Maria Notaristefano, Fabio Angeletti ed Esli Spahiu

*Privacy e cybersecurity nelle Smart City: un caso di studio**

Abstract: Le iniziative di smart city offrono numerosi vantaggi, tra cui lo sviluppo economico e la distribuzione efficiente delle risorse, nonché il miglioramento delle politiche e del benessere sociale. Il fulcro di queste iniziative è la raccolta, l'elaborazione e l'utilizzo dei dati. Tuttavia, la gestione di questi dati in una rete IoT coesa comporta rischi, in particolare per quanto riguarda la sicurezza dei dati e la protezione dei dati personali. Pertanto, un'efficace governance delle smart city deve incorporare solide misure di protezione dei dati per mantenere gli standard di sicurezza e privacy. Tuttavia, le applicazioni pratiche della letteratura accademica a questo proposito sono limitate. La presente ricerca si concentra quindi sull'offrire una panoramica completa delle migliori pratiche normative e tecnologiche che possono migliorare la sicurezza e la privacy dei dati nelle smart cities. Nel far ciò, lo scritto si concentra sulla Roma Data Platform (RDP), un progetto che mira ad accelerare la transizione di Roma verso un modello di smart city in vista del Giubileo del 2025.

Keywords: Smart City; Sicurezza; Privacy, Protezione dei dati; Roma Data Platform.

1. Introduzione

Le smart city rappresentano un tema di grande attualità. Non c'è città che non si metta alla prova nel progettare e realizzare soluzioni "smart" per migliorare i propri servizi e salvaguardare ambiente e condizioni di vita dei cittadini.

* Gli autori ringraziano il Prof. Paolo Spagnoletti dell'Università Luiss per la preziosa guida e il supporto forniti nello sviluppo di questo lavoro. Si ringrazia anche Unindustria per aver facilitato il confronto con gli stakeholder. Lo studio pubblicato è stato finanziato dall'Unione Europea – NextGenerationEU, Missione 4, Componente 2, nell'ambito del progetto GRINS – Growing Resilient, INclusive and Sustainable (GRINS PE00000018 – CUP B43C22000760006). I punti di vista e le opinioni espresse sono esclusivamente quelle degli autori e non riflettono necessariamente quelle dell'Unione Europea, nè può l'Unione Europea essere ritenuta responsabile per esse.

Teoria e Critica della Regolazione Sociale, n. 2, 2024 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320786 • DOI: 10.7413/197054760152

In questo contesto, i dati divengono una risorsa necessaria delle moderne aree urbane. Al riguardo, i big data e le nuove opportunità che essi rappresentano hanno senz'altro contribuito in modo determinante alla trasformazione delle smart city (Hashem et al., 2016; Bibri, 2018). Le ricerche dimostrano che un apposito disegno programmatico che riguardi la raccolta, la gestione e l'analisi dei dati nelle smart city è fondamentale per creare città che siano operativamente maggiormente efficienti (Al Nuaimi et al., 2015; Hashem, 2016; Lim et al., 2018). In qualunque smart city, la capacità di gestire questi dati e di facilitarne il trasferimento e lo scambio tra soggetti, sistemi e piattaforma, garantisce la loro interoperabilità e promuove una collaborazione sostenibile (Brutti et al., 2019; Buchinger et al., 2021). Tale interoperabilità consente un flusso efficiente di informazioni e una migliore comunicazione tra amministrazioni, organizzazioni private e cittadini (Koo & Kim, 2021). Inoltre, rendendo le informazioni prontamente disponibili e garantendo un accesso paritario ai dati, le smart city forniscono un approccio più trasparente alla condivisione dei dati e alla cooperazione (Hardy & Maurashat, 2017).

Partendo dalla osservazione che le smart city e le piattaforme che ne supportano il funzionamento si nutrono di dati, grandi masse di dati (big data), risulta cruciale individuare forme di condivisione dei dati che possano migliorare le smart city, utilizzando, ove possibile, anche le nuove risorse previste dal Data Governance Act e dal Data Act (Sánchez-Corcuera et al., 2019; Voorwinden, 2021).

Se si vuole, allora, migliorare i nostri contesti urbani e i servizi che li corredano si devono esplorare idonee forme di condivisione dei dati [1].

Questo articolo esamina, allora, le forme di condivisione dei dati, del tipo Business-to-Government data sharing per il pubblico interesse; Government-to-Business data sharing e Civic data sharing (Mossberger et al., 2023), le leve normative che possono incentivarle, magari, anche sfruttando il potenziale di "monetizzazione" dei dati (Ritala, 2024) e le soluzioni che devono essere implementate per garantire sicurezza e protezione dei dati.

2. Sfide aperte nelle smart city

Le smart city sono costituite da piattaforme interconnesse. Le infrastrutture ICT e digitali costituiscono la sua spina dorsale. Queste tecnologie digitali consentono a diversi dispositivi e reti di scambiare informazioni in tempo reale per migliorare i servizi che la città offre ai suoi cittadini. Le smart city si affidano

1 Come affermato anche dallo studio ENISA, Progettare La Condivisione dei Dati Personali, 2023, "il successo delle forme di condivisione dei dati dipenderà dall'istituzione di una forte governance dei dati e anche di garanzie efficaci per i diritti e gli interessi delle persone fisiche che siano pienamente conformi al GDPR. La progettazione della protezione dei dati può essere un fattore chiave per costruire un ambiente di condivisione affidabile, in cui le organizzazioni possono inviare dati senza divulgare dati personali o informazioni aziendali sensibili o divulgare dati personali con un adeguato livello di protezione".

tipicamente a dei "*data centers*" o dei "*data lake*" per ospitare tutte le informazioni digitali ottenute attraverso sensori, dispositivi IoT e reti interconnesse (Sinaeepourfard et al., 2020; Ramos et al., 2023). Tuttavia, senza solide misure di sicurezza, questi repository di dati possono essere soggetti ad attacchi informatici che possono mettere a rischio non solo il funzionamento del sistema, ma anche i dati personali dei cittadini (Elmaghraby & Losavio, 2015; Mehmood et al., 2017; Chan et al., 2018).

Secondo Sookhak et al. (2018), nelle smart city, le minacce alla sicurezza si possono manifestare in quattro modi principali. In primo luogo, gli aggressori possono accedere ai sistemi senza essere autorizzati. In secondo luogo, gli aggressori possono accedere a dati ed informazioni sensibili, violando gli accordi di riservatezza intercorrenti con gli utenti. In terzo luogo, gli aggressori possono rendere la piattaforma o il sistema non disponibile per gli utenti o rendere impossibile il suo funzionamento (ad esempio, con attacchi DoS). Infine, le violazioni della sicurezza possono consistere anche nella violazione dei dispositivi che sono utilizzati per inviare e ricevere false comunicazioni. È, quindi, essenziale sviluppare meccanismi resilienti per proteggere le applicazioni delle smart city. Tuttavia, la ricerca mostra anche che gli attuali modelli di difesa della cybersecurity non sono in grado di tenere il passo dello sviluppo delle smart city, in considerazione della natura scalabile e dinamica di questi nuovi modelli urbani (Cui et al., 2018; Chen et al., 2021). La sicurezza e la privacy sono strettamente dipendenti l'una dall'altra; pertanto, qualsiasi violazione della sicurezza può portare all'accesso abusivo e all'uso improprio di informazioni che dovrebbe rimanere riservate (Belance-Gracia et al., 2015; Khan et al., 2017; Cao et al., 2020). I dati devono essere protetti in tutte le attività di trattamento, che riguardano il loro trasferimento, l'archiviazione e l'elaborazione; mentre, qualsiasi violazione di una piattaforma può mettere a rischio l'integrità dell'intero sistema su cui poggia la smart city. Per questo motivo, è assolutamente indispensabile stabilire misure di sicurezza adeguate che evitino accessi abusivi da parte di soggetti non autorizzati (Propecul & Genete, 2016; Khatoun & Zeadally, 2017). Del resto, proprio per salvaguardare adeguatamente le informazioni sensibili ed evitarne la loro perdita di riservatezza, le smart city dovrebbero porre l'accento anche sulle specifiche misure richieste dai big data (Edwards, 2016; Khatoun & Zeadally. 2017) e investire nella progettazione e nell'implementazione di adeguate tecnologie (Khan et al., 2017; Gharaibeh et al., 2017; Cao et al., 2020).

Al giorno d'oggi, l'assenza di un quadro normativo omogeneo che abbia come oggetto le smart city può essere considerata una barriera per una più ampia adozione dei servizi smart city, poiché non esiste un quadro chiaro che indichi come affrontare e risolvere correttamente le questioni che si pongono nella pratica e come promuovere una cooperazione sicura tra le piattaforme (Lucic, et al., 2018; Weber & Žarko, 2019). Inoltre, è stato dimostrato che affrontare tali questioni è importante per mantenere il sostegno e la partecipazione dei cittadini allo sviluppo delle smart city (Van, 2016). Ciononostante, le amministrazioni locali sono spinte dalle aziende ad implementare le tecnologie per le smart city senza aver preventivamente affrontato le esigenze e le richieste dei

cittadini in merito alle modalità di generazione e utilizzo dei big data (Viitanen & Kingston). (Viitanen & Kingston, 2014). Sebbene diversi studiosi abbiano cercato di offrire una soluzione per tutelare i dati personali e la sicurezza nelle smart city, il compromesso tra il raggiungimento della sicurezza e la creazione di servizi efficienti è comunque estremamente impegnativo (Badii et al., 2020; Al-Turjman et al., 2022). Il motivo potrebbe essere agganciato al fatto che l'Internet delle cose (IoT) presenta molte vulnerabilità e l'eterogeneità e la scalabilità delle smart city oggi richiedono norme più puntali e severe (Qu et al., 2019). Di conseguenza, la costruzione di strategie personalizzate, quadri normativi e soluzioni tecnologiche su misura può essere considerata la chiave del successo delle applicazioni per le smart city.

3. Le smart city e la condivisione dei dati

Le smart city rappresentano al giorno d'oggi sicuramente un nuovo paradigma di condivisione dei dati che vengono raccolti ed elaborati mediante le tecnologie più varie: sensori, applicativi Big Data, IoT, algoritmi di AI (Hashem et al., 2016; Bibri, 2018).

L'inserimento delle tecnologie utilizzate nel sistema delle smart city nella più ampia rete dell'Internet of Things (IoT) amplifica – senz'altro – i rischi per i dati, tra cui anche quelli che dipendono da interconnessioni e scambi massivi (Mehmood et al., 2017; Chan et al., 2018; Colapietro, 2023).

Le smart city hanno bisogno di nutrirsi di dati, essendo la circolazione, la condivisione, la portabilità e l'interoperabilità le sue basi portanti (Paolucci & Pollicino, 2023). Non vi è dubbio, infatti, che più sono i dati raccolti ed elaborati dalle smart city, migliori e più efficienti sono i servizi erogati ai cittadini.

Ma la raccolta di grandi masse di dati, necessarie per l'operatività delle smart city, pone come già indicato significative criticità per quanto riguarda la sicurezza e la protezione dei dati personali.

È allora evidente che, nella fase di progettazione e poi nella concreta implementazione della loro governance, delle loro infrastrutture e delle tecnologie che le supportano e che rendono possibile la condivisione dei dati deve essere considerata anche la protezione dei dati personali (Khan et al., 2017; Cao et al., 2020).

Dopo di che, non c'è protezione dei dati senza adozione di misure di sicurezza adeguate. Sicurezza e protezione dei dati personali sono ambiti tra loro strettamente implicati e solo l'adozione di misure di sicurezza adeguate può realizzare un'efficace protezione dei dati. Nelle smart city, dunque, devono essere considerate, da un lato, le istanze di protezione dei dati personali; dall'altro, le sfide poste dalle moderne e sempre più insidiose minacce cibernetiche, da contrastare con le necessarie misure di prevenzione e reazione (Zhang et al., 2017; Appio et al., 2019; Makedoom et al., 2020).

Nonostante la chiarezza di una simile osservazione, la tutela dei dati personali nelle smart city è scarsamente considerata dalla letteratura e lo è ancora meno nelle sue applicazioni pratiche (Eckhoff, 2017).

Mentre, è stato evidenziato che per realizzare un sistema di condivisione dei dati utile e valido è necessario generare un clima di fiducia digitale nei cittadini[2].

La considerazione delle aspettative di *privacy* e di sicurezza dei dati dei cittadini è la premessa fondamentale – come detto – per qualsiasi attività di progettazione e sviluppo di una qualunque smart city o di sue parti e/o servizi[3].

Diventa, poi, pertinente e rilevante parlare di una "privacy" complessiva della smart city, piuttosto che di "privacy" delle singole tecnologie che la integrano (Paolucci & Pollicino, 2023).

Ma come si concilia la fame di dati delle smart city con le esigenze di protezione dei dati personali? Come si possono al contempo assicurare privacy e sicurezza senza limitare lo sviluppo delle smart city?

4. Metodologia

L'obiettivo che, allora, si pone è quello di affrontare le suddette questioni anche alla luce dei recenti interventi normativi in materia di Strategia Europea dei Dati e delle innovazioni emergenti, che possono rendere queste moderne aree urbane più sicure rispetto al trattamento dei dati e, di conseguenza, migliorarne la funzionalità. A tal fine, questo articolo si basa sulla osservazione della Roma Data Platform (nel seguito, RDP), una piattaforma digitale progettata per integrare informazioni provenienti da fonti diverse in un unico sistema preposto al governo della smart city di Roma. Nonostante il suo potenziale, l'attuale piattaforma ha una portata limitata. Nella configurazione attuale, gli archivi di dati e l'interoperabilità tra sistemi IoT sono efficaci solo per uso interno. Atteso che la RDP intende estendere il suo campo di applicazione a un sistema interconnesso di condivisione dei dati tra varie entità, nel tentativo di migliorare i propri servizi ai cittadini, questo articolo mira a fornire una panoramica delle pratiche che possono supportarla, basandosi su un'ampia revisione della letteratura e sulla stretta collaborazione con le figure chiave coinvolte nella progettazione e nell'amministrazione della RDP.

Per acquisire elementi utili di valutazione sono stati, quindi, raccolti dati primari e secondari. I dati primari sono consistiti in discussioni e incontri con i rappresentanti dello sviluppo della RDP. Ciò ha permesso di entrare in contatto diretto con

2 Documento di lavoro dei servizi della Commissione – Orientamenti sulla condivisione dei dati del settore privato nell'economia europea dei dati che accompagna il documento Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni 'Verso uno spazio comune europeo dei dati' (COM (2018) 232 final).

3 Come affermato anche dallo studio ENISA, Progettare La Condivisione dei Dati Personali, 2023, "il successo delle forme di condivisione dei dati dipenderà dall'istituzione di una forte governance dei dati e anche di garanzie efficaci per i diritti e gli interessi delle persone fisiche che siano pienamente conformi al GDPR. La progettazione della protezione dei dati può essere un fattore chiave per costruire un ambiente di condivisione affidabile, in cui le organizzazioni possono inviare dati senza divulgare dati personali o informazioni aziendali sensibili o divulgare dati personali con un adeguato livello di protezione".

le figure chiave coinvolte nel progetto e di ottenere una comprensione completa dello sviluppo graduale e del suo funzionamento in termini di infrastruttura informativa e governance dei dati. La raccolta di dati primari è stata particolarmente preziosa anche per comprendere le sfide e i limiti attuali del sistema. Quest'ultima aiuterebbe a riconoscere le aree che devono essere affrontate e le attuali barriere che impediscono alla RDP di operare a pieno regime. Inoltre, i dati secondari sono consistiti in un'ampia analisi della letteratura che si è articolata in tre fasi importanti: in primo luogo, è stata effettuata un'analisi desk su come le smart city raccolgono, monitorano e analizzano i dati condivisi tra autorità pubbliche e private. In secondo luogo, l'analisi è consistita nello smontare i progetti di smart city più consolidati dal punto di vista tecnologico, normativo e legale. Si è trattato di un passo fondamentale per capire come le iniziative attualmente più rivoluzionarie e di successo al mondo gestiscano i rischi legati ai temi della sicurezza e della privacy senza compromettere la loro efficienza operativa. Infine, l'analisi si è concentrata sul confronto tra le diverse iniziative nel tentativo di arrivare a delle soluzioni ideali (Baskerville et al., 2013).

5. Roma Data Platform

La Roma Data Platform (RDP nel seguito, per brevità) è una piattaforma digitale. La RDP ha una propria infrastruttura, i propri dataset, le proprie logiche ed anche sensori distribuiti. È in grado di raccogliere ed elaborare dati eterogenei e costituisce uno strumento utile di governance per l'Amministrazione comunale di Roma. La RDP si compone di un "cruscotto" centralizzato per l'osservazione e la gestione delle informazioni relative agli aspetti essenziali della vita urbana quotidiana nella città di Roma (Ariano, 2021).

La Roma Data Platform è stata lanciata nel 2020 dalla Città di Roma proprio con l'ambizioso scopo di diventare il cruscotto della città e di portarla ad essere un modello esemplare di smart city. La RDP mira a valorizzare le enormi quantità di informazioni prodotte dalla Città di Roma e dai cittadini tramite l'utilizzo di dispositivi connessi e intende migliorare la governance della città basata sui dati (data-driven), facendola evolvere a grande velocità.

Essa supporta, di fatto, molteplici forme di condivisione dei dati, non solo tra soggetti pubblici ma anche tra i predetti e le imprese private. La RDP è in continua evoluzione e sviluppo e incorpora ciclicamente nuovi stakeholder, dati, conoscenze, algoritmi e altri strumenti di elaborazione. L'architettura informatica che supporta RDP è in grado di raccogliere, registrare ed integrare molteplici flussi di informazioni provenienti da fonti diverse, riuscendo ad incorporarle in un unico sistema. Tutte queste informazioni vengono elaborate dalla RDP che restituisce dei *"data insights"* utili per la governance cittadina ed anche per gli stessi cittadini. In effetti, l'ulteriore obiettivo della RDP è proprio quello di promuovere la partecipazione attiva dei cittadini alla condivisione dei dati, in modo tale che questa partecipazione possa aggiungere valore per l'intero ecosistema dei dati, supportando ulteriormente una governance intelligente

della città e agevolando anche il processo decisionale-strategico delle imprese che scambiano dati.

Poiché la città di Roma genera un'enorme quantità di dati, il progetto Roma Data Platform offre l'opportunità di creare un ampio repository per l'archiviazione e lo scambio di dati con altri sistemi e vari stakeholder. Tuttavia, nel corso degli anni, il suo utilizzo è stato limitato alla governance della città, mancando l'interoperabilità diretta e le connessioni con attori esterni, nonché non più accessibile dai cittadini. In collaborazione con le figure chiave coinvolte nella creazione e nell'amministrazione della piattaforma, è stata condotta una valutazione strategica delle sue capacità e della possibilità di aprirsi allo scambio di dati con entità esterne come organizzazioni private, imprese e cittadini.

La RDP adotta un approccio federato per la gestione dei dati, allineandosi anche con i principi di Gaia-X[4]. Gaia-X rende disponibile le principali linee guida per realizzare piattaforme e strumenti che coinvolgono dati eterogenei ma non fornisce del software ne degli applicativi pronti all'uso. Al seguito di Gaia-X, per facilitare lo sviluppo ed il fiorire dell'economia dei dati europea, composto da molteplici realtà e stakeholder, nasce FIWARE. Contrariamente a Gaia-X, FIWARE non ha lo scopo di promulgare linee guida ma bensì rende disponibili diverse componenti software pronte all'uso e all'integrazione per realizzare smart city efficienti e soprattutto rispettose delle normative europee (Fiware, 2024). Utilizzando FIWARE come base software, RDP promuove la condivisione e l'interoperabilità dei dati tra i vari ecosistemi urbani. Ogni ecosistema è gestito in maniera quasi indipendente, supportando l'approccio federato nella gestione dei dati che è un pilastro fondante di Gaia-X. Proprio grazie a questo approccio, e con l'ausilio del software reso disponibile da FIWARE, la RDP consente non solo alla città di Roma ma anche a tutti gli altri stakeholder di mantenere la sovranità dei dati, assicurando che le informazioni rimangano sotto il controllo dei rispettivi proprietari e garantendo che siano utilizzati in conformità con le normative europee sulla privacy e la sicurezza. Di fatto, Gaia-X stabilisce un modello e le linee guida generali per la gestione decentralizzata, con lo scopo di evitare il proliferare dei silos di dati, ovvero la centralizzazione delle informazioni dove ogni stakeholder controlla e gestisce singolarmente i propri dati, mentre FIWARE mette a disposizione proprio gli strumenti informatici per poter dare forma a questa visione. In questo modo si

4 Con lo scopo di create un'economia europea dei dati nasce Gaia-X. Si tratta di un'iniziativa tutta europea con l'obiettivo di creare un'infrastruttura federata e sicura per i dati. Diversamente da altre soluzioni, è interamente basata su valori europei, quali controllabilità, trasparenza, interoperabilità e portabilità. Lo scopo principale di Gaia-X è gettare le basi per stabilire un ecosistema fidato di dati dove questi possano essere condivisi e resi disponibili, lasciando agli utenti la sovranità sui propri dati ed il loro controllo. Gaia-X mira quindi a collegare vari fornitori di servizi, anche cloud, ed utenti in un sistema trasparente e federato. È proprio questa federazione che consente la portabilità e l'interoperabilità di dati e servizi attraverso i più diversi settori e piattaforme. Regole comuni permettono ai fornitori ed agli utenti di fidarsi reciprocamente e sono basate su di una tecnologica che facilita lo scambio libero e sicuro tra molteplici stakeholders. Questo specifico punto è fondamentale nel supportare la sovranità digitale in Europa ed al contempo non limitare l'innovazione.

favorisce la collaborazione tra stakeholder eterogenei, inclusi produttori di dati, gli sviluppatori di applicazioni e gli enti sia pubblici che privati. La RDP, quindi, non solo intende garantire la sicurezza e la privacy dei dati, ma vuole anche facilitare l'innovazione e la competitività nell'economia digitale, contribuendo a un ecosistema urbano più intelligente, resiliente, sostenibile e con un valore aggiunto tangibile. Per ricapitolare i principali pilastri di Gaia-X, possiamo sintetizzare cinque i principali obiettivi di Gaia-X orientati su altrettanti cinque temi distinti (Bonfiglo, 2021):

- *Sovranità dei Dati*: Garantire che i proprietari dei dati mantengano il controllo sui loro dati;
- *Ecosistemi Federati*: Creare un'infrastruttura di dati interconnessa e decentralizzata;
- *Prestazioni e Scalabilità*: Costruire servizi cloud e di dati efficienti e scalabili;
- *Conformità e Standard*: Adesione alle normative e stabilimento di standard comuni;
- *Sicurezza e Fiducia*: Migliorare la cybersicurezza e costruire fiducia nei servizi digitali.

A marzo 2024, ha preso avvio il progetto "Evoluzione Roma Data Platform", in cui l'Amministrazione comunale di Roma ha inteso investire le risorse necessarie per potenziare la RDP, per migliorare l'efficienza e l'inclusività della gestione urbana in vista del Giubileo 2025 (Comune di Roma, 2024).

6. Incentivare la condivisione dei dati

Le collaborazioni, la condivisione dei dati e il coordinamento tra il settore pubblico e quello privato è, sicuramente, il "motore principale" di una smart city, nel cui ambito hanno un crescente ruolo attivo anche i cittadini (Voorwinden 2021).

La collaborazione sui dati consente di indirizzare i dati, che sono nel dominio di soggetti privati (imprese, in particolare), verso istanze di interesse collettivo (Spagnoletti et al., 2025; Kazemargi et al. 2023). Ma si tratta ancora di pratiche non sufficientemente sperimentate, atteso che – soprattutto nel settore privato – i dati sono prevalentemente utilizzati all'interno delle organizzazioni.

Si osserva che tradizionalmente lo scambio di dati nel settore privato è ostacolato da due cause principali[5]. Le aziende tendono a trattare i dati per il loro uso esclusivo e per mantenere un vantaggio competitivo rispetto ai loro concorrenti. Dopo di che, i privati mantengono i dati di cui sono titolari all'interno della loro organizzazione e non sono disposti a condividerli, quando i benefici che ne trae il pubblico sono poco chiari o quando il loro utilizzo non è sufficientemente remu-

5 European Commission, 2020. *Towards a European strategy on business-to-government data sharing for the public interest.* Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing.

nerativo rispetto alle loro missioni imprenditoriali" (Grimaldi & Fernandez, 2019; Mossberger et al., 2023).

Quindi, per invertire questa tendenza, va fatta pressione:

- da un lato, sulle imprese private, per migliorare lo scambio di dati secondo le formule "Business to Government data sharing" e "Government to Business data sharing";
- dall'altro, sui cittadini, che decidono di condividere i loro dati (c.d. "Civic data sharing"). Questi dati servono alle smart city, in quanto sono ricchi delle informazioni necessarie alla fornitura e al miglioramento dei servizi[6].

Le smart city devono, allora, adoperarsi per attirare il conferimento dei dati da parte degli stakeholder nelle forme del "Business to Government data sharing" e del "Civic data sharing".

Peraltro, assicurandosi che gli incentivi pensati a vantaggio dei partecipanti non costituiscano pratiche vietate proprio sotto il profilo della protezione dei dati personali.

Con provvedimento in data 8 giugno 2022, dal titolo *"Cittadinanza a punti": Garante privacy ha avviato tre istruttorie. Preoccupanti i meccanismi di scoring che premiano i cittadini "virtuosi"*, infatti, l'Autorità Garante per la Protezione dei Dati Personali ha comunicato di avere avviato alcune istruttorie su una serie di progetti sperimentali promossi enti pubblici e società private, volti ad attribuire dei premi ai cittadini che avessero scelto di condividere spontaneamente i loro dati nella smart city. L'intervento dell'Autorità Garante per la Protezione dei Dati Personali si è reso necessario, poiché queste pratiche risultavano rischiose per i diritti e le libertà degli interessati, tra i quali, anche soggetti vulnerabili. Tra queste istruttorie spicca quella avviata dall'Autorità Garante per la Protezione dei Dati Personali in merito al "Progetto Pollicino", che ha interessato il Comune di Bologna, la Fondazione per lo Sviluppo Sostenibile, il Ministero della Transizione Ecologica e il Ministero delle Infrastrutture e della Mobilità Sostenibile e alcune società private preposte alla erogazione dei premi ai cittadini (Vigorito 2023).

Nello specifico, il progetto prevedeva di svolgere di indagini statistiche di tipo sperimentale nelle quali i cittadini erano incentivati a conferire i loro dati (apparentemente "in forma anonima"), per consentire analisi utili allo sviluppo dei servizi della smart city. Quale contropartita della condivisione dei propri dati, il cittadino veniva poi ammesso ad usufruire dei premi offerti dai partner privati del progetto.

6 "Il successo delle forme di condivisione dei dati dipenderà anche dall'istituzione di una forte governance dei dati e di garanzie efficaci per i diritti e gli interessi delle persone fisiche che siano pienamente conformi al GDPR. L'ingegneria della protezione dei dati può essere un fattore chiave per costruire un ambiente di condivisione affidabile, in cui le organizzazioni possono inviare dati senza divulgare dati personali o informazioni aziendali sensibili o divulgare dati personali con un adeguato livello di protezione" (ENISA 2023).

7. Data Governance Act e Data Act

Anche i recentissimi interventi normativi relativi alla Strategia Europea per i Dati concretizzano ulteriori opportunità utili a raggiungere gli obbiettivi di smart city di cui sopra e dovranno – senz'altro – essere oggetto di approfondimenti e sviluppi.

Nello specifico, il Data Governance Act (Regolamento europeo 2022/868 del 30 maggio 2022) può essere sfruttato per la condivisione dei dati Government to Business Data Sharing.

Il Data Governance Act si propone di rimuovere gli ostacoli alla condivisione dei dati nel settore pubblico. Seppure la condivisione dei dati in questo settore sia una pratica senz'altro più sperimentata che nel settore privato – come visto sopra – è rimasta comunque sottoutilizzata per i motivi più vari. Tra questi, la scarsa fiducia e il poco interesse nella condivisione come tale (senza un qualche ritorno economico e, più in generale, di utilità), ma anche gli ostacoli normativi al riutilizzo dei dati[7].

Il considerando 5 del Data Governance Act afferma che "è necessaria per aumentare la fiducia nella condivisione dei dati istituendo adeguati meccanismi che garantiscano il controllo da parte degli interessati e dei titolari dei dati sui dati che li riguardano e al fine di affrontare altri ostacoli al buon funzionamento di un'economia competitiva basata sui dati".

L'intervento del legislatore europeo mira a "creare fiducia tra gli individui e le imprese per quanto riguarda l'accesso ai dati, la loro condivisione e il loro controllo, utilizzo e riutilizzo, in particolare stabilendo adeguati meccanismi per gli interessati affinché conoscano ed esercitino fattivamente i propri diritti nonché per quanto riguarda il riutilizzo di alcune tipologie di dati detenuti dagli enti pubblici, la fornitura di servizi da parte dei fornitori di servizi di intermediazione dei dati agli interessati, ai titolari e agli utenti dei dati, nonché la raccolta e il trattamento dei dati messi a disposizione a fini altruistici da persone fisiche e giuridiche". [8]

Il Data Governance Act sosterrà, inoltre, lo sviluppo di spazi comuni di dati europei in vari settori che interessano anche le smart city (come la sanità, l'ambiente e la mobilità) "per condividere o trattare congiuntamente i dati, anche ai fini dello sviluppo di nuovi prodotti e servizi, della ricerca scientifica o di iniziative della società civile. I servizi di intermediazione dei dati potrebbero includere la condivisione bilaterale o multilaterale dei dati o la creazione di piattaforme o banche dati che consentano la condivisione o l'utilizzo congiunto dei dati, nonché *l'istituzione di un'infrastruttura specifica per l'interconnessione di interessati e titolari dei dati con gli utenti dei dati*" (considerando 27).

Queste iniziative mirano a facilitare la condivisione dei dati, permettendo ai cittadini e alle imprese di appropriarsi dei relativi vantaggi.

7 European Commission, 2020. *Towards a European strategy on business-to-government data sharing for the public interest.* Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing.

8 https://digital-strategy.ec.europa.eu/en/policies/data-governance-act

Rientrano nell'ambito di applicazione del Data Governance Act sia i dati personali che quelli non personali, con tutte le complesse implicazioni che ne conseguono circa l'applicabilità – rispetto ai primi – del Regolamento europeo 2016/679.

Date queste premesse, è di immediata evidenza che il Data Governance Act potrebbe essere estremamente utile per incentivare forme di condivisione dei dati all'interno delle smart city. Infatti, i dati potenzialmente oggetto di riuso, detenuti dai soggetti pubblici, potrebbero costituire oggetto di scambio con le imprese private per attirare, nelle smart city in generale e nella Roma Data Platform in particolare, dati, congrui investimenti e nuove tecnologie utili a migliorare le sue infrastrutture e i suoi servizi.

Salva la necessità di approfondire più nel dettaglio le opportunità offerte dal Data Governance Act e le limitazioni che ad esso può porre il Regolamento europeo 2016/679, ai nostri fini sicuramente rileva l'art. 6, paragrafi 1 e 4 del Data Governance Act, alla cui stregua "Gli enti pubblici che consentono il riutilizzo … di dati … possono imporre tariffe per consentire il riutilizzo di tali dati" e che "Qualora gli enti pubblici applichino tariffe, essi adottano misure per incentivare il riutilizzo di dati… a fini non commerciali, quali la ricerca scientifica, e da parte delle PMI e delle start-up in conformità delle norme sugli aiuti di Stato. A tale riguardo, gli enti pubblici possono anche mettere a disposizione i dati a una tariffa ridotta o nulla, in particolare per le PMI e le start-up, la società civile e gli istituti di istruzione. A tal fine, gli enti pubblici possono stilare un elenco di categorie di riutilizzatori a cui i dati per il riutilizzo sono forniti a una tariffa ridotta o a titolo gratuito. Detto elenco è reso pubblico unitamente ai criteri adottati per la sua redazione".

Peraltro, il fatto che sia possibile applicare delle tariffe al riutilizzo dei dati, potrebbe anche aprire ad accordo o ad altre forme di monetizzazione e/o, comunque, di valorizzazione dei dati.

Il Data Act (Regolamento europeo 2023/2854 del 13 dicembre 2023) potrebbe, invece, essere utilmente sfruttato per la condivisione dei dati del tipo Civic Data Sharing, come sarà indicato di seguito.

Per converso, il Data Act non può essere utilizzato per sostenere forme di condivisione dei dati del tipo "Business to Government", di tipo volontario. A ben vedere, infatti, questo atteso intervento normativo non introduce elementi di novità rispetto ad iniziative volontarie di *data sharing* del tipo "Business to Government" (cfr. considerando 65 e 66), che restano escluse dal suo campo di applicazione, focalizzato su obblighi di condivisione dei dati per ragioni di emergenza pubblica (Masnada, 2023).

8. Dati dei Cittadini ("Civic Data Sharing")

Come detto, i cittadini hanno senz'altro un ruolo attivo rispetto agli obbiettivi di smart city che si stanno considerando (Grimaldi e Fernandez, 2019). In definitiva, si tratta di ipotizzare un contesto partecipato da vari stakeholder che mirano ad un obbiettivo comune di interesse pubblico. Segnatamente, gli autori dell'articolo

"*The public good and public attitudes toward data sharing through IoT*" mettono in evidenza che i cittadini sono disposti a conferire i dati a soggetti pubblici e privati se hanno un ritorno in termini di vantaggi personali o di tipo collettivo – una migliore sanità pubblica, minor traffico, ecc. (Mossberger et al., 2023).

In definitiva, i cittadini trasferiscono i loro dati quando hanno fiducia in colui che li riceve e che li tratterà e se ha anche un ritorno personale, che però – come abbiamo visto – non può basarsi su sistemi di scoring e correlati premi, se questo impatta sui loro diritti e libertà personali.

Ora interessanti prospettive di "*Civic Data Sharing*" possono conseguire – come detto – anche dalla applicazione del Data Act, alla cui stregua "su richiesta di un utente, o di una parte che agisce per conto di un utente, il titolare dei dati mette a disposizione di terzi i dati prontamente disponibili, nonché i pertinenti metadati necessari a interpretare e utilizzare tali dati, senza indebito ritardo, con la stessa qualità di cui dispone il titolare dei dati, in modo facile, sicuro, a titolo gratuito per l'utente, in un formato completo, strutturato, di uso comune e leggibile da dispositivo automatico e, ove pertinente e tecnicamente possibile, in modo continuo e in tempo reale" (art. 5, Data Act).

Il diritto dell'utente, di condividere i dati con terzi previsto dal Data Act, costituisce un'estensione del diritto alla portabilità dei dati personali, già previsto all'art. 20, Regolamento europeo 2016/679 e potrebbe avere rilevanti applicazioni nel contesto che ci sta occupando, rafforzando gli strumenti degli individui per trasferire i loro dati da un fornitore ad un altro.

9. Modelli di protezione dei dati personali

Per assicurare il diritto alla protezione dei dati personali trattati nell'ambito delle condivisioni di cui sopra sono tradizionalmente utilizzati due modelli.

Un primo modello che utilizza solo dati anonimizzati e, quindi, applica misure di "privacy", anziché misure di sicurezza. Una soluzione di questo genere elimina – senz'altro – qualsiasi questione in materia di protezione di dati personali, poiché i dati anonimi non sono dati personali e, quindi, non si applica il Regolamento europeo 2016/679.

È stato, però, osservato che – anche rispetto ai dati anonimi – non è sempre risolta ogni questione di protezione dei dati personali, se non sono implementate tecniche di anonimizzazione sufficientemente solide, poiché in questo caso resta alto il rischio di reidentificazione degli interessati. Ad esempio, sono stati reidentificati dati che si credeva fossero stati irreversibilmente anonimizzati, a seguito di incidenti che hanno interessato alcuni database sui dati di navigazione degli utenti (Germania), sui dati relativi alla salute (Italia, Australia), sui dati del trasporto pubblico (Lettonia) (De Cordes, 2019).

È stato, poi, ulteriormente sottolineato che l'anonimizzazione dei dati porta a perdere molte informazioni importanti. In definitiva, i dati anonimizzati diventano meno ricchi di informazioni e, quindi, meno utili agli obbiettivi delle smart city (De Cordes, 2019).

Un altro modello è rappresentato dalla definizione di appositi accordi contrattuali sui dati, che definiscano i soggetti e le responsabilità relative al trattamento dei dati personali. In questo modello, le questioni di "privacy" restano in tutta la loro portata e richiedono che siano definiti i ruoli dei soggetti coinvolti nel trattamento dei dati personali, le informazioni da dare agli interessati, le basi giuridiche necessarie per trattare i dati, le valutazioni d'impatto sulla protezione dei diritti e le libertà fondamentali degli interessati, da effettuare (de Montjoye, 2018).

Rispetto ai due approcci tradizionali visti sopra, si collocano delle soluzioni ulteriori che promuovono lo scambio dei dati sotto il dominio degli utenti, i quali potranno scegliere selettivamente le imprese o i soggetti pubblici che avranno accesso a tutti o parte dei loro dati, nonché la durata del loro utilizzo e tutte le altre condizioni per usufruirne (De Cordes, 2019).

Attraverso, poi, l'esercizio dei diritti degli interessati (artt. 15-2, Regolamento europeo 2016/679) i cittadini potranno, successivamente al loro conferimento, anche controllare come vengono utilizzati i loro dati.

10. Conclusioni e sviluppi futuri

Lo scopo di questo articolo sta nel mettere in evidenza le varie forme di condivisione dei dati tra soggetti pubblici, privati e i cittadini che possono essere utilizzate per migliorare ed accelerare lo sviluppo delle smart city, ponendole nella condizione di rispondere efficacemente ai bisogni di moderne ed affollate aree urbane, come anche la smart city di Roma e la piattaforma che la supporta.

L'attività di analisi di cui sopra è stata condotta andando a vedere se anche i recenti interventi normativi, relativi alla Strategia Europea dei Dati, potessero svolgere un ruolo di impulso e incentivo rispetto a quelle forme di condivisione.

Le smart city hanno, infatti, necessità di raccogliere grandi masse di dati per poter rendere utili ed efficaci servizi ai cittadini.

È, quindi, emerso che in effetti ci sono ulteriori significativi margini di sviluppo nel ricercare quali potrebbero essere le applicazioni concrete di quelle previsioni normative, per incentivare la condivisione dei dati nelle smart city, sfruttando e facendo leva anche sul potenziale di "monetizzazione" dei dati oggetto di scambio, da indirizzare comunque verso l'attuazione di interessi collettivi (mobilità, turismo, sanità).

In questo contesto, non abbiamo potuto prescindere anche dal considerare le problematiche poste dalla necessità di proteggere i dati personali dei cittadini (applicando il Regolamento europeo 2016/679 e la normativa interna in materia di protezione dei dati personali) che, in effetti, sono poco studiate nella letteratura e sono ancora meno considerate nelle loro applicazioni pratiche, delineando quali sono le soluzioni tradizionali proposte ed applicate e quali potrebbero essere le alternative da esplorare.

Nei successivi capitoli di questa ricerca vogliamo allora sviluppare ulteriormente questi temi di indagine, andando anche oltre lo scenario della smart city di Roma

(che è sicuramente riduttivo) per proporre un modello valido e tendenzialmente replicabile per qualunque moderna smart city.

Bibliografia

Abella A., Ortiz-de-Urbina-Criado, M. and De-Pablos-Heredero, C. 2017, "A model for the analysis of data-driven innovation and value generation in smart cities' ecosystems", in *Cities*, *64*, pp.47-53.

Al Nuaimi E., Al Neyadi H., Mohamed N. and Al-Jaroodi, J. 2015, "Applications of big data to smart cities", in *Journal of Internet Services and Applications*, *6*, pp.1-15.

Al-Turjman F., Zahmatkesh H. and Shahroze R. 2022, "An overview of security and privacy in smart cities' IoT communications", in *Transactions on Emerging Telecommunications Technologies*, *33*(3), p. e3677.

Angelidou M. 2015, "Smart cities: A conjuncture of four forces", *Cities*, *47*, 95-106.

Ariano A. 2021, "Il caso della Roma Data Platform", in *Una geografia delle politiche urbane tra possesso e governo. Sfide e opportunità nella transizione*, pp.177-183.

Batty M., Axhausen K.W., Giannotti F., Pozdnoukhov A., Bazzani A., Wachowicz M., Ouzounis G. and Portugali Y. 2012, "Smart cities of the future", in *The European Physical Journal Special Topics*, *214*, pp.481-518.

Baskerville R., de Marco M., & Spagnoletti p. 2013, *Designing Organizational Systems: an interdisciplinary discourse* Cham: Springer. https://doi.org/10.1007/978-3-642-33371-2.

Belanche-Gracia D., Casaló-Ariño L.V. and Pérez-Rueda A. 2015, "Determinants of multi-service smartcard success for smart cities development: A study based on citizens' privacy and security perceptions", in *Government information quarterly*, *32*(2), pp.154-163.

Bibri S.E. and Krogstie J. 2017, "Smart sustainable cities of the future: An extensive interdisciplinary literature review", in *Sustainable cities and society*, *31*, pp.183-212.

Bokolo A. Jnr. 2022, "Data driven approaches for smart city planning and design: a case scenario on urban data management", in *Digital Policy, Regulation and Governance*, vol. 25, n. 4, pp. 351.

Bolognini L. 2024, *Ammissibilità del modello "pay or consent": tra rivoluzione economica digitale e modernizzazione della protezione dei dati. Un* open access paper *dell'Istituto Italiano per la Privacy e la Valorizzazione dei Dati.*

Bonfiglio F. 2021, *Gaia-X Vision and Strategy* (https://gaia-x.eu/wp-content/uploads/2021/12/Vision-Strategy.pdf) (Accessed: May 14, 2024).

Brutti A., De Sabbata p. , Frascella A., Gessa N., Ianniello R., Novelli C., Pizzuti S. and Ponti G., 2019, "Smart city platform specification: A modular approach to achieve interoperability in smart cities", in *The internet of things for smart urban ecosystems*, pp.25-50.

Buchinger M., Kuhn p. , Kalogeropoulos A. and Balta D., 2021, "Towards interoperability of smart city data platforms", in *Proceedings of the 54th Hawaii International Conference on System Sciences*.

Cao Q.H., Giyyarpuram M., Farahbakhsh R. and Crespi N. 2020, "Policy-based usage control for a trustworthy data sharing platform in smart cities", in *Future Generation Computer Systems*, *107*, pp.998-1010.

Chan A.L., Chua G.G., Chua D.Z.L., Guo S., Lim p. M.C., Mak M.T. and Ng W.S., 2018, "February. Practical experience with smart cities platform design", in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)* (pp. 470-475). IEEE.

Chen D., Wawrzynski p. and Lv Z., 2021, "Cyber security in smart cities: a review of deep learning-based applications and case studies", in *Sustainable Cities and Society*, *66*, p. 102655.

Cheng B., Longo S., Cirillo F., Bauer M. and Kovacs E. 2015, "June. Building a big data platform for smart cities: Experience and lessons from Santander", in *2015 IEEE International Congress on Big Data* (pp. 592-599). IEEE.

Chourabi H., Nam T., Walker S., Gil-Garcia J.R., Mellouli S., Nahon K., Pardo T.A. and Scholl H.J., 2012, "January. Understanding smart cities: An integrative framework", in *2012 45th Hawaii international conference on system sciences* (pp. 2289-2297). IEEE.

Colapietro C. 2023, "Intelligenza artificiale e smart cities a mo' di introduzione", in *Smart cities, Diritti, libertà e governance*, pp. XVIII-XXXIV.

Comune di Roma 2024, https:// https://www.comune.roma.it/web/it/attivita-progetto.page?contentId=PRG1163717 (Accessed: May 30, 2024).

Cui L., Xie G., Qu Y., Gao L. and Yang Y. 2018, "Security and privacy in smart cities: Challenges and opportunities", in *IEEE access*, *6*, pp.46134-46145.

da Rosa Lazarotto B. 2022, "The implications of the Proposed Data Act to B2G data sharing in smart cities", available at SSRN.

De Cordes N., de Montjoye Y., Smoreda Z. 2019, *OPAL: reconciling open innovation and data security*.

de Montjoye Y. 2018, "On the privacy-conscientious use of mobile phone data", in *Scientific Data*, 5, Article number: 180286.

Eckhoff D. 2017, Privacy in the Smart City – Applications, Technologies, Challenges and Solutions.

Edwards L. 2016, "Privacy, security and data protection in smart cities: A critical EU law perspective", in *Eur. Data Prot. L. Rev.*, *2*, p. 28.

ENISA 2024, *Engineering Personal Data Protection in EU Sata Space*s. [Online], available at: https://www.enisa.europa.eu/publications/engineering-personal-data-protection-in-eu-data-spaces.

European Commission 2020, *Towards a European strategy on business-to-government data sharing for the public interest.* Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing.

Fiware 2024, https://fiware.org (Accessed: May 14, 2024).

Gharaibeh A., Salahuddin M.A., Hussini S.J., Khreishah A., Khalil I., Guizani M. and Al-Fuqaha A. 2017, "Smart cities: A survey on data management, security, and enabling technologies", in *IEEE Communications Surveys & Tutorials*, *19*(4), pp. 2456-2501.

Grimaldi D. and Fernandez V. 2019, "Performance of an internet of things project in the public sector: The case of Nice smart city", in *The Journal of High Technology Management Research*, *30*(1), pp.27-39.

Hardy K. and Maurushat A. 2017, "Opening up government data for Big Data analysis and public benefit", in *Computer law & security review*, *33*(1), pp. 30-37.

Harrison C., Eckman B., Hamilton R., Hartswick p. , Kalagnanam J., Paraszczak J. and Williams p. 2010, "Foundations for smarter cities", in *IBM Journal of research and development*, *54*(4), pp.1-16.

Hashem I.A.T., Chang V., Anuar N.B., Adewole K., Yaqoob I., Gani A., Ahmed E. and Chiroma H. 2016, "The role of big data in smart city", in *International Journal of information management*, *36*(5), pp.748-758.

Janssen M., Charalabidis Y. and Zuiderwijk A. 2012, "Benefits, adoption barriers and myths of open data and open government", *Information systems management*, *29*(4), pp.258-268.

Kazemargi N., Spagnoletti p. , Constantinides p. , & Prencipe p. 2023, "Data control coordination in cloud-based ecosystems: the GAIA-X case", in C. Cennamo, G. B. Dagnino, & F. Zhu (Eds.), *Handbook of Research on Digital Strategy*, Elgar, pp. 289-307 (https://doi.org/10.4337/9781800378902.00024).

Khan Z., Pervez Z. and Abbasi A.G. 2017, "Towards a secure service provisioning framework in a smart city environment", in *Future Generation Computer Systems*, *77*, pp.112-135.

Khatoun R., & Zeadally S. 2017, "Cybersecurity and privacy solutions in smart cities", in *IEEE Communications Magazine*, *55*(3), 51-59.

King J., Meinhardt C. 2024, *Rethinking Privacy in the AI Era*, Stanford University.

Kitchin R. and Dodge M. 2020, "The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention", in *Smart cities and innovative Urban technologies* (pp. 47-65). Routledge.

Klievink B., Van Der Voort H. and Veeneman W. 2018, "Creating value through data collaboratives", in *Information Polity*, *23*(4), pp.379-397.

Koo J. and Kim Y.G. 2021, "Interoperability requirements for a smart city" in *Proceedings of the 36th Annual ACM Symposium on Applied Computing* (pp. 690-698).

Lévy-Bencheton C. and Darra E. 2015, *Cyber security and resilience of intelligent public transport: good practices and recommendations*.

Lim C., Kim K.J. and Maglio p. P. 2018, "Smart cities with big data: Reference models, challenges, and considerations", in *Cities*, *82*, pp.86-99.

Liu J., Chen N., Chen Z., Xu L., Du W., Zhang Y. and Wang C. 2022, "Towards sustainable smart cities: Maturity assessment and development pattern recognition in China", in *Journal of Cleaner Production*, *370*, p. 133248.

Lučić D., Boban M. and Mileta D. 2018, "An impact of general data protection regulation on a smart city concept", in *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 0390-0394). IEEE.

Masnada M. 2023, "I dati al centro della strategia UE: Data Act e Data Governace Act a confronto", in *Agenda Digitale*, 6 settembre.

Mehmood Y., Ahmad F., Yaqoob I., Adnane A., Imran M. and Guizani S., 2017, "Internet-of-things-based smart cities: Recent advances and challenges", in *IEEE Communications Magazine*, *55*(9), pp.16-24.

Mossberger K., Cho S., Cheong p. H. and Kuznetsova D. 2023, "The public good and public attitudes toward data sharing through IoT", in *Policy & Internet*, *15*(3), pp. 370-396.

Paolucci F. e Pollicino O. 2023, "Intelligenza urbana e tutela dei diritti fondamentali. Antinomia o complementarità nella nuova stagione algoritmica?", in *Smart cities, Diritti, libertà e governance*, pp.17-43.

Pierce p. and Andersson B. 2017, *Challenges with smart cities initiatives–A municipal decision makers' perspective*.

Popescul D. and Genete L.D. 2016, "Data security in smart cities: challenges and solutions", in *Informatica Economică 20*(1).

Qu Y., Nosouhi M.R., Cui L. and Yu S. 2019, "Privacy preservation in smart cities", in *Smart cities cybersecurity and privacy*, Elsevier, pp. 75-88.

Ramos G.S., Fernandes D., Coelho J.A.P.D.M. and Aquino A.L. 2023, "Toward Data Lake Technologies for Intelligent Societies and Cities", in *Sustainable, Innovative and Intelligent Societies and Cities*, Cham: Springer, pp. 3-29.

Ritala p. , Keränen J., Fishburn J. and Ruokonen M. 2024, "Selling and monetizing data in B2B markets: Four data-driven value propositions", in *Technovation*, *130*, p. 102935.

Sánchez-Corcuera R., Nuñez-Marcos A., Sesma-Solance J., Bilbao-Jayo A., Mulero R., Zulaika U., Azkune G. and Almeida A. 2019, "Smart cities survey: Technologies, application domains and challenges for the cities of the future", in *International Journal of Distributed Sensor Networks*, *15*(6), p. 1550147719853984.

Silva B.N., Khan M. and Han K. 2018, "Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities", in *Sustainable cities and society*, *38*, pp.697-713.

Sinaeepourfard A., Krogstie J. and Sengupta S. 2020, "Distributed-to-centralized data management: a new sense of large-scale ICT management of smart city IoT networks", in *IEEE Internet of Things Magazine*, *3*(3), pp.76-82.

Sookhak M., Tang H., He Y. and Yu F.R. 2018, "Security and privacy of smart cities: a survey, research issues and challenges", in *IEEE Communications Surveys & Tutorials*, *21*(2), pp.1718-1743.

Spagnoletti p. , Kazemargi N., Constantinides p. , & Prencipe A. 2025, "Data Control Coordination in the Formation of Ecosystems in Highly Regulated Sectors", in *Journal of the Association for Information Systems,* forthcoming.

Topham S., Boscolo p. and Mulquin M. 2023, *Personal Data-Smart Cities: How cities can Utilise their Citizen's Personal Data to Help them Become Climate Neutral*, Taylor & Francis, p. 365.

Trencher G. and Karvonen A. 2020, "Stretching 'smart': Advancing health and well-being through the smart city agenda", in *Smart and Sustainable Cities?*, Routledge, pp. 54-71.

Trindade E.P., Hinnig M.P.F., da Costa E.M., Marques J.S., Bastos R.C. and Yigitcanlar T. 2017, "Sustainable development of smart cities: A systematic review of the literature", in *Journal of Open Innovation: Technology, Market, and Complexity*, *3*(3), pp.1-14.

Tripodi E. 2024, "Le prospettive potenziali della smart city 'evoluta': la digital twin city", in *Diritto di Internet*, 1/2024, pp. 23-36.

Van Zoonen L. 2016, "Privacy concerns in smart cities", in *Government Information Quarterly*, *33*(3), pp. 472-480.

Vigorito A. 2023, "Sul crinale tra data altruism e social scoring: esperienze applicative della sequenza dati-algoritmi nel nuovo contesto regolatorio europeo", in *Media Laws*, *1/2023*, pp. 104-127.

Viitanen, J. and Kingston R. 2014, "Smart cities and green growth: outsourcing democratic and environmental resilience to the global technology sector", in *Environment and Planning A*, *46*(4), pp. 803-819.

Voorwinden A. 2021, "The privatised city: Technology and public-private partnerships in the smart city", in *Law, Innovation and technology*, *13*(2), pp. 439-463.

Weber M. and Podnar Žarko I. 2019, "A regulatory view on smart city services", in *Sensors*, *19*(2), p. 415.

Wirsbinna A. and Grega L. 2021, "Assessment of economic benefits of smart city initiatives", in *Cuadernos de Economía*, *44*(126), pp. 45-56.

Zhang K., Ni J., Yang K., Liang X., Ren J. and Shen X.S. 2017, "Security and privacy in smart city applications: Challenges and solutions", in *IEEE communications magazine*, *55*(1), pp. 122-129.