti incentrati sul cliente e vasti livelli di integrazione, apportando benefici significativi sia per i cittadini sia per la società nel suo complesso.

Per avere una visione più ampia delle attività di Social Innovation di Hitachi e per condividere la nostra visione di un futuro digitale incentrato sull’uomo, visitate il sito **http://social-innovation.hitachi/it/**

Sommario

01 Introduzione

L'iniziativa Connected Cities, lanciata da Hitachi e The European House - Ambrosetti, si inserisce nel più ampio quadro di **attività della Social Innovation Business di Hitachi** e mira a disegnare le strategie più efficaci per affrontare le grandi sfide che le comunità, le città e i territori italiani stanno affrontando.

I temi dell'iniziativa includono la trasformazione digitale e l'integrazione dei servizi negli spazi urbani italiani, ponendo il cittadino come attore al centro di città sempre più intelligenti e connesse, con particolare attenzione ai concetti di **sicurezza, mobilità, energia** e **servizi idrici**.

Lo studio è stato realizzato sulla base dei seguenti **pilastri metodologici**:

- **Interviste** con esperti di alto livello e stakeholder coinvolti nello sviluppo urbano, tra cui: funzionari pubblici e autorità comunali, locali e nazionali, responsabili della Trasformazione Digitale delle principali città italiane, aziende private (tra cui fornitori e integratori digitali), erogatori di servizi pubblici, agenzie di trasporto pubblico locale, associazioni di cittadini, leader ed esperti tecnologici, start-up.
- **Survey di alto livello** condotta su un campione di circa 150 esperti qualificati e stakeholder, provenienti da imprese, pubblica amministrazione e mondo accademico.
- **Analisi statistiche** basate su informazioni raccolte attraverso le principali banche dati internazionali e fonti pertinenti.

I risultati di tali attività sono alla base di due diversi studi sulle implicazioni, le priorità e le opportunità future legate alla nascita delle tecnologie digitali e al loro supporto per la creazione di vere e proprie **Connected Cities** in Italia. Nel contesto odierno, le città stanno infatti diventando sempre più importanti e si affermano come dimensione chiave in grado di rispondere efficacemente alle sfide future e ai bisogni più rilevanti dei cittadini.

Pensare le città del futuro come **Connected Cities** significa pianificare e realizzare il loro sviluppo ponendo i cittadini al centro, attraverso un uso efficace della tecnologia e la partecipazione di tutti gli attori e stakeholder che possono svolgere un ruolo positivo in tali progressi.

Nell'ambito del progetto, il presente documento affronta la tematica della **Smart Safety**, uno dei temi più pressanti per il presente e, in particolare, per il futuro degli spazi urbani italiani, che subiscono oggi una **pressione** senza precedenti **per trasformarsi** ed evolversi: da un lato, per rispondere ai bisogni dei cittadini, e dall'altro influenzando i comportamenti e le aspettative dei cittadini stessi e delle comunità.

L'importanza dei temi legati alla sicurezza è confermata dai risultati della survey di alto livello: il **73% degli intervistati concorda sul fatto che il tema della sicurezza pubblica ha un ruolo sempre più cruciale per cittadini e comunità locali**, dichiarando che tale tema guiderà e influenzerà le loro scelte e i loro programmi futuri come decisori delle Connected Cities italiane.

Smart Safety è una definizione ampia che comprende molteplici aree di intervento e interessa una pluralità di attori e stakeholder. Si riferisce al modo in cui le tecnologie e i progressi dei modelli operativi e organizzativi, resi possibili dalla digitalizzazione, contribuiscono a nuovi paradigmi di sicurezza dei cittadini tout court (salute, mobilità, sicurezza sul posto di lavoro, affidabilità delle infrastrutture, …).

Si basa sulla diffusione di tecnologie e infrastrutture che consentono la raccolta di una quantità di dati senza precedenti. Tali tecnologie stanno riscrivendo il concetto stesso di sicurezza, creando un ambiente di "Smart Safety" in cui l'**individuo è allo stesso tempo utente e contributore**.

La Smart Safety interessa diversi luoghi. Questo studio si concentra sugli "**Spazi Sociali**", che comprendono non solo gli spazi pubblici, ma anche i luoghi privati ad uso pubblico (come ad esempio aeroporti, stazioni ferroviarie, metro, piazze pubbliche, centri commerciali, …).

Grazie alle evoluzioni tecnologiche, le **città sono diventate più connesse, più monitorate, più digitalizzate**. Un flusso costante di dati scorre all'interno degli spazi sociali, crescendo e ampliandosi costantemente. Una trasformazione così importante incide su ogni aspetto della gestione dello spazio e della vita dei cittadini, permettendo di soddisfare vecchie esigenze di sicurezza e creandone di nuove.

In questo momento - percepito da molti come un momento di radicale trasformazione nelle aree urbane e nella loro pianificazione - questo studio **inquadra e indaga la reale portata di tali processi**, discutendo scenari e obiettivi futuri e le priorità per raggiungerli.

Per fare ciò, le nostre analisi definiscono le principali tendenze e le sfide rilevanti con l'obiettivo di comprendere come le nuove tecnologie e i modelli organizzativi possano fornire soluzioni efficaci di "Smart Safety", ponendo i **cittadini e le loro esigenze al centro dei servizi**.

Il documento vuole **supportare i policymaker** italiani e accompagnarli nella trasformazione digitale, indagando come i temi legati alla sicurezza si stiano trasformando nel tempo e come le tecnologie innovative siano essenziali per gestire la Smart Safety nell'ambito di una vera e propria Connected City.

La struttura dello studio è la seguente:

- Il capitolo 2 analizza i principali fattori e scenari che stanno rimodellando gli spazi urbani;
- Il capitolo 3 analizza i trend e le prospettive future;
- Il capitolo 4 tratta le criticità più rilevanti e le sfide più urgenti;
- Il capitolo 5 descrive quali soluzioni tecnologiche innovative possono essere utilizzate per affrontare tali criticità e sfide e cosa occorre per porle in essere;
- Il capitolo 6 riassume le priorità di intervento.

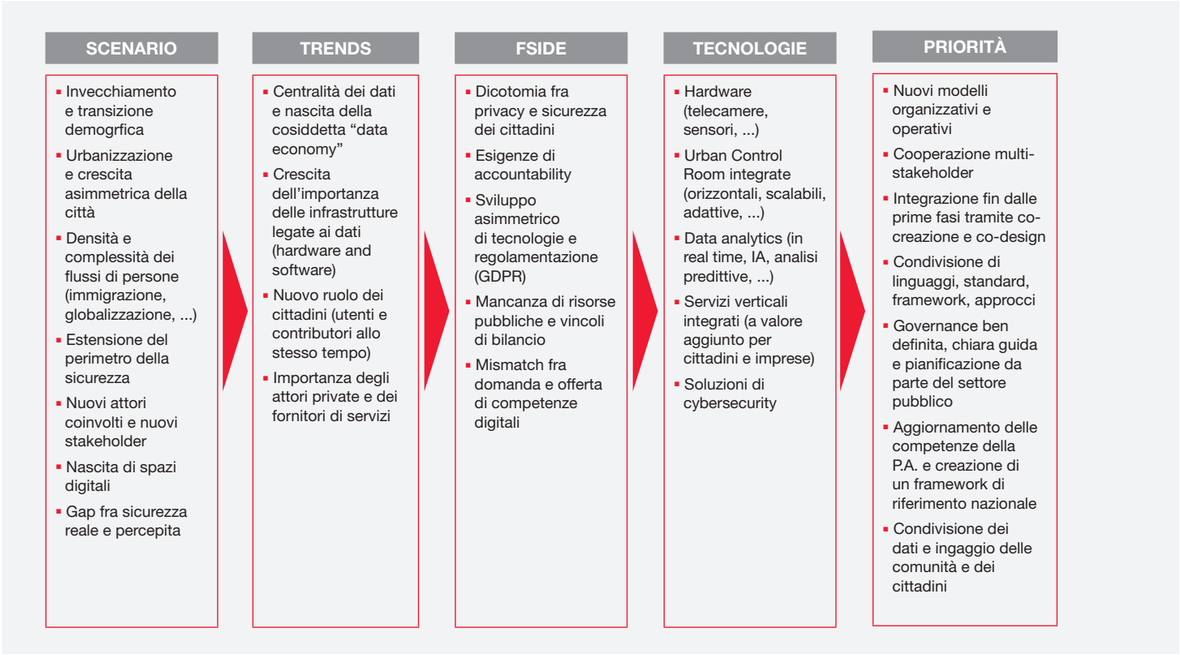


Figura 1. Flusso logico dello studio. Fonte: The European House - Ambrosetti, 2019

Punti chiave dello studio

01 Città Connesse

Gli sviluppi tecnologici promettono oggi di rimodellare e trasformare le aree urbane. La sicurezza rimane un tema centrale per gli attori coinvolti nella pianificazione cittadina, nello sviluppo delle città italiane e nella gestione dei servizi. Come evidenziato dai risultati della survey, il **73% degli intervistati concorda sul fatto che il tema della sicurezza pubblica è ritenuto sempre più cruciale dai cittadini e dalle comunità locali**, dichiarando che tale tema guiderà e influenzerà le loro scelte e programmi come stakeholder delle future Connected Cities.

02 Urbanizzazione

Le esigenze fondamentali e le caratteristiche stesse della sicurezza si stanno evolvendo in uno **scenario in rapida trasformazione**. L'evoluzione demografica e l'invecchiamento della popolazione italiana stanno rimodellando i bisogni e le esigenze di sicurezza. L'espansione delle città produce una crescita asimmetrica, aumentando la pressione sulle periferie, generando vuoti urbani e aree densamente popolate. Aumenta la densità e la complessità dei flussi di persone (turisti, pendolari, migranti, ...), aggiungendo rischi e sottolineando la necessità di un rinnovato paradigma di sicurezza nelle aree urbane italiane.

03 Perimetro di sicurezza

Parallelamente, il **perimetro stesso della Safety va espandendosi**: mentre la sicurezza rimane fondamentale, i cittadini diventano sempre più consapevoli delle nuove problematiche e le includono nella loro definizione di sicurezza, trasformando di conseguenza le loro esigenze (es. sicurezza infrastrutturale, sicurezza ambientale, salute, ...). Nuovi attori sono coinvolti nella fornitura di servizi di sicurezza ed emergono nuovi spazi da tenere in considerazione (come lo spazio digitale, che apre le porte al tema della sicurezza dei dati). Infine, un crescente divario tra sicurezza percepita e sicurezza reale aumenta l'importanza della creazione di un ambiente manifestatamente sicuro.

04 Trasformazione digitale

Così come diversi altri settori, i servizi legati alla sicurezza si trovano oggi nelle fasi iniziali della cosiddetta "trasformazione digitale". Ciò è reso possibile soprattutto grazie ai dati (raccolta, accumulo, archiviazione, analisi, ...) nell'ambito dell'emergente **data economy**. Ciò comporta anche una crescente rilevanza di nuove infrastrutture e tecnologie (data center, 5G, interconnettori, ...), nuove capacità e competenze (analisi dei dati, sicurezza informatica, ...), e nuovi attori (anche privati).

05 Cittadini "smart"

La trasformazione delle città in Connected Cities e l'erogazione di servizi cosiddetti Smart, basati sui dati, trasforma i cittadini in cittadini smart: diventano al tempo stesso **utenti e contribuenti** di tali servizi. Gli individui diventano nodi chiave all'interno della rete urbana digitalizzata. Allo stesso tempo, sono anche uno degli anelli più vulnerabili della catena digitale, con ripercussioni sulla sicurezza informatica dell'intero sistema. Per questi motivi, la loro inclusione fin dall'inizio del progetto di una Connected City è cruciale.

06 Smart Safety

In tale scenario, la Smart Safety incentrata sull'uso di dati genera diverse ripercussioni e implicazioni. La più importante è legata all'uso dei dati personali: **emerge** un **compromesso tra sicurezza e privacy dei cittadini**, poiché servizi di sicurezza più efficaci richiedono quantità sempre più pervasive di dati personali. La discussione sul trattamento dei dati personali ha catturato l'attenzione dell'opinione pubblica, e la consapevolezza sociale sul valore delle informazioni private sta crescendo. Pertanto, l'**accountability** diventa un requisito obbligatorio per ogni piattaforma digitale integrata, al fine di costruire un sistema inclusivo in cui ogni attore (cittadini, settore pubblico, servizi e fornitori di sicurezza) ha visibilità sulle modalità di utilizzo dei dati.

07 GDPR

In questo quadro in evoluzione, la **regolamentazione svolge un ruolo centrale**. Lo sviluppo normativo non sempre promuove l'innovazione, creando un ambiente non favorevole allo sviluppo, né fornisce il miglior equilibrio tra la protezione dei cittadini e la fornitura di servizi. La General Data Protection Regulation (GDPR), l'ultima disposizione emanata dalla Commissione Europea, introduce una serie di severi requisiti per coloro che raccolgono, conservano e gestiscono dati privati. Il regolamento crea quindi la necessità di un'architettura digitale in grado di soddisfare tali requisiti.

08 Urban Control Room

Le tecnologie oggi disponibili permettono di risolvere molti degli attuali problemi, consentendo la creazione di Connected Cities efficienti ed efficaci, in grado di fornire servizi innovativi di Smart Safety che pongano al centro le nuove esigenze delle comunità e dei cittadini. A tal fine, **l'integrazione di tutti gli attori coinvolti nella pianificazione, nello sviluppo e nella gestione urbana è fondamentale**. Questa integrazione può essere abilitata da una piattaforma orizzontale, la cosiddetta Urban Control Room, che permetta di raccogliere, archiviare e analizzare i dati provenienti da diverse fonti (antenne urbane, fornitori di servizi, cittadini....). Sotto il controllo pubblico, tale piattaforma trasforma i dati grezzi in informazioni, analisi, metriche e KPI significativi, consegnandoli ai fornitori di servizi verticali, creando servizi integrati efficaci.

09 Intelligenza Artificiale

Insieme alla Control Room, altre tecnologie possono supportare la creazione di sistemi innovativi di Smart Safety, superando le criticità esistenti (scarse capacità e competenze digitali, riduzione dei bilanci pubblici, ...). Tra le varie tecnologie disponibili, ad esempio, contatori, sensori e antenne consentono la raccolta di dati utili provenienti da diverse fonti. I software di analisi basati sull'Intelligenza Artificiale permettono **analisi in tempo reale**, fornendo informazioni preziose alle forze dell'ordine e ad altri fornitori di servizi. È possibile anche effettuare analisi predittive, mentre la sicurezza informatica diventa un prerequisito (sia a livello hardware che software) in un sistema integrato di questo tipo.

10 Integrazione

Per ottenere i risultati di cui sopra, l'**integrazione è il prerequisito principale**. Per creare questa piattaforma orizzontale e alimentarla con dati significativi, consentendo l'implementazione di servizi verticali intelligenti, tutte le parti interessate dovrebbero collaborare. Sono necessari nuovi modelli operativi e organizzativi e nuove competenze e capacità a tutti i livelli della Pubblica Amministrazione. La **co-progettazione e il cosviluppo** di tecnologie, infrastrutture e servizi sono elementi essenziali per consentire un'integrazione efficace e devono essere perseguiti fin dall'inizio, insieme a una chiara governance e a un approccio strategico che ponga i cittadini e le comunità al centro di tali processi.

02 Connected Cities e scenario italiano

Il paradigma della “Smart Safety1” applicato alle città italiane si inserisce in un contesto di grandi **trasformazioni attualmente in atto nella società italiana** e iniziate negli ultimi decenni. Diversi **trend** hanno avuto, e continuano ad avere, un impatto rilevante sulla sicurezza pubblica nelle aree urbane. Tra questi, il rimodellamento della popolazione urbana sia in termini di struttura demografica che in termini di bisogni, la nascita della cosiddetta data economy e il crescente divario tra sicurezza reale e percepita. ›

Ognuna di queste trasformazioni incide sul contesto della sicurezza e richiede nuove soluzioni per affrontarla. Il primo passo è quindi **la comprensione**, da parte dei decisori urbani e nazionali, e di tutti gli attori coinvolti nelle decisioni e nelle attività di pianificazione urbana e di sviluppo urbano, **di tali tendenze**.

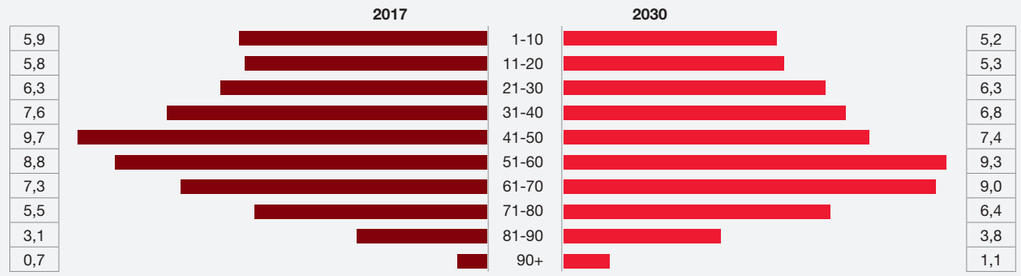
Per questo motivo, il presente capitolo **inquadra lo scenario di riferimento per la Smart Safety** nelle città italiane, indagando l’evoluzione della domanda di sicurezza negli ultimi anni.

Il primo trend individuabile riguarda i **cambiamenti nella composizione della popolazione**. L’invecchiamento, i fenomeni migratori e l’urbanizzazione hanno trasformato la demografia delle aree urbane, portando nuove priorità ed esigenze in termini di sicurezza.

La popolazione italiana sta progressivamente invecchiando: è una tendenza iniziata oltre 30 anni fa e si prevede che continuerà in futuro, come evidenziato dal confronto tra l’attuale struttura demografica rispetto alla proiezione al 2030:

- Nel 1980, l’età media in Italia era di 35,4 anni, nel 2000 era di 40,9 anni, nel 2018 di 44,7 anni. La tendenza dovrebbe continuare a causa del progressivo aumento dell’aspettativa di vita e del calo del tasso di natalità [2], raggiungendo un’età media attesa al 2030 di 47,1 anni. [3]
- La conseguenza di tale processo di invecchiamento è la **crescita della quota della popolazione over 65** sulla popolazione italiana totale (tale quota è passata dal 12,1% nel 1980 al 17,0% nel 2000, al 21,4% nel 2018 e si prevede un ulteriore aumento al 25,3% nel 2030).

Figura 2. Struttura demografica per classi di età in Italia (milioni di persone), 2017 e 2030. Fonte: elaborazione The European House - Ambrosetti su dati Istat e UN population prospects, 2019



Questo processo di invecchiamento influisce sulle esigenze di sicurezza della popolazione. Ad esempio, una ricerca condotta negli Stati Uniti [4] ha dimostrato come, sebbene le persone più anziane rappresentino circa l’11% della popolazione, essi siano oggetto di circa il 23% dei decessi accidentali. Inoltre, i cittadini più anziani vivono con più difficoltà gli spostamenti, sia considerando i trasporti (pubblici e privati) che gli spostamenti a piedi. [5] Tali preoccupazioni necessitano un monitoraggio più approfondito e distribuito sul territorio, concentrandosi sulla prevenzione e richiedendo, allo stesso tempo, capacità di risposta rapida. Devono essere presi in considerazione anche gli investimenti per realizzare un profondo ridisegno delle città, creando un ecosistema urbano più vicino alle esigenze della popolazione più anziana (ad esempio intervenendo sulle infrastrutture, sulla mobilità, rimuovendo le barriere architettoniche in edifici e spazi pubblici, …).

Il progressivo invecchiamento della popolazione italiana è accompagnato da un costante processo di urbanizzazione. Non si tratta di una tendenza recente – il processo di **urbanizzazione** in Italia è infatti iniziato più di 50 anni fa - ma negli anni ha lentamente e costantemente modificato la struttura delle città e le aspettative dei cittadini in termini di sicurezza. L’impatto maggiore riguarda il modo in cui gli spazi urbani devono essere pensati e progettati:

- Nelle due maggiori città italiane (Roma e Milano) vive oggi il 7% della popolazione italiana totale. [6] Solo cinque anni fa il 6,5% della popolazione italiana viveva in queste due città (senza considerare le loro aree metropolitane). In generale, **la popolazione delle dieci città italiane più grandi èaumentata del 6,5% dal 2012 al 2018**, a fronte di una crescita generale della popolazione nazionale media dell’1,8%.

Tabella 1. Popolazione nelle dieci maggiori città italiane (abitanti), 2012 e 2018. Fonte: elaborazione The European House - Ambrosetti su dati Istat, 2019.

	2012	2018	Variazione
Romo	2,614,263	2,872,800	+ 9,9 %
Milano	1,240,173	1,366,180	+ 10,2 %
Napoli	961,106	966,144	+0,5 %
Torino	869,312	882,523	+ 1,5 %
Palermo	656,829	668,405	+ 1,8 %
Genova	584,644	580,097	- 0,8 %
Bologna	371,151	389,261	+ 4,9 %
Firenze	357,318	380,948	+ 6,6 %
Bari	315,408	323,370	+ 2,5 %
Catania	293,104	311,620	+ 6,3 %

1 Sia il termine “safety” che il termine “security” vengono tradotti in italiano con “sicurezza”, anche se afferiscono a due diversi ambiti. In particolare, la security indica protezione da minacce e attacchi deliberati a cose o persone (come ad esempio la criminalità), mentre la safety indica la protezione da rischi e incidenti fortuiti che possono pregiudicare l’incolumità o la salute. Nel documento è utilizzato il termine safety, in quanto più ampio ed inclusivo.

2 Inoltre, nel 2017 il saldo demografico - la differenza tra nascite e decessi - è stato per la prima volta negativo.

3 Fonte: elaborazione The European House – Ambrosetti su prospettive demografiche Istat e ONU, 2019.

4 Evolve Resources for Basic Geriatric Nursing, 6a edizione, Patricia A. Williams, RN, MSN, MSN, CCRN.

5 Il tasso di mortalità dei conducenti di età superiore agli 85 anni è nove volte superiore a quello dei conducenti di età compresa tra i 25 e i 69 anni; la velocità di camminata delle persone di età superiore ai 65 anni è quasi la metà rispetto alla velocità media di un giovane.

6 In Italia, più di 9,5 milioni di persone vivono nelle città metropolitane. Di questi, si stima che più di un terzo viva in periferie dove le difficoltà economiche sono più sentite.

- Parallelamente, in molte città italiane **le periferie stanno vivendo una rapida crescita**, la popolazione ivi residente sta aumentando ad un ritmo molto sostenuto. Tale crescita è solitamente inorganica e mette sotto pressione le amministrazioni comunali, che devono far fronte sia al sovraffollamento di alcune aree che alla comparsa dei cosiddetti "vuoti urbani" in altre. Tale coesistenza di fratture urbane e aree congestionate incide sulla sicurezza cittadina e sul modo in cui viene gestita.

La pressione sulla sicurezza è determinata anche da una **maggiore densità e complessità dei movimenti e nei flussi di persone**.

- **Le migrazioni sono in aumento**. Nonostante non ci sia alcuna "emergenza migratoria" [7], la mancanza di un piano strutturato di gestione e integrazione dei migranti nelle città italiane crea un ambiente che pone nuove minacce per la sicurezza sia dei migranti che dei residenti, soprattutto nelle periferie urbane e nei cosiddetti "vuoti urbani".
- Anche i **flussi ordinari** sono in aumento a causa della globalizzazione e della crescente interconnessione delle diverse aree geografiche. Ad esempio, tra il 2012 e il 2018 il volume di turisti in visita in Italia è aumentato del 10,5%, raggiungendo nell'ultimo anno sono stati registrati oltre 420,6 milioni di turisti. Nelle 10 città più grandi, citate nella tabella precedente, il tasso di crescita del turismo è stato del 20,2%. L'ultimo anno sono stati registrati più di 96 milioni di turisti. [8]

Tale complessità comporta **esigenze di sicurezza molto diverse**, provenienti da soggetti sempre più eterogenei, e fa sì che le geometrie urbane cambino rapidamente e in modo difficile da prevedere. Questi fenomeni richiedono anche un monitoraggio più complesso e flessibile (sia della società che degli spazi).

In conclusione, questa combinazione di invecchiamento, aumento dei flussi urbani e urbanizzazione sta drasticamente ridisegnando la struttura degli Spazi Sociali con riferimento alla Smart Safety, esercitando una **maggiore pressione** sia sulle aree cittadine che sui soggetti coinvolti nella pianificazione delle città, e rende più complesso fornire adeguati livelli di sicurezza agli individui.

L'importanza delle questioni relative alla sicurezza è confermata dai risultati dell'indagine: il 73% degli intervistati concorda sul fatto che il tema della sicurezza pubblica è percepita come più cruciale da parte dei cittadini, e guiderà quindi le scelte degli intervistati e i loro programmi futuri. I risultati della survey confermano come il crescente stress sugli spazi sociali, e in generale il sovraffollamento, sia una delle principali preoccupazioni legate alla sicurezza, come mostrato in *figura 4.*

Un secondo macro-trend riguarda l'**evoluzione del concetto stesso di sicurezza**, in quanto il perimetro della "sicurezza urbana" si va allargando fino a comprendere **ambiti aggiuntivi** diversi dalla sicurezza in senso stretto (ovvero la sicurezza legata alla criminalità, alla violenza, al terrorismo, …). Questi ambiti diventano ugualmente – o forse assumono un ruolo ancora più importante – nella vita quotidiana dei cittadini, e sono per certi versi molto più difficili da garantire in modo efficace:

- I cittadini chiedono forme di protezione diverse ed estese, mentre la **sicurezza percepita** diventa sempre più rilevante, accanto a quella reale.
- **Nuovi spazi digitali e virtuali** emergono accanto a quelli tradizionali. Questi spazi, tradizionali e digitali, si influenzano a vicenda, e la sicurezza di uno si ripercuote sulla sicurezza dell'altro.

In particolare, l'estensione del perimetro della sicurezza urbana comprende temi quali l'**ambiente, la salute e l'obsolescenza delle infrastrutture:**

- Terremoti, inondazioni, ondate di calore e danni dovuti al vento intenso minacciano la sicurezza degli individui. Nel 2016, in Italia, ci sono stati 20.629 decessi dovuti a condizioni meteorologiche e climatiche estreme. [9]
- In Italia ci sono circa 45.000 ponti e gallerie. Di questi, circa 11.000 (il 25%) hanno bisogno di sorveglianza e manutenzione regolare. Ci sono inoltre più di 2 milioni di abitazioni in mediocre o pessimo stato di conservazione. [10]
- L'inquinamento atmosferico è responsabile ogni anno in Italia di circa 30.000 morti per il solo particolato fine (PM 2,5), pari al 7% dei decessi complessivi (escludendo i decessi dovuti ad incidenti). In termini di mesi di vita perduta, l'inquinamento accorcia la vita di ogni italiano di una media di 10 mesi: 14 per chi vive al Nord, 6,6 per gli abitanti del Centro e 5,7 per il Sud e le isole. [11]

I risultati della survey confermano tale pluralità di esigenze e di priorità di intervento, evidenziando l'ampiezza dell'attuale definizione e del concetto di sicurezza urbana.

Figura 3. Percentuale della popolazione che ritiene che le questioni ambientali abbiano un effetto diretto sulla vita quotidiana e sulla salute (percentuale), 2017.
Fonte: elaborazione The European House - Ambrosetti su dati Eurobarometro, 2019

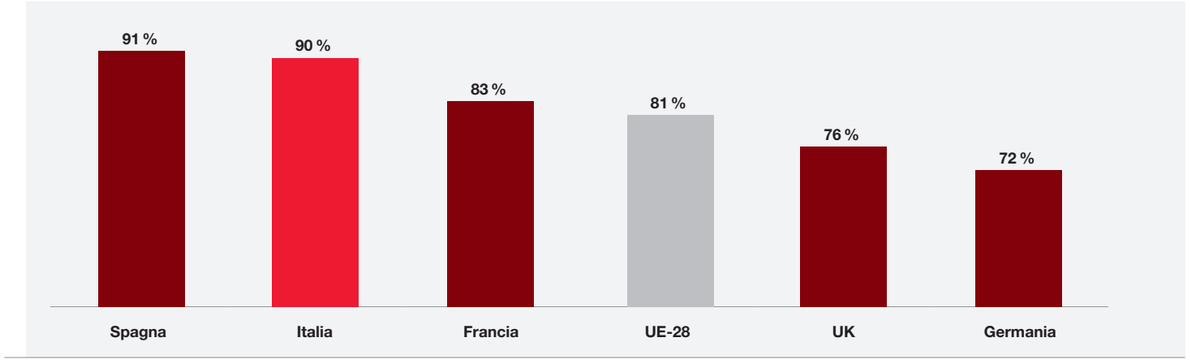
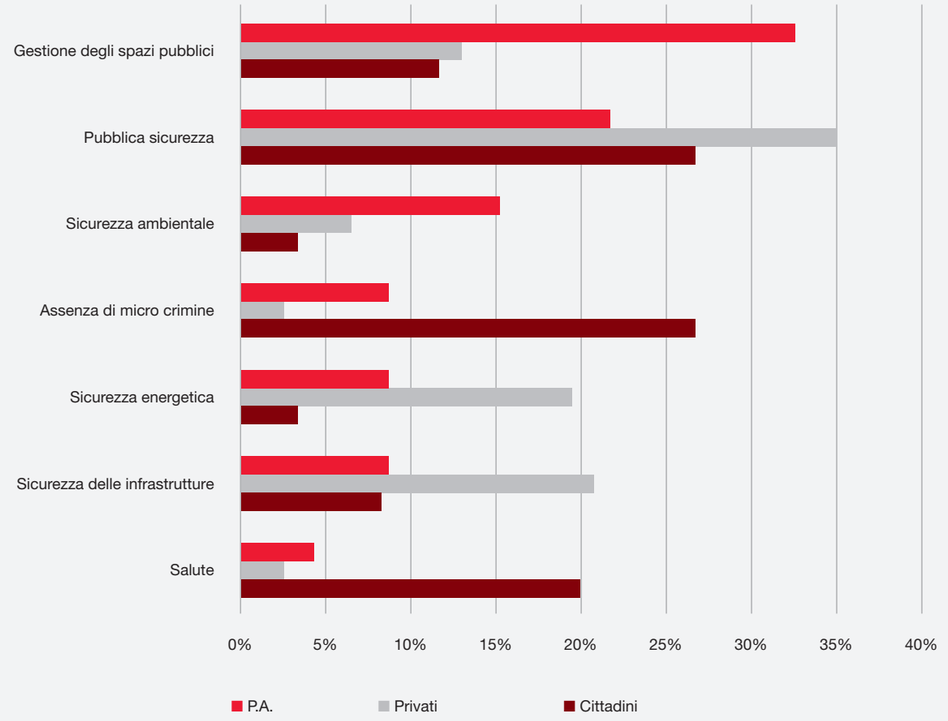


Figura 4. Risposte alla domanda: "Quali aspetti considera parte integrante del concetto di sicurezza per i cittadini?" per intervistati (percentuale sul totale), 2019.
Fonte: elaborazione The European House - Ambrosetti su risultati della survey, 2019



7 In Italia ci sono circa 4 milioni di immigrati registrati, il 6,7% rispetto alla popolazione totale, contro il 9,9% in Austria, l'8,5% in Francia, l'8% in Germania e l'11,6% in Svezia. Gli immigrati clandestini sono stimati essere al di sotto dell'1% della popolazione totale.

8 Fonte: elaborazione The European House - Ambrosetti su dati Istat, 2019.

9 Fonte: elaborazione The European House - Ambrosetti dei dati dell'Agenzia europea dell'ambiente, 2019.

10 Fonte: elaborazione The European House - Ambrosetti su dati Istat e Scenari Immobiliari, 2019.

11 Fonte: elaborazione The European House - Ambrosetti su dati Ministero della Salute, 2019.

Parallelamente, cresce anche lo spettro dei soggetti coinvolti nell'organizzazione e gestione della sicurezza urbana. Negli ultimi anni, **la gestione della sicurezza è diventata una responsabilità di una pluralità di soggetti**, coinvolgendo sia attori istituzionali a diversi livelli - sovranazionale (UE), nazionale e locale - sia attori privati.

Accanto agli spazi tradizionali, **nuovi spazi emergono** grazie alle innovazioni e ai progressi tecnologici. I dati digitali sono oggi un asset prezioso. L'estrazione, l'archiviazione e l'utilizzo dei dati creano anche nuove professioni e nuovi business. Richiedono nuove infrastrutture, nuovi investimenti e nuove competenze, abilitando nuovi modelli di business. In altre parole, i dati stanno creando un'economia di per sé, una **data economy** in cui il valore è rappresentato dall'informazione che può essere ricavata dai dati.

Allo stesso tempo, la digitalizzazione sempre più pervasiva e l'importanza crescente delle tecnologie digitali hanno portato alla nascita di un nuovo spazio: il cosiddetto "**spazio digitale**". Come succede con gli spazi fisici, lo spazio digitale richiede specifiche azioni per garantirne la sicurezza individuale e collettiva:

- Con l'aumento della pervasività dei dati, della frequenza della loro raccolta e delle fonti disponibili **aumentano anche le dimensioni e la profondità delle informazioni potenzialmente acquisibili**. Elettrodomestici intelligenti, tecnologie indossabili, sensori per uso industriale, app, strumenti di pagamento avanzati e registri elettronici della pubblica amministrazione sono solo alcuni esempi di fonti di dati grezzi da cui è possibile ricavare una quantità sempre maggiore di informazioni.

- **La dimensione globale dei dati dovrebbe raggiungere cumulativamente i 44 zettabyte** (44 trilioni di GB) entro il 2020, dieci volte la dimensione attuale. [12] Il valore della data economy dovrebbe superare i 100 miliardi di euro entro il 2020 (il doppio rispetto al Giappone, la metà degli Stati Uniti).

- **L'economia dei dati in Italia vale 28,4 miliardi di euro**, con un peso sul PIL pari all'1,5%. Si prevede che tale peso si attesti tra il 2 e il 3,5% del PIL nel 2020. Nel 2021 il traffico dati sarà 1,8 volte superiore a quello del 2018, con un tasso di crescita del 23% all'anno.

- Per contro, in Italia, **nell'ultimo anno si sono verificati oltre 10.000 attacchi informatici**. Il 76% di questi attacchi sono furti di database. Il 61% degli attacchi informatici sono perpetrati utilizzando tecniche di attacco non sofisticate (SQLi, DDoS, Known Vulnerabilities, Phishing e Simple Malware). Tuttavia, questi attacchi risultano efficaci a causa della mancanza di investimenti adeguati e di protezioni digitali. [13]

- Nel 2017 il mercato delle soluzioni di sicurezza informatica in Italia ha raggiunto un valore di **1,09 miliardi di euro**, in crescita del 12% rispetto al 2016. Tuttavia, il 78% di tali investimenti è effettuato esclusivamente da grandi imprese private.

L'importanza degli spazi digitali è quindi chiara, e si accompagna alla necessità di garantirne la sicurezza per proteggere efficacemente le persone e i cittadini. A tal fine è fondamentale una forte **cooperazione** tra gli attori privati, le imprese del settore delle ICT, le autorità di regolamentazione, la pubblica amministrazione, le forze dell'ordine e, naturalmente, i cittadini.

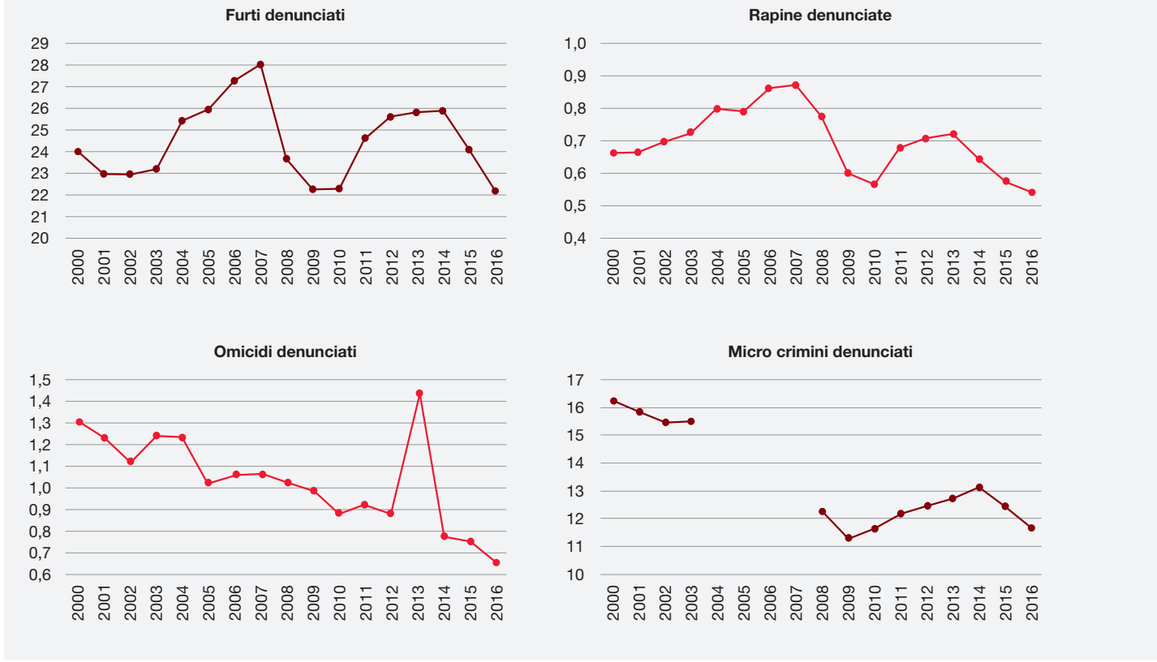
La sicurezza degli spazi digitali richiede misure e decisioni che coprano un ampio spettro di argomenti complessi (come la protezione della privacy, la cyber-security, la conservazione e la trasmissione dei dati, …) che possono avere gravi effetti anche sugli spazi fisici, creando un **rapporto simbiotico** che deve essere chiaro a tutti i soggetti coinvolti nel garantire la sicurezza dei cittadini nelle città italiane.

Parallelamente - e contro intuitivamente - la disponibilità di così tante informazioni, insieme alla crescente rilevanza delle piattaforme digitali (ancora immature nel loro ruolo di media), porta ad un bias della percezione pubblica. Emerge il fenomeno delle fake news, mentre il **divario tra la sicurezza reale e quella percepita** rappresenta una questione nuova che deve essere affrontata. Infatti, nonostante la costante diminuzione di molti indicatori di criminalità, i cittadini italiani dichiarano di sentirsi meno sicuri che in passato.

12 Fonte: Commissione europea – "Comunicato stampa, Data in the UE: Strong Commission commitment to increase data availability and promote data sharing in healthcare", Bruxelles, 25 aprile 2018.

13 Fonte: Relazione Clusit sulla sicurezza in Italia, 2018.

Figura 5. Principali indicatori di criminalità (reati segnalati per 1.000 abitanti), 2000-2016 (non sono disponibili i dati relativi ai microcrimini segnalati per il periodo 2004-2007). Fonte: elaborazione The European House - Ambrosetti su dati Istat, 2019



- Nonostante la riduzione degli indicatori di criminalità, riportati nei grafici precedenti, il "**Rischio criminale percepito**" (indicatore elaborato dall'Istat, calcolato come il numero di famiglie che vivono in condizioni di disagio elevato, a rischio di criminalità, nell'area in cui vivono rispetto al totale delle famiglie) è cresciuto da 30,6 rischi segnalati per 1.000 abitanti nel 2000 a 38,9 nel 2016.

- Il **37% degli italiani ritiene di trovare un'informazione che travisa la realtà**, o addirittura falsa, ogni giorno. Le fake news sono percepite come un problema dal 90% della popolazione. [14]

- Solo il **25% della popolazione dichiara di non avere sufficiente fiducia nella propria capacità di distinguere correttamente tra notizie vere e false**: la restante maggioranza è convinta di essere in grado di identificare le fake news.

- Secondo il Perils of Perception 2017 - un'indagine che esplora la **differenza tra i dati di fatto e la percezione** progettata da Ipsos - il 49% della popolazione ritiene che il tasso di omicidi sia stato più alto nel 2015 rispetto al 2000, e il 35% ritiene che sia stato uguale. In realtà, c'è stato un forte calo del tasso di omicidi negli ultimi due decennis.

La sicurezza sta diventando un tema sempre più complesso: nuovi spazi, nuove esigenze e nuovi attori richiedono l'adozione di soluzioni innovative, rese possibili dall'innovazione e dalla digitalizzazione. Per questo motivo, il capitolo seguente cercherà di chiarire le principali tendenze derivanti dallo scenario di "Smart Safety", al fine di fornire una base di conoscenza per i decisori e gli stakeholder delle città italiane.

14 Fonte: elaborazione The European House – Ambrosetti su dati Eurobarometro, 2019.

03 Trend emergenti

Con l'aumentare della complessità dello scenario di riferimento, i **nuovi trend** richiedono un'attenzione specifica. Lo scopo di questo capitolo è quello di identificare i trend rilevanti legati al paradigma della "Smart Safety" e di evidenziarne le sottostanti implicazioni. L'obiettivo è quello di supportare i decisori nella progettazione di strategie di sviluppo urbano efficaci e solide.

Il primo trend riguarda la **crescente importanza dei dati**. Oggi i dati sono un asset a pieno titolo (così come il petrolio, l'acqua, il capitale umano, …) sia per gli attori privati che per i responsabili politici, i decisori e i cittadini. Come tali, essi hanno implicazioni inevitabili per la sicurezza:

- Le informazioni sensibili e i dati puntuali alla base di queste informazioni si affermano oggi come il principale fattore abilitante per lo sviluppo di servizi di **Smart Safety**.
- Il livello di sicurezza che le città saranno in grado di fornire dipenderà sempre più dall'entità e dalla **profondità** dei dati dei cittadini disponibili (correlazione diretta).
- La velocità del processo di raccolta dati e la capacità di trasformarli rapidamente in **KPI e informazioni** utilizzabili saranno anch'esse cruciali. Le forze dell'ordine, così come altri fornitori di sicurezza e gestori di città coinvolti nella definizione di strategie urbane a lungo termine necessitano di informazioni processate, analisi e KPI piuttosto che di grandi quantità di microdati disaggregati.

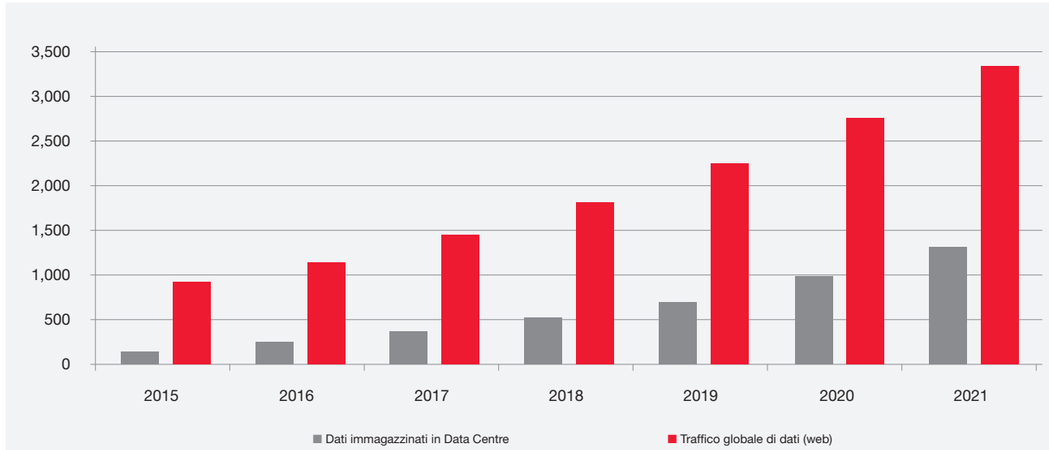
Di conseguenza, diverse **esigenze** si stanno affermando:

- Capacità di **raccogliere** dati da diverse fonti, in tempi diversi, in modo capillare e pervasivo, conformemente alla vigente normativa su privacy e dati.
- **Aggregazione** dei dati e loro **trasformazione** in informazioni di valore, KPI, analisi ed evidenze.
- **Conservazione e protezione dei dati**, in maniera tale da garantirne l'integrità e prevenire abusi.

Per soddisfare tali esigenze sono necessarie **sia soluzioni hardware che software**. Con l'aumento dei volumi di dati, le infrastrutture di base devono crescere di conseguenza.

- I software in grado di **estrarre valore** da quantità crescenti di dati saranno sempre più preziosi. Tali software devono essere in grado di reagire in tempo reale agli input, garantendo una risposta immediata.
- Per quanto riguarda l'hardware, i **data centre** industriali diventeranno asset strategici. Saranno fondamentali anche le infrastrutture a supporto di sistemi altamente digitalizzati (cavi, connettori, satelliti e reti di telecomunicazione).
- Il sistema-Paese, con i suoi asset e le sue infrastrutture, dovrà sostenere tali evoluzioni. A titolo di esempio, il sistema energetico dovrà essere pronto a soddisfare l'aumento di domanda di elettricità. Nel 2014, ultimo anno per il quale sono disponibili i dati, **i data center statunitensi hanno utilizzato il 2% dell'energia elettrica consumata nel Paese**. In tutto il mondo, i data center hanno utilizzato circa lo 0,9% del consumo complessivo di energia elettrica, ma si prevede che entro il 2025 la cifra supererà il 5%. Significativo anche l'impatto ambientale: le emissioni di CO_2 dei Data Centre mondiali ammontano al 2% del totale globale: una quota pari a quella del trasporto aereo. [15]

Figura 6. Previsione della crescita del traffico dati e del volume di dati memorizzati nei Data Centre globali (milioni di terabyte), 2015-2021. Fonte: elaborazione The European House - Ambrosetti su dati Cisco, 2019



In questo contesto, **il ruolo dei cittadini** nell'ambito della sicurezza urbana è in crescita:

- Con l'aumento della centralità dei dati, i cittadini diventano allo stesso tempo **fruitori e contributori** di sicurezza.
- I cittadini guidano **l'estensione del concetto di sicurezza**, richiedendo anche quei servizi e quegli aspetti "soft" discussi nel capitolo precedente, che sono più che mai percepite di fondamentale importanza.
- Crescono anche le **esigenze e le aspettative in materia di sicurezza dei cittadini**. La diffusione capillare degli smartphone e la possibilità di connettersi con il mondo in tempo reale rendono gli individui costantemente consapevoli di ciò che accade nelle loro vicinanze: siamo al punto in cui il modo più veloce per sapere cosa sta succedendo è leggere Twitter. L'accelerazione e la frammentazione della trasmissione delle informazioni implicano che gli individui siano costantemente informati di ogni problema che può verificarsi, sia esso reale o solamente percepito.
- I cittadini diventano **nodi chiave** della Smart Safety. Negli spazi digitali l'"infezione di un singolo nodo" rischia di generare ripercussioni a livello di sistema e non solo: il ruolo dei cittadini è quindi essenziale anche per garantire la sicurezza del sistema stesso. In tale direzione è auspicabile un percorso condiviso di "alfabetizzazione digitale", in quanto la robustezza di un sistema digitale verrà sempre più misurata sulla base del suo anello più debole.

Insieme al coinvolgimento dei cittadini, diventa centrale anche il **ruolo degli attori privati** nella sicurezza urbana:

- **Molti spazi sociali sono gestiti privatamente** (per esempio i centri commerciali e gli stadi). Poiché le tendenze demografiche discusse nel capitolo precedente contribuiscono a modificare le abitudini e le strutture dei consumatori, la conseguenza è una trasformazione dei compiti del settore privato in materia di sicurezza.
- Inoltre, gli attori privati sono sempre più coinvolti nel processo di raccolta dei dati dei cittadini. Tali dati, anche se non strettamente legati alla sicurezza, devono essere messi a sistema assieme a tutti i dati a gestione pubblica (trasporti, energia, acqua, acqua, salute, ...) per fornire KPI, informazioni e analisi che possano essere utilizzati per i servizi di Smart Safety integrati.

15 Fonte: "Geopolitica dell'era digitale", The European House - Ambrosetti, 2018

04 | Sfide e domande aperte

Le suddette tendenze pongono **sfide** senza precedenti **alla gestione dei servizi di sicurezza**. Ciò è particolarmente manifesto nel più ampio contesto della trasformazione digitale della società italiana e delle aree urbane. Tali sfide sono legate a diversi aspetti, ma sono anche intrecciate e collegate tra loro. Lo scopo di questo capitolo è quello di presentare una breve descrizione di queste sfide, con le loro principali implicazioni.

Prima di tutto, emerge una **dicotomia tra sicurezza e privacy**.

- Da un lato, la crescente pervasività della misurazione e della raccolta dei dati consente **soluzioni più efficaci e servizi più completi**, insieme a risposte mirate e tempestive da parte delle autorità e delle forze dell'ordine.
- Dall'altro lato, la raccolta di tali dati e informazioni personali mette a **rischio la privacy dei cittadini**, soprattutto perché servizi di Smart Safety efficaci richiedono la condivisione di tali informazioni all'interno di piattaforme multistakeholder.[16] Emergono anche aspetti etici, che richiedono quindi una riflessione di ampio livello, non solo su un piano meramente tecnico.

L'importanza di questo problema è evidenziata anche dai risultati della survey. Il 76% degli intervistati al nostro sondaggio dichiara che i loro sforzi e i loro investimenti saranno principalmente dedicati a trovare il miglior **equilibrio tra privacy e sicurezza**.

La raccolta e l'utilizzo dei dati amplifica una domanda che è presente in ogni settore economico: il processo di creazione di valore genera solitamente un problema di attribuzione della **proprietà** di tale valore. Nella data economy il valore è costituito da informazioni personali, generando quindi un interrogativo su come questo valore dovrebbe essere ridistribuito.

Quando si parla di sicurezza, la ridistribuzione di tale valore dovrebbe implicare un **accordo tra i cittadini e i raccoglitori di dati**: il gestore raccoglie i dati e, in cambio, fornisce servizi di sicurezza che generano un valore aggiunto per gli individui. Poiché è impossibile quantificare tale valore in termini monetari, vi è un equilibrio instabile tra la quantità minima di dati necessari per garantire un ambiente sicuro e l'eccessiva estrazione di informazioni tale da invadere la privacy.

La **necessità di trovare un equilibrio ottimale tra sicurezza e privacy** è un tema urgente e prioritario:

- C'è una crescente preoccupazione per il trattamento delle informazioni personali e la consapevolezza sociale sull'importanza dei dati sta crescendo. Inoltre, l'opinione pubblica potrebbe essere influenzata dalla pervasiva raccolta di dati a fini esclusivamente commerciali effettuata da società web e altri soggetti privati. Di conseguenza, l'**importanza dell'uso dei dati privati** sta emergendo come argomento chiave, anche se il processo è ancora nella sua fase iniziale.
- I cittadini diventano **consapevoli del valore delle loro informazioni e dei loro dati personali**. Il 70% della popolazione italiana ritiene che i fornitori di computer, smartphone o tablet dovrebbero fornire loro aggiornamenti regolari del software per proteggere le loro informazioni; il 68% ritiene che le impostazioni predefinite del browser dovrebbero impedire la condivisione delle informazioni; solo il 5% afferma che è accettabile che le aziende condividano le proprie informazioni personali senza il loro permesso, se questo li aiuta a fornire loro nuovi servizi (il 27% afferma che è accettabile in una certa misura).[17]
- Su questo tema, la **regolamentazione** sta muovendo i primi passi verso un sistema più protettivo nei confronti dei cittadini. Il 25 maggio 2018 è entrata in vigore la regolamentazione GDPR. La GDPR (cfr. riquadro 1) ridefinisce il quadro normativo in cui operano i soggetti che rilevano e analizzano dati, stabilendo un regime molto preciso trasparenza modalità di gestione dei dati secondo un approccio "data as value" basato su sistemi di prevenzione in capo al singolo utilizzatore di dati e sanzioni fino a €20.000 o al 4% del fatturato totale dell'impresa inadempiente.
- In generale, la tendenza che si sta affermando sembra essere la seguente: ci saranno sempre più dati disponibili per motivi di sicurezza, e ci saranno sempre più esigenze di accountability, trasparenza e privacy.

I REQUISITI GDPR PER L'UTILIZZO DI DATI PERSONALI

Il principale sviluppo normativo è rappresentato dalla General Data Protection Regulation (GDPR), stilata dalla Commissione Europea ed entrata in vigore il 25/05/2018.

La GDPR afferma che "La protezione delle persone fisiche in relazione al trattamento dei dati personali è un diritto fondamentale" (articolo 1). Il regolamento sposta l'attenzione della legislazione dalla protezione dei dati alla responsabilità dei gestori del trattamento. In particolare, la GDPR stabilisce i seguenti punti:

- *Il diritto dei cittadini di accedere più facilmente alle informazioni sui loro dati e sulle finalità e modalità del loro trattamento: una persona può chiedere a ciascuna organizzazione privata quale dei suoi dati è in loro possesso e come essi vengono utilizzati; una richiesta di accesso ai dati personali (SAR) deve essere soddisfatta entro un mese.*
- *L'istituzionalizzazione del diritto all'oblio (indicato nel regolamento come diritto alla cancellazione), come previsto dalla Corte di giustizia europea, che consentirà di chiedere e ottenere la cancellazione dei dati quando non è più presente un interesse pubblico per la conservazione dell'informazione.*
- *L'obbligo per le imprese di notificare gravi violazioni dei dati dei cittadini.*
- *Sanzioni amministrative fino al 4% del fatturato totale delle imprese in caso di violazione delle norme.*

I soggetti interessati hanno il diritto di opporsi in tutto o in parte al trattamento dei propri dati, di ottenere la cancellazione, l'aggiornamento, la rettifica, l'accesso, la conversione in forma anonima e il blocco o la limitazione del trattamento.

Il regolamento europeo prevede diversi obblighi proattivi per coloro che raccolgono, conservano e utilizzano i dati, al fine di dimostrare l'adozione concreta e non solo formale del regolamento stesso. In questo contesto, la preparazione e l'aggiornamento di un'adeguata documentazione è essenziale, in quanto necessaria ad indicare la corretta applicazione delle norme. La documentazione necessaria riguarda:

- *Documentazione comprovante le operazioni di trattamento effettuate (registro delle operazioni di trattamento; valutazione d'impatto, trasferimento di dati al di fuori dell'UE);*
- *Documentazione attestante il rispetto dei diritti degli interessati (informazioni, moduli di consenso);*
- *Documentazione sulla ripartizione dei ruoli e delle responsabilità (contratti e nomine di manager esterni e nomine; procedure interne, ecc....);*
- *Documentazione attestante le misure di sicurezza attuate.*

16 Tale tecnologia sarà discussa nel capitolo 5, "Tecnologie".

17 Fonte: elaborazione The European House - Ambrosetti su dati Eurobarometro, 2019.

I gestori urbani e gli stakeholder, insieme ai regolatori nazionali e sovranazionali, devono quindi creare un **sistema equilibrato**, massimizzando la sicurezza complessiva del sistema e salvaguardando il livello minimo richiesto di privacy per i cittadini. L'utilizzo dei dati, i limiti a cui devono essere sottoposti i soggetti fruitori dei dati, così come le modalità di raccolta, stoccaggio, conservazione e utilizzo dei dati rimangono una questione chiave che deve essere risolta attraverso la cooperazione e la codecisione di tutti gli attori del sistema.

Fondamentale è anche la definizione di **quale soggetto dovrebbe controllare i dati**: la pubblica amministrazione potrebbe essere al tempo stesso utilizzatore e garante della privacy? La questione diventa ancora più complessa se i dati vengono raccolti da soggetti privati, per utilizzarli sia per la fornitura di servizi di sicurezza che per scopi commerciali. Le tecnologie e la regolamentazione dovrebbero quindi fornire soluzioni in grado di bilanciare il compromesso tra l'interesse legittimo dei privati che raccolgono i dati e il diritto alla privacy dei cittadini.

Infine, è importante sottolineare il concetto di accountability all'interno di questa equazione. Il flusso di dati non deve essere monodirezionale - dal basso verso l'alto, da persona a raccoglitore di dati - ma bidirezionale. Le informazioni raccolte devono essere ridistribuite in modo chiaro e trasparente verso la popolazione, creando un ambiente cooperativo dove gli individui possano comprendere i miglioramenti generati dai loro dati e riconoscere il valore che stanno ricevendo per ciò che, in cambio, forniscono.

Una seconda sfida legata alla protezione della privacy - così come alla regolamentazione dell'uso dei dati - deriva dallo **sviluppo asimmetrico dell'innovazione e della regolamentazione**:

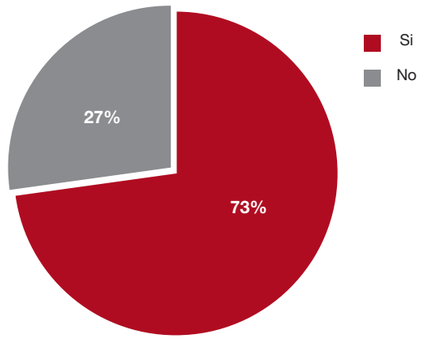
- **La trasformazione digitale avviene rapidamente** e apporta cambiamenti rapidi e dirompenti ai settori e ai servizi tradizionali (compresa la sicurezza).
- Gli adeguamenti del **quadro normativo sono molto più lenti** rispetto alle innovazioni digitali. Inoltre, la regolamentazione dello spazio digitale richiede un insieme innovativo di strumenti e politiche, completamente nuovo rispetto a quelli utilizzati per regolare gli spazi fisici.

Inoltre, lo sviluppo normativo non sempre contribuisce a creare un ambiente favorevole all'innovazione, né fornisce il miglior equilibrio tra la protezione dei cittadini e la fornitura di servizi, in quanto può imporre **vincoli burocratici eccessivi**.

Una regolamentazione come la **GDPR** rischia di porre sfide di per sé, non solo agli operatori industriali e tecnologici, ma anche alle amministrazioni pubbliche locali, ai fornitori di servizi e ad altri soggetti coinvolti nella sicurezza urbana, compromettendo l'efficacia complessiva del paradigma della Smart Safety.

- Il 75% delle multinazionali europee (con più di 75.000 dipendenti) ha previsto un investimento di almeno €5 milioni per adattarsi alla GDPR, prevedendo l'assunzione di almeno 2 o 3 dipendenti a tempo pieno dedicati alle questioni di privacy.
- In Italia, al fine di ottemperare i requisiti imposti dalla GDPR è previsto un investimento complessivo di €2 miliardi per le imprese italiane. [18]
- La survey conferma le difficoltà degli attori urbani ad essere pienamente conformi alla normativa GDPR. [19] La principale preoccupazione espressa dai partecipanti alla survey riguarda l'uso dei dati: la maggioranza teme che la GDPR possa imporre limitazioni al loro sfruttamento. Un'altra preoccupazione riguarda l'integrazione dei dati raccolti da fonti eterogenee, in quanto potrebbe portare ulteriore complessità in termini di proprietà e responsabilità dei dati.

Figura 7. Risposte alla domanda: "Percepite come requisito strategico una soluzione innovativa che consenta di gestire i dati in modo conforme alla GDPR", 2019. Fonte: elaborazione The European House - Ambrosetti su risultati della survey, 2019

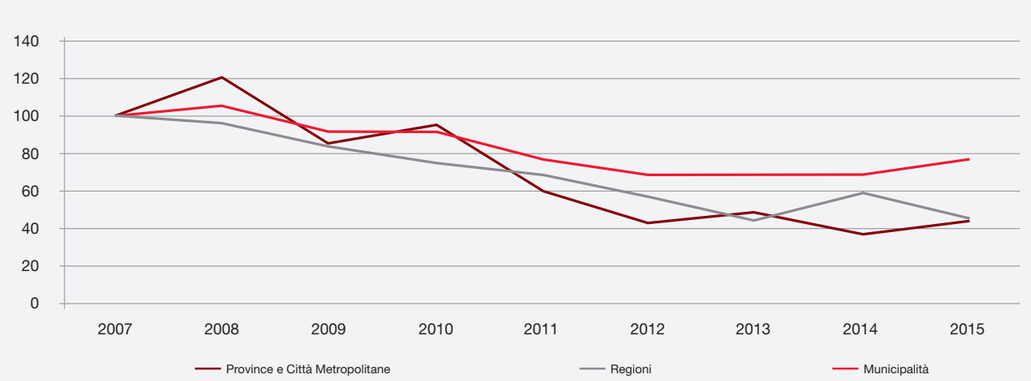


Per risolvere questa frattura tra regolamentazione e innovazione, la cooperazione, la cocreazione e il **dialogo tra le parti interessate sono fondamentali**. Il coinvolgimento dei fornitori di tecnologia potrebbe contribuire alla discussione e alla definizione del nuovo quadro normativo, offrendo un punto di vista informato circa la fattibilità dei requisiti legali e le modalità ottimali per raggiungere gli obiettivi prefissati. Inoltre, il coinvolgimento degli attori tecnologici potrebbe consolidare la forza delle prescrizioni normative, approfittando di un punto di vista "pratico" fin dall'inizio del processo. [20]

La trasformazione digitale richiede anche investimenti per nuove infrastrutture e nuovi software e per la formazione del personale così da creare le competenze necessarie per sfruttare le soluzioni di sicurezza digitale. Tuttavia, il contesto in cui questi trend si evolvono è soprattutto caratterizzato da una **generale mancanza di risorse pubbliche**:

- Sia a livello nazionale che locale, l'amministrazione pubblica si trova a fronteggiare problemi di equilibrio tra le esigenze della popolazione e i costi per soddisfarle.
- La spesa della pubblica amministrazione italiana per investimenti si è ridotta di circa 10 punti percentuali dal 2001 (€37.605 milioni) al 2017 (€33.937 milioni).
- Una quota consistente della spesa della pubblica amministrazione è destinata alla spesa sociale (pensioni e assistenza sociale) e alla spesa corrente improduttiva: questa parte non è elastica - e si prevede che cresca, a causa del cambiamento demografico sopra descritto. [21]
- Anche i Comuni e gli enti locali italiani sono soggetti a vincoli di bilancio che hanno provocato un calo degli investimenti, come mostra il grafico seguente.

Figura 8. Spese di costruzione, acquisto e manutenzione per entità (anno di riferimento 2007 = 100), 2007 - 2015 (ultimi dati disponibili). Fonte: elaborazione The European House - Ambrosetti su dati Istat, 2019



Appare evidente come l'amministrazione pubblica non possa sostenere l'intero costo della trasformazione digitale, a meno di non ridurre altri tipi di spesa, cosa che potrebbe non essere fattibile per difficoltà politiche e tecniche. I vincoli di bilancio impattano oggi in particolare i tre requisiti necessari per sviluppare appieno un ambiente di Smart Safety: **installazione e manutenzione dell'hardware; software di analisi dei dati; formazione del personale e inserimento di nuove figure professionali**. [22]

18 Fonte: elaborazione The European House - Ambrosetti su dati Confesercenti, 2019.

19 Come già accennato, la GDPR pone una serie di compiti per coloro che raccolgono e gestiscono i dati e può creare difficoltà quando organizzazioni diverse devono condividere i dati per scopi comuni (come sistema integrato di sicurezza intelligente).

20 A volte c'è un divario tra le prescrizioni normative e la loro fattibilità tecnologica. Ad esempio, il cosiddetto "diritto alla cancellazione" (noto anche come "diritto all'oblio"), che è un diritto umano fondamentale, pone problemi di attuazione non banali in un'epoca dominata dai social media e dalla diffusione dell'informazione online.

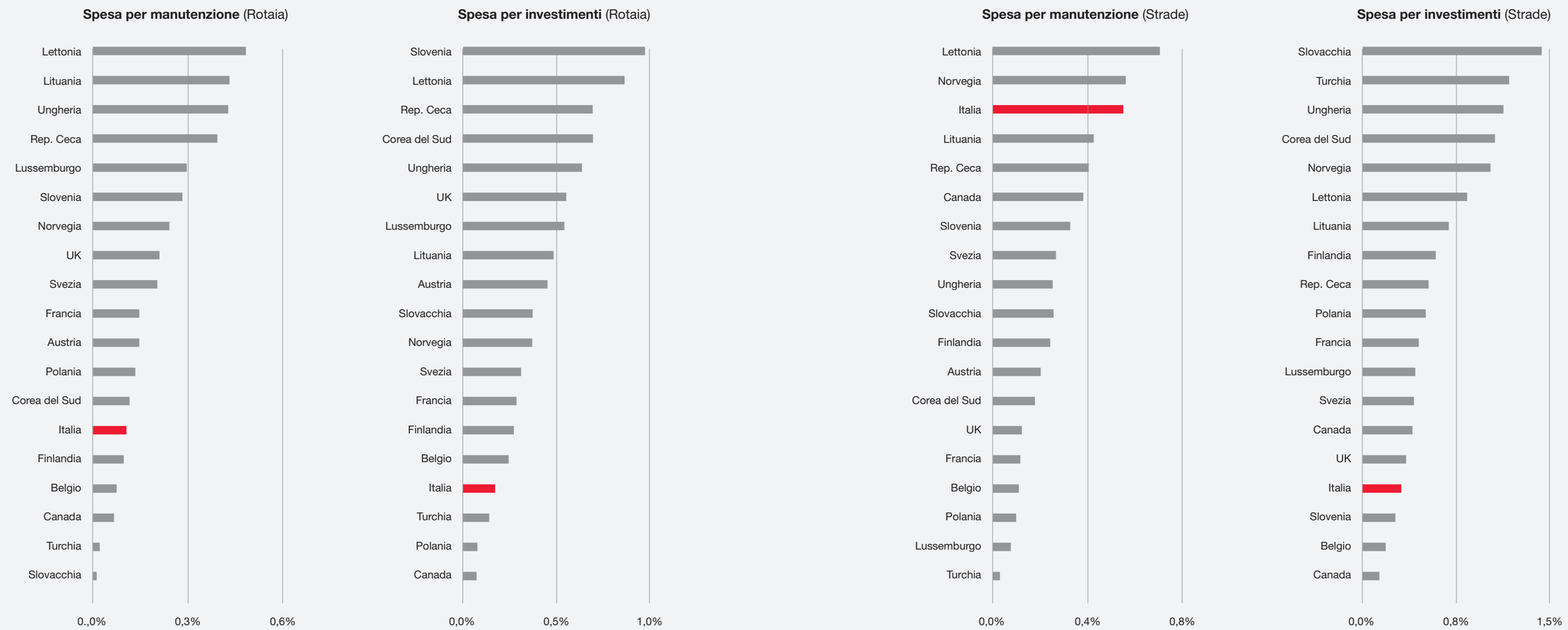
21 Per la spesa sociale sono stati investiti €203.108 milioni nel 2001 (36,4% delle spese correnti totali) e €342.072 milioni nel 2017 (44,2% delle spese correnti totali). Fonte: elaborazione The European House - Ambrosetti su dati Istat e Ministro dell'Economia e delle Finanze, 2019.

22 Questi argomenti saranno discussi in modo più approfondito nella seguente sezione del presente documento.

Tale vincolo di bilancio incide su ogni aspetto della sicurezza. Un tema importante, che ben sottolinea questa criticità, riguarda le **infrastrutture di mobilità**, che non sempre soddisfano le esigenze dei cittadini in termini di possibilità d'uso e sicurezza. La spesa pubblica stanziata in questo settore è dedicata principalmente alla manutenzione piuttosto che all'innovazione intelligente e agli investimenti. La sicurezza di tali infrastrutture è una questione impellente, poiché il rimodellamento delle città sta aumentando la domanda di mobilità. Anche in conseguenza di ciò tali infrastrutture sono quindi uno dei settori in cui oggi la questione della sicurezza è più sentita.

La figura 9 illustra le spese per la manutenzione e gli investimenti per ferrovie (sopra) e per strade (sotto), in termini di percentuale sul PIL. Per una migliore comprensione, i dati italiani vengono confrontati con un gruppo selezionato di paesi OCSE. Come mostrano i grafici, la **spesa italiana per gli investimenti è inferiore alla media sia per quanto riguarda le strade che per le ferrovie**. Il costo della manutenzione stradale, d'altro canto, occupa una parte sostanziale delle risorse pubbliche. La figura 9 illustra la difficoltà sintomatica del processo di innovazione e a cui viene preferita la manutenzione costante rispetto all'innovazione strutturale.

Figura 9. Spesa per la manutenzione e gli investimenti per ferrovie (figura in alto) e strade (figura in basso) nelle economie sviluppate (percentuale del PIL nazionale), 2015. Fonte: elaborazione The European House - Ambrosetti su dati OCSE, 2019



Inoltre, al settore pubblico italiano non mancano solo risorse finanziarie, ma anche capacità e competenze. I Comuni e la Pubblica Amministrazione italiana, a tutti i livelli, non dispongono di competenze adeguate nelle attività connesse a dati (gestione, protezione, analisi), ICT e digitalizzazione. Soprattutto lo **squilibrio cronico tra domanda e offerta di adeguate capacità e competenze nel settore dell'informatica e del management** è una questione di primaria importanza nel settore pubblico, così come per l'economia italiana nel suo complesso:

- In questo momento, le imprese italiane in media dichiarano di avere difficoltà a coprire il 30% dei posti vacanti in quanto non vi è un numero sufficiente di potenziali lavoratori con un adeguato set di competenze digitali.
- In generale, le competenze informatiche sono carenti: in Italia, i laureati ICT sono solo l'1,1% sul totale (quota più bassa tra i paesi OCSE), mentre solo il 13,5% è laureato in discipline STEM (Scienze, Tecnologia, Ingegneria e Matematica), rispetto alla media dei paesi OCSE, 19,1%.[23]
- L'età media dei dipendenti pubblici è di 50,34 anni[24], con una prevalenza di profili giuridici e amministrativi.
- Questo in un contesto UE in cui il 43% dei lavoratori ha subito cambiamenti significativi nelle tecnologie utilizzate per svolgere il proprio lavoro negli ultimi cinque anni e il 47% ha vissuto cambiamenti nel modo in cui organizza o svolge le proprie mansioni.
- Nonostante questa drastica trasformazione delle competenze necessarie, la spesa per l'istruzione è in costante diminuzione. Un dato ancora più preoccupante riguarda l'istruzione post-laurea, la cosiddetta formazione permanente: un'indagine condotta dall'OCSE nel 2016 mostra come solo il 25% dei lavoratori italiani ha frequentato un corso di formazione o aggiornamento nell'ultimo anno.

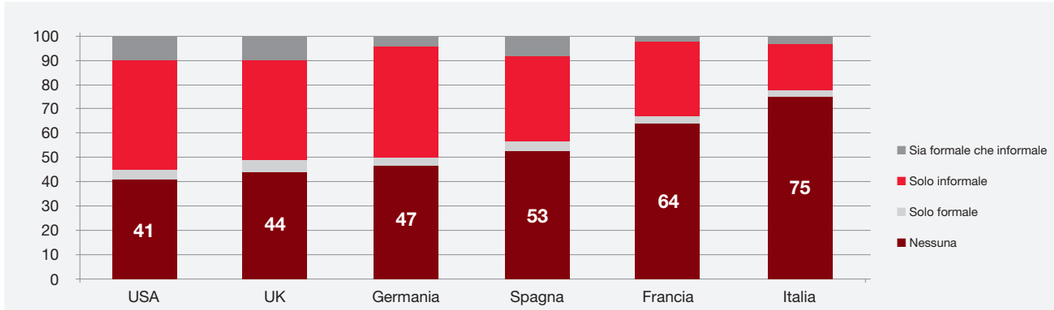
Tali criticità (vincoli di bilancio e scarsità di capitale umano) sottolineano l'importanza di **un approccio integrato e cooperativo** di tutti gli attori coinvolti nello sviluppo urbano, in particolare tra settore pubblico e privato.

Tra gli altri benefici, infatti, l'integrazione tra il settore pubblico e quello privato può anche contribuire a ridurre i costi e a **condividere gli oneri di bilancio**, offrendo soluzioni a valore aggiunto derivanti dall'integrazione e schemi innovativi di finanziamento, utili per gli attori coinvolti in un modello cooperativo vantaggioso per tutti.

Dall'altro lato, la presenza di una molteplicità di attori e la crescente necessità di cooperazione tra questi costituisce di per sé una sfida. La diffusione delle responsabilità e la creazione di una struttura di gestione multicentrica potrebbe potenzialmente creare un **problema di sovrapposizione e segmentazione delle informazioni**, che si aggiunge alle preoccupazioni relative alla privacy e alla gestione dei dati.

Per questo motivo, la cooperazione e l'integrazione tra tutti gli attori coinvolti nella pianificazione e gestione urbana devono iniziare **fin dalla fase iniziale** dello sviluppo di concetti, strategie e infrastrutture (hardware e software) di "Smart Safety". Questo è il modo più efficace per garantire adeguati livelli di co-sviluppo, ovvero il pilastro fondamentale e di una rivoluzione digitale efficace.

Figura 10. Formazione permanente (percentuale di lavoratori che hanno partecipato a corsi di formazione nell'ultimo anno), 2015. Fonte: elaborazione The European House - Ambrosetti su dati OCSE, 2019



23 Fonte: elaborazione The European House - Ambrosetti su dati OCSE, 2019.

24 Fonte: elaborazione The European House - Ambrosetti su dati Ragioneria dello Stato, 2019.

05 Tecnologie

Come descritto nel capitolo precedente, i grandi temi e le sfide legate all'implementazione della "Smart Safety" nelle città italiane possono essere superati attraverso la **collaborazione di tutti gli attori coinvolti** nella pianificazione, sviluppo e gestione urbana.

Le tecnologie, in questo senso, possono fungere da importante strumento di cooperazione, consentendo pratiche di co-creazione pervasive ed efficaci che portino a sviluppare architetture comuni. Le soluzioni tecnologiche possono anche supportare la transizione verso "servizi intelligenti" che pongono il cittadino al centro dell'attenzione, fornendo gli **elementi costitutivi dei servizi di "Smart Safety"** in grado di soddisfare nuove esigenze e nuove richieste della popolazione.

Tuttavia, per farlo, le singole tecnologie, gli strumenti digitali o le innovazioni ICT non sono sufficienti. Il rischio è quello di impiegare le limitate risorse per sviluppare e distribuire elementi scarsamente utili o servizi limitati verticalmente e con un impatto inadeguato. Il paradigma di Smart Safety non richiede un semplice aggiornamento della strumentazione o l'utilizzo di tecnologie più sofisticate: questo è un elemento necessario, ma non sufficiente.

Una Connected City non si affida solo a "gadget tecnologici" all'avanguardia, ma anche all'**integrazione orizzontale**, alla **profondità verticale** e ai **nuovi modelli organizzativi e operativi** resi possibili dalla rivoluzione digitale. Solo attraverso tale approccio è possibile sfruttare il valore derivante dall'interconnessione di più fonti di dati.

Come evidenziato dai risultati dell'indagine, il vero valore dei dati risiede nella possibilità di utilizzarli per scopi diversi, al fine di moltiplicare in modo esponenziale le possibilità di analisi e le opportunità di servizi.

Di conseguenza, il primo elemento tecnologico necessario per creare una vera e propria "Connected City" dovrebbe essere la cosiddetta "**Piattaforma Integrata**". Essa costituisce il quadro di riferimento per i diversi attori coinvolti (individui, P.A., attori privati quali fornitori di tecnologia o servizi di pubblica utilità) che forniscono, raccolgono, distribuiscono e utilizzano i dati da (e verso i) cittadini e la città.

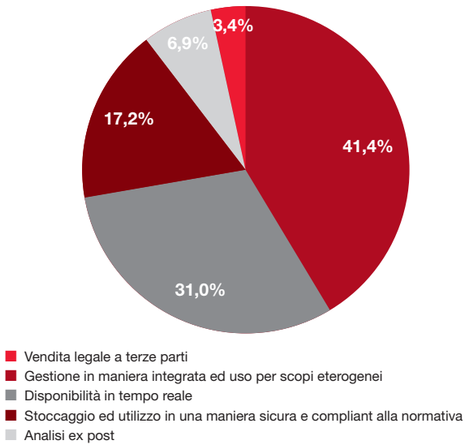
Questa piattaforma è essenziale in quanto risponde ad un'esigenza cruciale. Fornisce standard condivisi e riconosciuti, regole e perimetro tecnologico, consentendo **flussi di dati tra i diversi attori coinvolti**. Questa funzione richiede l'integrazione tecnologica di diversi software, tale da consentire il dialogo tra tutti gli attori che partecipano ai servizi di Smart Safety.

Inoltre, tale piattaforma dovrebbe essere concepita al fine di raccogliere dati grezzi (input) e di distribuire ai singoli utenti (in particolare ai fornitori di servizi verticali come le utility e le forze dell'ordine) **KPI utili, analisi e informazioni** (output).

Ad esempio, i dati raccolti da una telecamera stradale (es. l'intensità del traffico) potrebbero essere utili non solo per i soggetti coinvolti nella mobilità urbana, ma anche per la gestione dell'illuminazione, per la polizia municipale, le aziende di trasporto pubblico, i vigili del fuoco, le ambulanze e così via. Ogni soggetto, tuttavia, è interessato ad una diversa sfumatura di tale dato: mentre le ambulanze sono interessate ad analisi in tempo reale (ad esempio sono interessate a sapere quale sia l'itinerario che riduce al minimo i tempi di percorrenza di un tragitto), le aziende di trasporto pubblico possono essere interessate alla previsione della congestione del traffico durante il giorno al fine di progettare corse e tratte in modo più efficiente.

- Il monitoraggio di treni, metropolitane e stazioni attraverso un insieme integrato di sensori e analisi permette di prevedere, evitare e gestire i problemi di sicurezza più comuni in tali spazi pubblici critici (es. smarrimento di oggetti e persone, incidenti dovuti al sovraffollamento, minacce di pubblica sicurezza, ...). Al tempo stesso, i medesimi dati sui flussi di persone possono essere utilizzati per rendere più efficiente il servizio, ad esempio aumentando la frequenza dei viaggi nelle ore di punta ed evitando quindi il sovraffollamento. Infine, l'introduzione di tecnologie di guida autonome e di servizi di mobilità integrata nella mobilità pubblica e privata, a loro volta basate sui dati, influisce positivamente sulla sicurezza (oltre che sulla mobilità in sé), soprattutto per gli utenti più fragili.

Figura 11. Risposta alla domanda: "Qual è, a suo giudizio, il principale valore dei dati urbani?" (percentuale degli intervistati). Fonte: elaborazione The European House - Ambrosetti su risultati della survey, 2019



Appare chiaro come i dati possano essere utilizzati in modo prezioso per una pluralità di scopi, anche molto diversi da quello iniziale per il quale sono stati raccolti. Inoltre, tali dati possono essere analizzati in vari modi per diversi obiettivi, generando valore aggiunto per un intero sistema grazie all'innovazione. I risultati dell'indagine sottolineano la possibilità di integrazione dei dati e lo sviluppo di servizi a valore aggiunto come risultato chiave della raccolta di informazioni.

Una piattaforma centralizzata e integrata (di seguito "Control Room") sviluppata come sopra indicato è fondamentale per consentire la raccolta e l'utilizzo sistemico di dati diversi, fornendo il quadro orizzontale e garantendo un corretto flusso di KPI e informazioni a (e tra) tutti i soggetti coinvolti. È quindi la **tecnologia necessaria, che consente di implementare una vera e propria Connected City**.

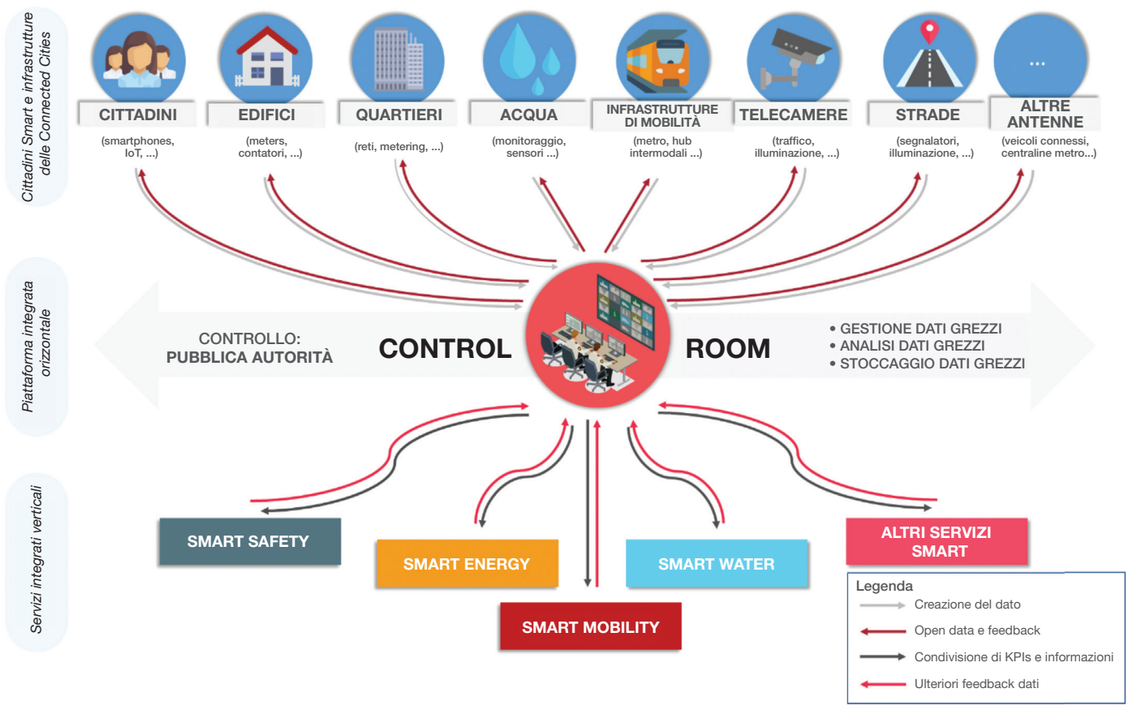
Una Control Room è anche una piattaforma indispensabile per **superare le questioni relative alla privacy**, soprattutto in considerazione dei **vincoli normativi** derivanti dalla normativa GDPR che stabilisce un insieme rigoroso di regole e doveri per la raccolta dei dati in capo a ciascun stakeholder. Tale Control Room consente di bilanciare le esigenze di sicurezza e privacy, in quanto fornisce una piattaforma centralizzata, gestita dalla Pubblica Amministrazione a livello cittadino, garante del rispetto di tale insieme di regole.

È importante sottolineare che una Control Room non implica una centralizzazione dell'uso dei dati cittadini, ma solamente della loro conservazione, protezione e analisi. La raccolta dati può essere assegnata a questa piattaforma o a singoli fornitori di servizi (utilities), player tecnologici o antenne all'interno della città. Il punto più importante, tuttavia, è che **grazie a tale Control Room i dati provenienti da più fonti possono essere condivisi in modo da rispettare la privacy**: possono essere immagazzinati ed elaborati dal pubblico, mentre solo i KPI, le analisi aggregate e le informazioni strategiche possono essere condivise con altri attori privati verticali, salvaguardando i dati personali sensibili.

Una volta sviluppata in modo collaborativo, la Control Room diventa il fulcro tecnologico centrale per gli Smart Services e la Smart Safety, assumendo l'onere della conformità normativa e favorendo **comportamenti collaborativi** verso la trasparenza e la standardizzazione, elemento fondamentale per il funzionamento del sistema urbano su di essa basato. Fornisce anche uno spazio virtuale dove i dati possono essere aggregati, analizzati e poi condivisi, aggiungendo valore all'ambiente urbano nel suo complesso.

Tale Control Room urbana diventerà anche il garante della sicurezza stessa del sistema: deve assicurare il controllo e la sicurezza dello spazio virtuale, prevenire furti di dati ed evitare violazioni della privacy. Inoltre, deve garantire la **sicurezza dei dati e la sicurezza informatica** (individualmente, privatamente e pubblicamente). Per fare ciò, una progettazione e implementazione tecnologica all'avanguardia deve garantire la sicurezza informatica nel tempo, anche considerando la continua evoluzione delle minacce digitali e la rilevanza di ogni singolo nodo che la piattaforma integra, compresi i cittadini, gli operatori umani e i modelli organizzativi.

Figura 12. Funzionamento della sala di controllo integrato (illustrativo). Fonte: elaborazione The European House - Ambrosetti su interviste e risultati dell'indagine, 2019



Grazie all'integrazione, a standard comuni e pratiche riconosciute, una Control Room cittadina potrebbe anche migliorare le opportunità offerte dall'**accumulo di dati e** dall'**integrazione di più fonti**, consentendo economie di scala, processi di razionalizzazione e di riduzione dei costi, senza compromettere la qualità dei servizi offerti e offrendo la possibilità di elaborare soluzioni personalizzate.

- Tali piattaforme sono già disponibili, fornendo servizi integrati in grado di soddisfare efficacemente molteplici esigenze. Ad esempio, le **forze dell'ordine** possono già beneficiare di piattaforme verticali che le supportano durante l'intero corso delle indagini. Tale piattaforma permette di raccogliere tutte le prove rilevanti; di analizzarle automatizzando processi a basso valore aggiunto quali trascrizioni audio e analisi video; di utilizzare una piattaforma sicura e sviluppabile nel tempo per consentire la condivisione conforme di documenti e prove con il personale della giustizia e dei pubblici ministeri; di costruire un

database completamente scalabile che consente la valutazione ex post e l'estrazione dei dati. Tale piattaforma è inoltre progettata per garantire sia un sistema adattivo, integrato e facile da usare, sia per proteggere i dati stessi nel tempo.

L'importanza di una Control Room integrata con le suddette caratteristiche **non è ancora pienamente riconosciuta** dalle autorità pubbliche che hanno partecipato all'indagine: nonostante la maggioranza relativa (47% degli intervistati) la considera una priorità di investimento nei prossimi anni. Una percentuale non indifferente degli intervistati non è invece consapevole dei potenziali benefici o non la considera una priorità nel prossimo futuro (31%).

Inoltre, per evitare problemi di obsolescenza infrastrutturale (hardware e software), tale piattaforma dovrebbe essere progettata in modo cooperativo sin dall'inizio, in modo da essere **adattabile e scalabile**, al fine di costruire uno strumento in grado di fornire soluzioni a quei problemi che potrebbero emergere in un momento successivo, e dovrebbe essere capace di ospitare strumenti e architetture future. Il ritmo veloce della trasformazione urbana, come discusso nelle sezioni precedenti, continua a generare nuove esigenze di sicurezza e crea nuove sfide oggi forse nemmeno ipotizzabili. Queste sfide possono essere affrontate solo con tecnologie che possono essere migliorate con la stessa rapidità con cui gli spazi sociali si trasformano.

A cambiare rapidamente e imprevedibilmente non sono solo le esigenze di sicurezza, ma anche i requisiti normativi. È il caso della GDPR, che richiede una **"politica di divulgazione" non solo durante la raccolta dei dati**, ma anche durante il processo di elaborazione, fornendo chiare indicazioni sulla finalità d'uso dei dati raccolti. A questo si aggiunge il ruolo delle associazioni di cittadini e del Garante della privacy, e la crescente consapevolezza dei singoli individui sui loro diritti digitali.

In questa direzione, nel quadro di co-sviluppo attivato dalla "Control Room", è possibile elaborare utili "**Ethical Checklist**" [25], controllando e minimizzando le ripercussioni etiche della raccolta dati, attraverso il monitoraggio di aspetti quali:

- **Trasparenza**, cioè la capacità dell'individuo di sapere e controllare quali dei suoi dati sono memorizzati e come vengono utilizzati;
- **Responsabilità**, la capacità di un fornitore di dati di verificare che essi siano utilizzati correttamente secondo regole prestabilite al fine di garantire la comprensibilità e l'interpretabilità dei risultati;
- **Equità**, vale a dire la non discriminazione o la non polarizzazione (distorsione) dei risultati (ad esempio con una prioritizzazione eticamente scorretta);
- **Affidabilità**, la garanzia della qualità delle fonti, in termini di origine dei dati e della loro autenticità (ad esempio utilizzando metadati);
- **Qualità dei dati**, ovvero precisione, accuratezza, completezza, correttezza, e tempestività dell'aggiornamento.

Inoltre, le tecnologie in grado di fornire una forma di anonimizzazione dei dati possono essere integrate e aggiornate nel tempo, al fine di estrarre tutte le informazioni necessarie massimizzando al contempo la privacy dei cittadini. A tal fine, le tecnologie intelligenti sono essenziali, poiché possono essere utilizzate per raccogliere **tutti e solo i dati necessari** per l'ambito di analisi.

- A titolo di esempio, una telecamera che ha lo scopo di controllare i flussi di persone e monitorare i pericoli di sovraffollamento (in luoghi come stazioni metropolitane o ferroviarie, luoghi di eventi, ...) potrebbe utilizzare processi di **anonimizzazione** (la cosiddetta avatarizzazione, cioè la trasformazione di persone registrate in avatar, in modo che sia possibile monitorare i movimenti, ma non sia possibile riconoscere volti o identità).

Un altro vantaggio derivante dalla combinazione di tali piattaforme integrate, dagli strumenti di condivisione dei dati, dalle tecnologie intelligenti e dalle soluzioni analitiche, è quello di consentire ai Comuni e ad altri attori di **condividere i dati in tempo reale**.

- È possibile creare una piattaforma per visualizzare in **tempo reale** informazioni e statistiche su questioni ambientali, fenomeni di sovraffollamento, statistiche sulla microcriminalità e altre informazioni rilevanti per i cittadini.

Tali informazioni possono essere messe a disposizione dei cittadini (anche in tempo reale, tramite app). In questo modo, processi basati su Control Room cittadine possono portare alla formazione di **iniziative dal basso**, promosse dai cittadini informati, e contribuiranno a mettere in evidenza i benefici per la comunità derivanti dalla raccolta e dall'uso strategico dei loro dati.

Inoltre, la diffusione di informazioni mirate potrebbe prevenire o disinnescare la formazione di opinioni distorte, contribuendo a **ridurre il divario tra la sicurezza reale e quella percepita**. La costante interconnessione consentita dalle Control Room integrate crea la possibilità di condividere i dati con i cittadini attraverso piattaforme aperte, coinvolgendoli e promuovendo spazi sociali più salubri.

Inoltre, la quantità di dati disponibili richiede tecnologie adeguate ad analizzarli, estraendo le **informazioni rilevanti in tempo reale**.

- Le soluzioni di **Intelligenza Artificiale (I.A.)** possono identificare autonomamente e in tempo reale problemi e minacce, portandoli all'attenzione dell'operatore umano, il cui compito non sarà più quello di monitorare, ma di operare scelte strategiche ed eseguire task a più alto valore aggiunto.
- In caso contrario, a causa della mole di dati oggi disponibili (e in crescita), la risposta degli esseri umani senza il supporto dell'I.A. sarebbe troppo lenta e non focalizzata, o finanche impossibile. L'assenza di un sistema automatico e rapido di analisi dei dati - in grado di **estrarre le informazioni rilevanti** e di eliminare il cosiddetto "white noise" [26] – comprometterebbero le opportunità offerte da Smart Safety.
- L'esempio più eclatante a questo proposito è fornito dalla videosorveglianza: l'assenza di una **piattaforma di analisi video** consentirebbe solo una sorveglianza in tempo reale e una valutazione ex post.
- Tali caratteristiche sono già esistenti: la **tecnologia di Video Analysis**, integrata con i database di riconoscimento facciale, permette l'**identificazione in tempo reale di soggetti selezionati** su feed video, e la conseguente possibilità di fornire un allarme immediato.

Le soluzioni di analisi in grado di gestire Big Data, inoltre, possono essere utilizzate per scopi di sicurezza non solo in tempo reale, ma anche per analisi predittiva, una caratteristica preziosa per la sicurezza. Infatti, con un numero adeguato di dati è possibile estrapolare i trend non immediatamente identificabili e trovare modelli di comportamento. Queste informazioni sono essenziali per migliorare l'efficienza dei servizi, sia riducendone i costi e gli sprechi energetici, sia garantendo un servizio migliore, basato sulle esigenze dei cittadini.

Lo strumento di **analisi predittiva della criminalità** permette agli agenti di integrare i dati esistenti (track record di crimini, ecc.) con altre fonti (social media, antenne…) al fine di prevedere, in maniera granulare per singole aree della città, i crimini potenzialmente perpetrabili.

Infine, le tecnologie consentono di **superare la resistenza degli attori privati** a partecipare a tali sforzi integrati. Il costo della perdita del controllo individuale dei dati di ciascun player è infatti bilanciato da:

- Il fatto che, grazie al ruolo di raccordo dei player pubblici all'interno della Control Room, solo KPI e informazioni aggregate e concordate saranno condivise con altri player privati (non dati grezzi o sensibili);
- La disponibilità di ulteriori informazioni e servizi a valore aggiunto, percepiti come estremamente utili (es. offerte geo-based, smart marketing, ...), in grado di aumentare la sicurezza dei propri clienti o di fornire loro **servizi integrati a valore aggiunto** (monitoraggio sanitario, monitoraggio degli anziani, assicurazioni, ...), senza compromettere la privacy dei cittadini.

25 Cfr. L. Tanca, P. Atzeni, D. Azzalini, I. Bartolini, L. Cabibbo, L. Calderoni, P. Ciaccia, V. Crescenzi, J. C. De Martin, S. Fenoglietto, D. Firmani, S. Greco, F. Isgrò, D. Maio, D. Martinenghi, M. Matera, P. Merialdo, C. Molinaro, M. Patella, R. Prevete, E. Quintarelli, A. Santangelo, A. Tagarelli, G. Tamburrini, R. Torlone, Ethics-aware Data Governance (Vision Paper) – SEBD 2018, 49, Castellaneta Marina, 2018.

26 Ovvero l'insieme di informazioni di contorno che impediscono una chiara focalizzazione sugli aspetti rilevanti.

06 Priorità per lo sviluppo e la diffusione delle Connected Cities in Italia

Le tecnologie oggi disponibili consentono di superare le principali criticità e problematiche legate alla fornitura di servizi di Smart Safety all'interno delle città italiane. Insieme alle tecnologie, tuttavia, sono necessari **modelli operativi e organizzativi** innovativi per creare una vera e propria Connected City, ponendo i cittadini e le comunità al centro di servizi utili e integrati.

Come illustrato nei capitoli precedenti, il principale elemento abilitante per lo sviluppo e la realizzazione delle Urban Control Room è l'**integrazione**. Questo obiettivo può essere raggiunto solo attraverso una reale cooperazione di tutti gli attori coinvolti nella pianificazione, nello sviluppo e nella gestione urbana. Tale cooperazione dovrebbe iniziare nelle primissime fasi della creazione di una Connected City.

Per fornire servizi integrati e di valore e per ottenere il massimo da una Control Room cittadina scalabile, la sua architettura dovrebbe infatti essere **co-progettata e co-sviluppata con la collaborazione di molteplici attori** tra cui la Pubblica Amministrazione, i servizi pubblici, altri fornitori di servizi, fornitori di tecnologia e integratori, agenzie di finanziamento e, naturalmente, i cittadini e le comunità. Per raggiungere l'interoperabilità (che è la base di una Control Room integrata), gli standard, gli approcci e i linguaggi condivisi dovrebbero essere definiti e concordati fin dall'inizio.

In questo senso, una priorità è la **formazione di funzionari e manager pubblici** per aggiornare il paniere di competenze oggi disponibile, in quanto le Pubbliche Amministrazioni hanno un ruolo cruciale nella creazione di Connected Cities. Per questo motivo, è necessaria una forte discontinuità anche nelle modalità di sviluppo e gestione dei progetti comunali. È necessaria la cooperazione tra i diversi settori e dipartimenti (anche con altri livelli locali e nazionali). Inoltre, un cambiamento culturale è la chiave di volta verso una maggiore spinta all'innovazione.

All'interno di una Control Room urbana integrata, la Pubblica Amministrazione dovrà gestire le gare d'appalto, guidare i processi di co-design, effettuare la raccolta, la gestione e l'analisi dei dati e quindi condividere le informazioni. Il **personale tecnico deve essere competente, idoneo allo scopo e in grado di realizzare uno sviluppo contrattuale intelligente**. La mancanza di competenze, al contrario, rischia di lasciare l'iniziativa a singole utility o integratori tecnologici, che potrebbero limitarsi a fornire gadget tecnologici superflui (o meno preziosi ed efficaci) rispetto ad un sistema di servizi verticali integrati abilitati da una piattaforma orizzontale. Anche i servizi di statistica all'interno dei Comuni dovrebbero essere potenziati.

La governance di una Connected City è fondamentale e dovrebbe essere definita fin dall'inizio. Dovrebbero essere definiti chiaramente i ruoli politici e tecnici, come ad esempio i responsabili dello sviluppo strategico, della gestione architettonica e delle infrastrutture e della protezione dei dati.

A livello nazionale, dovrebbero essere sviluppati quadri tecnici e allegati per fornire alle amministrazioni locali orientamenti adeguati, linee guida formalizzate e modelli standardizzati. Tali documenti dovrebbero essere conformi alla normativa e agli obiettivi internazionali, includendovi anche le migliori pratiche a livello nazionale e sovranazionale.

La cooperazione dovrebbe applicarsi anche tra le amministrazioni pubbliche e gli stakeholder di città diverse. Mentre è richiesto un adeguato livello di personalizzazione delle architetture e delle soluzioni digitali – dal momento che ogni città ha caratteristiche ed esigenze specifiche - soluzioni comuni, standard di riferimento e un quadro tecnologico condiviso tra le diverse città italiane (o internazionali) potrebbero portare a **minori costi e possibilità di licensing** (custom vs. tailor).

Il ruolo della Pubblica Amministrazione è quindi fondamentale, deve **guidare il dialogo e la co-progettazione**, fornendo orientamenti e chiare richieste ad altri attori (servizi pubblici, fornitori di tecnologia, integratori, comunità, ...), stabilire standard, regolamenti, obiettivi e priorità fin dall'inizio. Tale leadership consente la scalabilità ed evita il lock-in tecnologico di specifiche aziende o attori. Definisce inoltre le modalità di raccolta e condivisione dei dati. Fornisce infine un'intermediazione centrale.

Al tempo stesso, occorre sottolineare come le Connected City non si basano su processi centralizzati, ma su **modelli orizzontali, decentralizzati e integrati**. Per questo motivo, tutti gli stakeholder assumono un ruolo chiave a livello sistemico: il dialogo, la co-progettazione e il co-sviluppo diventano una priorità. La Connected City dovrebbe includere diverse aziende: fornitori di tecnologia che utilizzano l'architettura orizzontale (Urban Control Room), ma anche gestori di servizi verticali e servizi di pubblica utilità.

Una singola azienda non può costruire una Connected City: la cooperazione è la chiave. Gli attori privati dovrebbero accettare di inserire i propri dati nel sistema, rassicurati dal controllo pubblico dell'architettura orizzontale e incentivati dalla possibilità di offrire servizi integrati e di ricevere a loro volta informazioni preziose. Le **comunità e i cittadini** devono partecipare al co-design, anche attraverso nuovi canali di partecipazione. Devono ricevere dati utili, KPI e metriche, che trasformano gli individui in prosumer e pro-utilizzatori di servizi pubblici, coinvolgendoli nel co-sviluppo dei servizi. La trasparenza aumenta anche la responsabilità del sistema nel suo complesso.

Infine, anche gli **istituti di ricerca** (ad esempio l'ENEA) e le **agenzie di finanziamento** devono partecipare attivamente. I programmi di finanziamento possono essere estremamente efficaci nell'incentivare il dialogo e la co-progettazione di una Connected City, svolgendo un ruolo molto più efficace della legislazione. Attraverso schemi di finanziamento dovrebbero incentivare le partnership pubblico-privato, l'Open Innovation, il collegamento in rete con gli istituti di ricerca e le nuove imprese, garantendo cooperazione, integrazione, trasparenza e interoperabilità.

In conclusione, la maggior parte delle tecnologie necessarie per creare una Connected City sono oggi disponibili, e sono in continua evoluzione e miglioramento. Inoltre, è possibile concepire architetture scalabili per collegare nei prossimi anni fonti di dati aggiuntive e nuove soluzioni software e hardware. Ad oggi, la priorità è invece quella di **sviluppare modelli organizzativi e operativi innovativi, basati sulla digitalizzazione e la co-creazione**, attivando tutti gli attori coinvolti nella pianificazione, sviluppo e gestione delle città e dei servizi urbani.

Questo è un prerequisito che dovrebbe **diventare urgentemente una priorità per i decisori italiani**: senza mettere in atto un quadro operativo e adottare una mentalità cooperativa, è impossibile creare una vera e propria "Connected City" che fornisca servizi intelligenti ai propri cittadini. Al contrario, un approccio frammentato e non coordinato rischia di tradursi nell'adozione di singole soluzioni o "gadget tecnologici", che non riescono a beneficiare al massimo delle potenzialità dal progresso digitale o, peggio ancora, a sprecare risorse pubbliche ritardando o influenzando la capacità del sistema urbano di dispiegare una Connected City ben sviluppata.

Appendice

Le soluzioni di Hitachi per la Smart Safety

Nel campo delle tecnologie per la Smart Safety, Hitachi ha già sviluppato e implementato soluzioni innovative in grado di consentire il paradigma di integrazione delineato nel documento. Tali soluzioni aiutano e supportano efficacemente le Pubbliche Amministrazioni, i gestori di spazi sociali e i singoli individui a fornire **servizi di Smart Safety avanzati e completi**. Telecamere e sensori innovativi, analisi in tempo reale e predittive, piattaforme di controllo integrate, aiutano efficacemente gli amministratori locali e le forze dell'ordine a garantire ai cittadini un livello di sicurezza in **linea con i più elevati requisiti e aspettative, all'interno dell'estensione del paradigma** nell'era digitale. **Treni, metropolitane, tram, stazioni** diventano spazi dove il pericolo può essere prevenuto, ma anche dove è possibile identificare oggetti o persone smarrite, gestire l'affollamento e informare i passeggeri in tempo reale, offrendo un servizio di sicurezza più ampio. Diventa inoltre possibile **monitorare le infrastrutture** e agire tempestivamente. Queste soluzioni concrete coniugano i progressi tecnologici e i modelli di co-sviluppo con l'idea centrale dell'innovazione sociale: **trovare soluzioni non per una persona o un'organizzazione, ma per tutta la società**. Tra gli altri, esempi di soluzioni concrete di Smart Safety includono:

ARGOMENTO DI STUDIO:

L'integrazione di sistemi pubblici e privati offre l'ambiente più sicuro possibile a Washington D.C.

Dal 2009 la collaborazione tra Hitachi e il Dipartimento di polizia metropolitana di Washington D.C. ha fornito un sistema integrato di sicurezza intelligente per gestire un'area critica e fornire l'ambiente più sicuro a oltre 700.000 residenti. Hitachi Visualization Suite ha fornito un'unica interfaccia di sicurezza che ha permesso di integrare un'ampia gamma di sistemi, tra cui Computer Aided Dispatch (CAD), Records Management Systems (RMS), License Plate Recognition (LPR), Gunshot Detection, sistemi di gestione video multipli e singole telecamere di enti privati (1500).

https://www.hitachivantara.com/en-us/products/iot-operations-intelligence/video-analytics.html

ARGOMENTO DI STUDIO:

L'Intelligenza Artificiale supporta Las Vegas nella delivery di un livello di servizio in linea con le alte aspettative della popolazione

Sfruttando l'integrazione di una vasta gamma di soluzioni tecnologiche (Hitachi Smart Cameras, Hitachi Edge Gateway, Hitachi Video Analytics (HVA) per le analisi, Hitachi Visualization Suite (HVS) per la visualizzazione e Pentaho per l'integrazione dei dati), Hitachi ha costruito un "Innovation District" nel centro di Las Vegas, offrendo modalità di trasporto multimodale, sicurezza fisica e servizi urbani avanzati, integrati e interconnessi ai cittadini.

http://social-innovation.hitachi/us/think-ahead/smart-spaces/las-vegas-iot/index.html

ARGOMENTO DI STUDIO:

Tecnologie integrate contribuiscono all'utilizzo sicuro degli aeroporti da parte dei passeggeri

L'integrazione dell'Intelligenza Artificiale (I.A.) nei feed video e nei sistemi di videosorveglianza esistenti permette all'Aeroporto Internazionale di Vienna di monitorare in breve tempo ore di riprese, permettendo l'identificazione di bagagli smarriti e il monitoraggio del proprietario, per la ricerca di persone disperse, come i bambini. Il sistema fornisce una completa anonimizzazione dei dati video, poiché acquisisce i tratti fisici di una persona senza catturare il suo volto in dettaglio.

http://social-innovation.hitachi/it/topics/all-in-the-sky/

ARGOMENTO DI STUDIO:

Innovativi sensori di movimento forniscono un ambiente più sicuro sia a casa che in luoghi commerciali

Il sensore di movimento 3D LiDAR (TOF) è in grado di calcolare la dimensione, la forma e la posizione di persone e oggetti e di tracciarne il movimento, riportando le azioni individuali, i trend e le situazioni insolite in spazi commerciali e pubblici che possono rappresentare una potenziale minaccia. Inoltre, i sensori forniscono informazioni utilizzabili preservando al contempo l'anonimato e la privacy. I sensori di movimento 3D LiDAR hanno trovato applicazione sia per garantire la sicurezza negli spazi pubblici che in ambito domestico: i sensori possono prevenire il taccheggio, monitorare la postura e i movimenti di persone vulnerabili e avvisare i familiari in caso di cadute, lesioni o altri incidenti domestici.

http://social-innovation.hitachi/eu/topics/3d-lidar-tof-motion-sensor/

ARGOMENTO DI STUDIO:

Un centro di governance intelligente e in tempo reale è stato realizzato in uno Stato di 53 milioni di cittadini grazie alla co-creazione

Hitachi ha fornito allo Stato indiano di Andhra Pradesh in India una piattaforma che fornisce un'istantanea in tempo reale delle prestazioni dei vari dipartimenti del governo. La piattaforma aggrega i dati di oltre 30 dipartimenti governativi (con oltre 300 agenzie di reporting, che forniscono quasi 750 servizi), consentendo di comunicare tra loro. Grazie alla co-creazione, i dati relativi a trasporti, interventi di emergenza, agricoltura, sicurezza e altri servizi e programmi pubblici sono analizzati in modo integrato, fornendo una visione complessiva e consentendo decisioni informate.

https://insights.hitachiconsulting.com/post/102enqc/under-the-hood-a-peek-into-the-real-time-governance-system

HITACHI
Inspire the Next

@HitachiEurope

linkedin.com/company/HitachiEurope

hitachi.eu

social-innovation.hitachi

youtube.com/HitachiBrandChannel

Hitachi Europe Ltd.
Whitebrook Park, Lower Cookham Road, Maidenhead, Berkshire, SL6 8YA
Tel: +44 (0) 1628 585000 Fax: +44 (0) 1628 585373