DOI: 10.24193/tras.SI2025.10
Published First Online: 12/16/2025

GOVERNING SMART CITY DEVELOPMENT IN POST-WAR UKRAINE*

Oleh ZAIARNYI
Petro KATERYNYCH

Oleh ZAIARNYI

Professor, Educational and Scientific Institute of Law, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
E-mail: olehzaiarnyi@knu.ua
ORCID ID: 0000-0003-4549-7201

Petro KATERYNYCH (corresponding author)

Assistant Professor, Educational and Scientific Institute of Journalism, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
E-mail: petro.katerynych@knu.ua
ORCID ID: 0000-0002-5967-2368

Abstract

This paper examines the critical governance choices for integrating 'smart city' principles into Ukraine's post-war reconstruction, aiming to transform devastated urban areas into resilient, inclusive, and technologically advanced environments. The study combines a doctrinal analysis of Ukraine's current legal gaps with a comparative review of EU and international governance models. It incorporates qualitative findings from a rapid expert elicitation with senior Ukrainian public officials, providing actionable, context-specific insights. The analysis reveals a fragmented legal landscape that lacks a dedicated Smart City Law, which creates risks of uncoordinated deployments and vendor lock-in. While alignment with the EU digital acquis (GDPR, NIS2, AI Act) is a stated goal, significant compliance and capacity challenges persist. Expert consultations confirm unanimous agreement regarding the necessity of a framework statute to set clear mandates, institutionalize citizen participation, and mandate safeguards for public-private partnerships (PPPs) to prevent the erosion of public value. This study offers a structured legal and policy framework tailored to Ukraine's unique post-conflict context.

Keywords: smart city, legal framework, post-war reconstruction, Ukraine, digital transformation, data governance, citizen participation, public-private partnerships.

* **Acknowledgement:** This research was supported by the Ministry of Education and Science of Ukraine under grant number 25БП013-01M (2025-2027).

1. Introduction

Ukraine's post-war urban reconstruction presents a challenge of historic proportions. However, it is also a rare opportunity to leapfrog legacy systems and embed modern governance principles into the digital infrastructures that will shape daily life for decades (Kuzior *et al*., 2022). The imperative to 'build back better' transcends restoring physical assets; it calls for a resilient, sustainable, and citizen-centred transformation (Cabinet of Ministers of Ukraine, 2018). This context reveals an inherent tension between the need for rapid rebuilding to address urgent humanitarian needs and the strategic planning required for long-term sustainability. Hasty decisions, often made under pressure, risk locking Ukraine into suboptimal solutions, such as proprietary technologies that compromise interoperability or surveillance systems that undermine public trust (Greenfield, 2018).

This paper navigates this dilemma by adopting the concept of 'substantial smartness' – the co-production of technological capability with robust, human-centric institutions that guarantee rights, inclusion, and security (Nam and Pardo, 2011). This framework posits that a city is not genuinely 'smart' because it has sensors and dashboards, but because it uses technology to enhance public value and materially improve quality of life (Meijer and Bolívar, 2016). This aligns with a performative view of digital citizenship enacted across platforms rather than possessed as a mere status (Isin and Ruppert, 2015). Data governance sits at the core of these choices. Decisions about what data are collected, who can access them, and under what safeguards will shape future power asymmetries and sustainability outcomes (OECD, 2021). Cities that default to proprietary, vendor-defined platforms may gain short-term speed but risk long-term lock-in and opacity; by contrast, open-data and civic-data-rights approaches can catalyse innovation and sustain transparency (Cardullo and Kitchin, 2019).

Given Ukraine's trajectory toward European integration, this research addresses two central questions:

1. What legal and institutional frameworks are needed to govern smart city reconstruction in Ukraine effectively and ethically, in line with European norms?
2. How can public-private partnerships (PPPs) and citizen participation be structured to ensure accountability, data protection, and human rights in post-war smart city initiatives?

Consequently, this paper hypothesizes (*H1*) that without a comprehensive, EU-aligned legal framework, Ukraine's smart city efforts will remain fragmented, undermining interoperability and citizen trust; conversely, a dedicated 'Smart City Act' will significantly improve coherence and privacy protection. Furthermore, we hypothesize (*H2*) that while well-governed PPPs can accelerate reconstruction, they risk vendor lock-in and the erosion of citizen rights if not buttressed by clear legal safeguards on data ownership, transparency, and accountability. This study combines a doctrinal analysis of Ukrainian laws, a comparative review of international governance models, and qualitative insights from Ukrainian public-sector experts to investigate these propositions.

2. Laying the digital foundation: Ukraine's legal gaps and the European acquis

Ukraine enters its reconstruction phase with notable achievements in digital public services, exemplified by the national Diia platform, which has created a strong foundation of digital literacy and citizen adoption (Ministry of Digital Transformation of Ukraine, 2025). However, this front-end success masks the absence of a consolidated statutory backbone for smart urban development (Oliukha, 2024, p. 340). City leaders encounter significant challenges in procuring complex digital systems under wartime constraints while navigating fragmented mandates and legacy procurement rules that are ill-suited for technology acquisition. The absence of a single, principle-based smart city statute creates an institutional vacuum where long-term decisions on data ownership, interoperability, and liability are being locked into contracts, often without sufficient foresight (Oliukha, 2024, p. 342). This fragmentation tends to result in ad-hoc projects, significant interoperability challenges between cities, and immense difficulties in scaling successful pilots to a national level.

The current legal framework is insufficient for the complex needs of smart city governance in Ukraine. While local governments have constitutional responsibilities under the Law on Local Self-Government, smart city projects – such as city-wide data platforms and sensor networks – often exceed traditional competencies and require new coordination with national authorities (Clement, Ruysschaert and Crutzen, 2023). This results in a 'grey area' of authority, leaving municipalities without clear legal guidelines for implementing smart solutions, which can lead to privacy and security risks. The lack of a dedicated smart city law causes uncoordinated initiatives, with cities potentially adopting varying platforms and data standards that hinder interoperability and national data analysis. Furthermore, existing laws, like the Law on Personal Data Protection (2010) and Ukraine's Cybersecurity Law (2017), are outdated and do not adequately address the challenges posed by modern technology for municipalities managing critical smart systems like power grids (Law no. 2297-VI, 2010, Art. 2; Law no. 2163-VIII, 2017, P. I)

There is currently no liability framework for AI and IoT services in Ukraine. While the Civil Code includes general tort provisions, their application to incidents involving autonomous vehicles or faulty AI is unclear. This highlights the need for a comprehensive legal framework to coordinate reconstruction efforts and establish standards. In a post-conflict context, a smart city requires prioritizing resilience, adaptability, and inclusivity, fostering collaboration between authorities and citizens (Dunayev, Gavkalova and Kud, 2023).

Ukraine's goal of EU membership serves as a roadmap for reconstruction by aligning with the European digital acquis. Understanding these core instruments is crucial as they provide a baseline for municipal deployments (European Parliament and Council, 2024). They establish standards for data privacy, cybersecurity, data sharing, and AI that Ukraine would need to adopt to ensure interoperability and build trust with citizens and

international partners. Table 1 summarizes five key EU instruments and their implications for Ukrainian cities.

Table 1: The EU digital acquis: a practical guide for Ukrainian urban reconstruction

EU instrument	Core Requirements for non-European readers	Implications and actions for Ukrainian cities
General Data Protection Regulation (GDPR)	The EU's cornerstone data privacy law establishes strict rules for processing personal data and grants individuals strong rights (e.g., access, deletion). It mandates a 'privacy-by-design' approach, requiring safeguards to be built into systems from the start.	Every smart system handling personal data–from CCTV to city apps – should be supported by a lawful basis and undergo a Data Protection Impact Assessment (DPIA). Cities would benefit from preparing for the new GDPR-aligned Law (no. 8153, passed first reading on 20 November 2024 (Resolution 4065-IX) by appointing Data Protection Officers (DPOs) and training staff.
NIS2 Directive	A cybersecurity law requiring operators of essential services (energy, transport, digital infrastructure) to implement robust risk management measures, manage supply chain risks, and report significant cyber incidents to national authorities.	Smart city infrastructure (e.g., smart grids, intelligent traffic systems) should be treated as critical infrastructure. Municipalities are advised to conduct continuous risk assessments, ensure contracts with tech vendors include cybersecurity clauses, and integrate with national incident response networks.
Data Governance Act (DGA)	Creates a framework for trusted and secure data sharing. It enables public bodies to share sensitive data under controlled conditions for research and innovation and establishes certified 'data intermediaries' to facilitate sharing between organizations.	Cities can unlock innovation by sharing valuable non-personal data (e.g., traffic patterns, environmental sensor data) with researchers and startups under clear rules. This provides a model for creating municipal 'data trusts' or intermediaries to manage cross-sector data sharing securely.
Open Data Directive	Mandates that non-personal public sector data (e.g., geospatial, mobility, environmental data) be made available for reuse by default in machine-readable formats. It aims to stimulate innovation and transparency by making public data an open resource.	Cities could enhance transparency by publishing datasets like transit schedules, air quality readings, and city budgets on open data portals. All new smart systems should be procured with the requirement that the non-personal data they generate will be made public, fostering a local civic tech ecosystem.
AI Act	A landmark regulation introducing a risk-based framework for Artificial Intelligence. It bans certain harmful AI practices and imposes strict requirements – such as data quality, transparency, and human oversight – on 'high-risk' systems often used in cities (e.g., biometric identification, critical infrastructure management).	Any AI used in public services, like algorithms for welfare benefits or traffic management, should undergo risk evaluation. Cities would benefit from creating public registries of these AI systems and implementing human oversight boards for high-risk applications. For instance, a computer vision module for traffic enforcement that affects fines or prioritization is considered high-risk under Regulation (EU) 2024/1689. This requires compliance with several criteria, including risk management, data governance, automatic logging, transparency for deployers, human oversight, and post-market monitoring.

Source: Authors' analysis of European Union legislation (European Parliament and Council 2016; 2019; 2022a; 2022b and 2024)

While EU alignment provides a robust framework, Ukraine must adapt rather than adopt these instruments wholesale. The GDPR's privacy-by-design principles are universally applicable, but enforcement mechanisms require contextualization to Ukrainian

administrative capacity. Similarly, NIS2's cybersecurity standards are essential but must account for Ukraine's conflict-specific threats.

For Ukraine, adopting these regulations is essential for developing smart infrastructure. The new draft law (Verkhovna Rada, 2024) aligns with GDPR and requires a 'data protection by design' approach, making privacy impact assessments standard in project planning. A strong commitment to privacy is crucial in a post-conflict society with fragile public trust. Compliance with NIS2 principles ensures that city utilities and digital services are secure and integrated into national cyber defense networks amid hostilities. The Data Governance Act (DGA) and the Open Data Directive enhance transparency, promote innovation, and serve as anti-corruption tools during reconstruction by ensuring public visibility of spending and project outcomes.

Anticipating the AI Act is essential for Ukrainian cities. They can build trust and prevent discrimination by conducting risk assessments for AI projects and ensuring human oversight. This proactive approach aligns with international best practices emphasizing transparency and ethical governance (UN-Habitat, 2025; Cowley, Joss and Dayot, 2018). We use UN-Habitat's People-Centered Smart Cities guideline for core principles (UN-Habitat, 2021) and the International Guidelines on People-Centred Smart Cities for implementation-oriented requirements (UN-Habitat, 2025). The People-Centered Smart Cities guidelines stress that digital innovations should enhance social inclusion and human rights, a principle vital to Ukraine's strategy (UN-Habitat, 2021). Adopting a rights-based governance model will ensure technology serves the people, reflecting a global trend towards democratic smart city governance (Calzada, 2021; Wernick and Artyushina, 2023).

3. Global governance models and post-conflict lessons

Examining global governance models that balance state capacity, market involvement, and civic engagement is beneficial in shaping Ukraine's strategy. Examples like Seoul, Singapore, and Dubai illustrate different approaches to smart city governance, providing valuable lessons for Ukraine's democratic goals. Additionally, the experiences of post-war cities such as Sarajevo, Beirut, and Mosul highlight the importance of inclusive, human-centered reconstruction. This section distills these insights for Ukraine.

3.1. Seoul: institutionalized civic participation

Seoul is a model for civic participation, using consistent digital channels to enhance governance (Seoul Metropolitan Government, 2025). Over the past decade, the city has integrated platforms like Democracy Seoul for policy proposals and participatory budgeting into its decision-making (Seoul Metropolitan Government, 2025). A key example is the mVoting app, which allows citizens to influence local issues, from the placement of public benches to late-night bus routes. This goes beyond consultation; the outcomes directly shape municipal actions. These practices instantiate 'acts of citizenship' through datafied

participation (Isin and Ruppert, 2015). The essential takeaway is the bureaucratic culture that ensures participation leads to visible results supported by open data (Cowley, Joss and Dayot, 2018).

The Seoul model highlights the importance of creating simple, auditable participation mechanisms for Ukrainian municipalities, where war has damaged trust. For instance, Chernihiv could use a similar app to involve residents in prioritizing community space reconstruction. The existing civil society and participatory elements of the Diia platform provide a strong base for this initiative. The main challenge is transforming occasional consultations into established laws and routines to ensure longevity beyond political cycles (UN-Habitat, 2025).

3.2. Singapore: state-led engineering and efficiency

Singapore's Smart Nation program is the archetype of a whole-of-government engineering core. A central agency, GovTech, designs shared platforms, enforces secure baselines, and brokers interoperability across all public bodies (GovTech Singapore, 2025). A key case study is the Smart Nation Sensor Platform, a nationwide network of sensors and data-sharing gateways that provides real-time data for public agencies. This central infrastructure enables services like predictive maintenance for elevators in public housing and dynamic traffic light control to ease congestion, all managed through a common technical backbone. While Ukraine is unlikely to replicate Singapore's centralized political economy, it can imitate its logic by creating a national centre of excellence – a 'GovTech-lite' model. This body could provide an 'engineering spine' for reconstruction by developing national data standards, cybersecurity protocols, and reusable software components (e.g., a standardized module for utility payments) that municipalities can adopt. This would be particularly valuable for smaller cities that lack specialized expertise, preventing them from becoming dependent on single-vendor solutions. However, unlike Singapore, Ukraine would need to ensure such a central body is subject to robust democratic oversight to foster, rather than stifle, local innovation.

3.3. Dubai: PPP-driven innovation with guardrails

Dubai's evolution showcases the impressive speed and scale possible through a public-private partnership (PPP) model in implementing advanced urban technologies (Government of Dubai, 2015). A key example is the Smart Dubai Platform, developed in partnership with IBM, which consolidates city data for public and private use, facilitating innovations like AI-powered traffic management and paperless services. The crucial lesson for Ukraine is establishing a business-friendly environment with transparent procurement processes. Dubai's experience also highlights the risks of vendor lock-in if contracts lack safeguards (March and Ribera-Fumaz, 2018). Rather than replicate Dubai's model, Ukraine could benefit from pursuing a 'Dubai-with-guardrails' approach, promoting PPPs while ensuring contracts include provisions for open standards, municipal

ownership of non-personal data, and auditing rights. This strategy will enable Ukraine to harness private sector agility while protecting long-term public interests.

3.4. Lessons from post-conflict reconstruction

The experiences of cities recovering from armed conflict provide an essential filter for these models, grounding them in the realities of social trauma, fragmented governance, and urgent human needs. Sarajevo's reconstruction in a complex multi-ethnic environment underscores the critical importance of inclusive governance. Initially plagued by uncoordinated efforts from various international donors, the city's recovery gained traction only when local authorities and community groups were empowered to set priorities. The lesson for Ukraine is that a top-down, purely technocratic approach to 'smart' rebuilding will fail if it does not engage local communities, including displaced persons, in the planning process (Municipality of Sarajevo, 2025).

In Ukraine, adopting this policy can provide a low-risk foundation for using non-personal public data, such as mobility counts and environmental metrics, aligned with the EU's Open Data Directive. Beirut's post-war reconstruction is a cautionary tale against elite-centered redevelopment, as seen with the Solidere project, which created an exclusive district disconnected from the broader city (Marot, 2018). For places like Mariupol, the lesson is to avoid privatizing public spaces and ensure reconstruction includes affordable housing and accessible services to prevent social inequalities. An equitable 'smart' city is essential for true success.

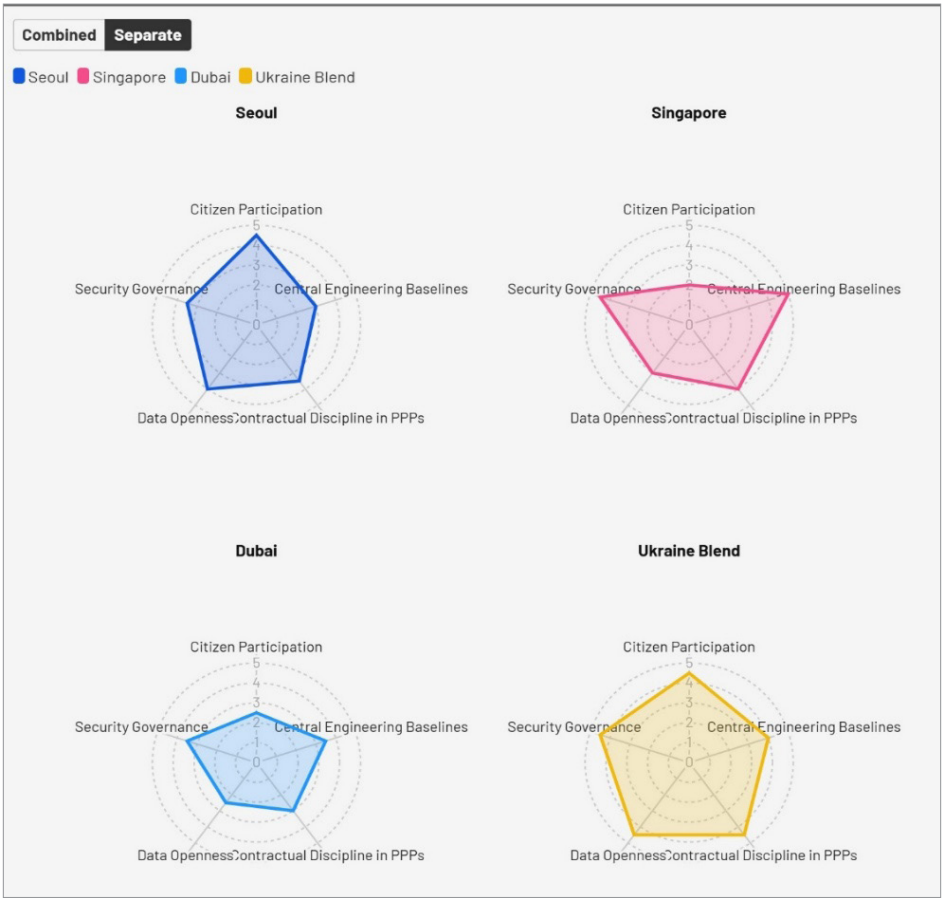
Mosul's recent recovery highlights the role of cultural restoration and community involvement in healing a traumatized society. UNESCO's initiative to 'Revive the Spirit of Mosul' focused on rebuilding iconic landmarks with local artisans, reclaiming cultural identity (UNESCO, 2020). Ukraine can adopt a similar 'smart heritage' approach, using digital tools like 3D scanning and virtual reality to document and reconstruct destroyed cultural sites, and involving local IT specialists and youth in these projects to build skills and a sense of ownership (Clement, Ruysschaert and Crutzen, 2023).

3.5. Synthesizing a 'Ukraine Blend'

Adopting a single global governance model is unsuitable for Ukraine due to its unique context of post-conflict state-building, vibrant civil society, and European integration aspirations. Instead, a tailored governance structure called the 'Ukraine Blend' is needed, which combines strengths from various global approaches.

To operationalize these insights, we constructed comparative governance profiles for each archetype. Scores were assigned through a two-stage process: (1) authors' structured coding of documented governance practices from cited sources using explicit rubrics (e.g., Seoul's mVoting app and Democracy Seoul platform scored high on Participation; Singapore's GovTech-mandated interoperability standards scored high on Central Engineering). The Ukraine Blend profile integrates expert-ranked priorities from Table 3

rather than describing current implementation. Figure 1 visualizes these assessments. We limited the comparison to five vectors for visual clarity because these dimensions emerged as most salient in expert consultations.



Note: Scores reflect documented governance emphases (Seoul, Singapore, Dubai) and recommended priorities (Ukraine Blend) on a 1-5 scale. See text for methodology. This is an analytical framework, not a performance ranking.

Figure 1: Comparative governance vectors and a proposed Ukraine Blend

Source: The authors

Scores assigned to each archetype (Seoul, Singapore, Dubai) along these five vectors are based on a structured qualitative assessment framework detailed in Annex 2. The scoring methodology employed a three-stage process: (1) systematic extraction of documented governance practices from cited primary sources (e.g., official government reports, peer-reviewed case studies); (2) mapping of these practices onto five pre-defined governance dimensions using explicit operational criteria; and (3) independent cross-validation by both authors, with discrepancies resolved through consensus discussion. For instance, Seoul's

high 'Citizen Participation' score (5/5) reflects documented institutionalized mechanisms such as the mVoting app with legally binding outcomes and the Democracy Seoul platform integrated into municipal decision-making processes (Seoul Metropolitan Government, 2025). Singapore's 'Central Engineering Baselines' score (5/5) derives from GovTech's statutory mandate to enforce interoperability standards and manage shared platforms across all public agencies (GovTech Singapore, 2025). The 'Ukraine Blend' profile represents normative recommendations synthesized from expert elicitation findings (Table 3) rather than current implementation status. Full scoring rubrics and source documentation are provided in Annex 2 to ensure methodological transparency and replicability.

4. Data governance and public-private partnerships: a core challenge

Policy stances (definitions used throughout): Open-data-first – default publication of non-personal, non-sensitive municipal data in machine-readable formats with OpenAPI access and clear reuse rights; Civic-data-rights – enforceable rights for residents to access, correct, port, and contest data-driven decisions that materially affect them (GDPR-aligned plus local grievance mechanisms); Proprietary-with-guardrails – allowance for vendor-operated or closed components only where functionally necessary, with municipal ownership of non-personal operational data, interoperability requirements, auditability, and step-in rights.

Data governance is 'at the heart of any future smart city' (Kitchin, 2015). For Ukrainian municipalities, choices about data architecture are not merely technical; they are fundamentally political. These choices will determine who benefits from the digital transformation, how accountability is maintained, and whether citizen rights are protected. We can formalize three stylized models of data governance, each with distinct implications for transparency, accountability, and innovation.

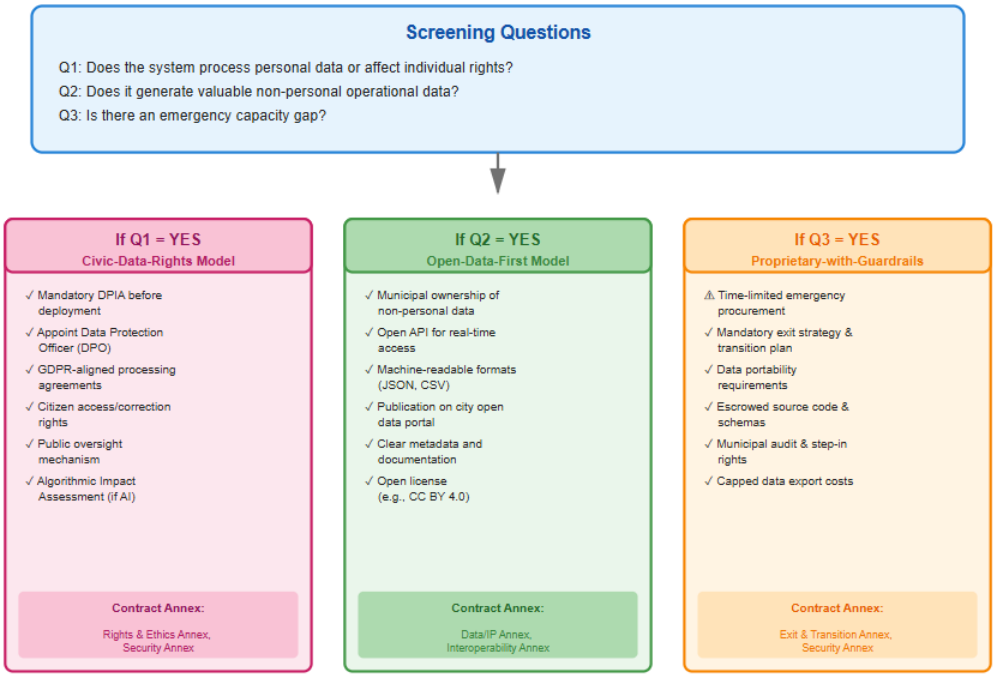
The proprietary platform model centralizes control under a single vendor by bundling devices, connectivity, data storage, analytics, and dashboards into one contract. This model appeals to Ukraine's emergency context due to its speed and reduced coordination needs. However, it poses risks such as a lack of transparency, vendor lock-in, and shifting bargaining power from cities to vendors (Voorwinden, 2021).

Cities' early experiences with proprietary traffic systems indicated that modifications or integrations often required substantial vendor fees. While wartime urgency in Ukraine may necessitate these proprietary solutions for critical services, they should be viewed as temporary measures. Contractual safeguards, including data portability, escrowed source code, and pre-agreed limits on data export costs, prevent vendors from wielding excessive leverage when contracts expire (Lee, Han and Cho, 2025).

The civic-data-rights model expands on open-data-first by providing enforceable rights to individuals and communities, enhancing transparency. It aligns with GDPR, DGA, and AI Act obligations by granting citizens access to personal data, algorithmic explanations,

and participation in data governance through intermediaries (Calzada, 2021). In rebuilding efforts, the smart city concept focuses on resilience and inclusivity, enabling authorities and citizens to co-create urban futures. This approach supports Ukrainian cities in transitioning from crisis to sustainable development (Dunayev, Gavkalova and Kud, 2023). It may involve municipal data trusts for mobility data, co-governed by cities and citizens, fostering legitimacy and public trust in a post-conflict society.

Ukrainian municipalities would benefit from a clear decision-making framework to operationalize these choices. Figure 2 presents a proposed data governance decision flow that city teams can use before any major technology deployment.



Note: Systems may require provisions from multiple models: for example, a smart traffic system triggers both Q1 (personal data) and Q2 (operational data), requiring both Civic-Data-Rights and Open-Data-First contractual annexes.

Figure 2: Data governance decision flow for municipal deployments

Source: The authors

The open-data-first model views non-personal municipal operational data as a public good, with only essential privacy and security exceptions. This approach enhances transparency, reduces vendor information imbalances, and fosters a local innovation ecosystem where third-party developers can create new services (Barns, 2018; OECD, 2021). We operationalise Open-data-first as a contractual default for non-personal operational datasets (see Figure 2 and Section 3.4).

4.1. The PPP dilemma: balancing innovation with public value

Public-private partnerships will be indispensable for financing and implementing Ukraine's smart city reconstruction. The scale of the need for capital and specialized technological expertise far exceeds the current capacity of the Ukrainian public sector. However, as the reviewers rightly suggest, it is crucial to move beyond a simple description of PPPs and reflect on the deep implications of different governance choices. International experience provides a rich, if cautionary, set of lessons on the recurring challenges of PPPs in smart city projects: local context misfit, stakeholder complexity, and the difficulty of building trust. Without robust governance, PPPs can lead to the privatization of public value, the erosion of democratic accountability, and the creation of technologically-driven inequalities.

Public value and accountability erosion are significant risks in public-private partnerships (PPPs). Cities cannot delegate their essential responsibilities to private companies, especially when public functions involve human rights, like CCTV surveillance or social housing algorithms. Such arrangements require adhering to public law norms.

To ensure accountability, contracts could stipulate that private operators comply with GDPR-equivalent rules, publish performance and privacy incident reports, and undergo independent audits by bodies like the Data Protection Authority. Accountability can become blurred without these safeguards, leaving citizens with limited recourse for rights violations.

The challenges and opportunities associated with data governance and PPPs are already manifest in Ukraine. For instance, deploying city-wide video surveillance systems in several Ukrainian cities, often under direct procurement or simplified PPPs, illustrates the dual nature of smart infrastructure. The 'Safe City' program in Kyiv alone has installed over 4,000 CCTV cameras with facial recognition capabilities. However, legal experts have raised concerns about the compliance of such systems with GDPR-level data protection standards (Avdieieva, 2025). While these systems contribute to public safety and law enforcement, particularly during wartime, their data governance frameworks often lack the granularity and transparency required by contemporary privacy regulations.

A pertinent example is the rapid growth of e-governance platforms at the municipal level. Many cities use cloud-based solutions to streamline administrative processes and offer services like online utility payments and permit applications. However, the adherence to data sovereignty, cybersecurity protocols, and interoperability standards varies. Without clear national guidelines, municipalities may inadvertently create data silos, which complicate data exchange and analysis for urban planning. Furthermore, contracts often lack clarity regarding the long-term ownership of anonymized data, potentially ceding valuable public assets to private entities. This situation highlights the potential value of a comprehensive legal framework to guide these initiatives.

A disciplined, proactive approach to contract design is essential to manage these complex risks. For DPIA scope and terminology, see Section 5.1.

Table 2 proposes a detailed risk-allocation matrix for smart city PPPs in Ukraine. This matrix is not merely a checklist but an analytical tool designed to force a clear allocation of responsibilities and to embed mitigation mechanisms directly into legal agreements.

Table 2: Smart city PPP risk-allocation matrix for Ukraine

Risk factor	Primary responsibility	Mitigation mechanisms in contract
Data Ownership & Access (Data collected by the system)	Public (City): Owns non-personal data; acts as controller for personal data.	Data/IP Annex: Explicitly declares all non-personal data a public asset. It mandates real-time city access via open APIs and requires the publication of key datasets on the city's open data portal. Specifies that the private partner is a 'processor' under GDPR terms, with strict limitations on data use.
Vendor Lock-In (Difficulty switching providers)	Public (City): Ensures long-term market contestability.	Interoperability Annex: Requires using specified open standards (e.g., OGC for geospatial data, TALQ for smart lighting). The vendor must provide the city with full system documentation and data schemas. Exit & Transition Plan: Obligates the vendor to support a smooth transition to a new provider for a defined period at a capped cost.
Cybersecurity & System Integrity	Shared: Private partner implements security; public partner oversees and validates.	Security Annex: Mandates compliance with NIS2-aligned standards (e.g., encryption, incident response). The private operator must report significant incidents within a specified timeframe (e.g., 24 hours) to the city and the national CERT. The city reserves the right to conduct independent penetration tests and security audits.
Privacy & Human Rights Compliance	Public (City): Ultimate guarantor of rights. Private (Partner): Operational compliance.	Rights & Ethics Annex: Requires a mandatory, pre-deployment DPIA and, for AI systems, an Algorithmic Impact Assessment. Establishes a public oversight mechanism, such as a city data ethics committee. The city can suspend the contract for serious or persistent rights violations.
Financial & Performance Risk (Cost overruns, service quality)	Private (Partner): Bears commercial and operational risks.	Performance & SLA Annex: Defines clear Key Performance Indicators (KPIs) with financial penalties for non-compliance. Fixed-price or capped-cost models for deployment place the risk of cost overruns on the private partner. The city retains 'step-in' rights to take over operations in case of critical failure.

Source: Authors' design, adapted from global PPP guidelines (World Bank, 2020) and expert elicitation findings

This matrix adopts the 'Dubai-with-guardrails' approach, allowing Ukraine to utilize private sector efficiency while protecting key public interests. By establishing non-negotiable contractual mechanisms for high-value procurements, municipalities can shift power dynamics to ensure partnerships benefit the public good rather than just vendor profits. This structured approach attracts reputable international firms who prefer clear legal frameworks and predictable rules. Evidence from expert consultations indicates that standardized contracts would boost investor confidence and enhance the resilience of Ukraine's urban infrastructure.

5. Citizen-centric governance: from theory to practice

Rebuilding trust in government is as vital as rebuilding physical infrastructure in post-war Ukraine. This imperative shifts the focus from purely technological solutions to the institutional design of participation, inclusion, and rights protection. While the previous sections established the legal and strategic frameworks, this section grounds the analysis in the current realities of the Ukrainian public administration. To move from theory to practice, we conducted a rapid expert elicitation with senior officials directly involved in Ukraine's digital reconstruction efforts. This empirical component provides a crucial 'reality check', revealing key practitioners' consensus, concerns, and priorities. The findings not only validate the analytical framework of this paper but also offer a nuanced roadmap for implementing citizen-centric governance on the ground.

5.1. Methodology of the expert elicitation

To capture informed judgment, we conducted a two-round rapid expert elicitation from August to September 2025, using a mini-Delphi technique to synthesize expert opinions and identify consensus. The panel included ten anonymized senior civil-service experts from key Ukrainian institutions: the Ministry of Digital Transformation, the Ministry of Economy, and the Government Office for European and Euro-Atlantic Integration. Participants had active roles in municipal digitalization, urban PPPs, data protection, or EU acquis alignment, ensuring deep practical knowledge of the subjects.

The elicitation was conducted online to accommodate senior officials' schedules. In the first round, participants completed a 16-question guide covering four themes: governance, PPP and procurement, data governance, and citizen participation. The instrument included seven-point Likert items, forced-ranking tasks, and open-ended questions. Plain-language definitions were provided for technical terms like DPIA and civic-data-rights. Participants reviewed anonymized medians and rationales from the first and second rounds and could revise their judgments. This encouraged reflection and consensus-building. A 71.4% completion rate and detailed qualitative feedback highlighted participant engagement. All participation was voluntary, based on informed consent, and conducted anonymously to ensure candor, reflecting informed professional judgment rather than official positions.

Experts were purposively sampled based on (i) ≥5 years of domain experience (municipal digital policy, data protection, PPPs), (ii) prior authorship of peer-reviewed or official guidance, and (iii) absence of direct vendor contracting on the evaluated projects. Consensus rule: items with IQR ≤ 1 were considered consensus; stability was confirmed if the median shift between rounds was ≤ 1 Likert point.

5.2. Expert findings: a mandate for structured, rights-based governance

The expert elicitation revealed a striking consensus across ministries on the core principles guiding Ukraine's smart city reconstruction. The findings strongly support the central hypotheses of this paper, highlighting an urgent demand from within the government for a

structured, EU-aligned framework that empowers local innovation within clear, rights-respecting guardrails.

There was unanimous agreement on the necessity of a foundational legal framework. The proposition that 'Ukraine needs a principle-based Smart City Act before large-scale deployments' moved from a Round 1 median score of 6 (on a 7-point scale) to a clear consensus at 7 in Round 2 (IQR = 0). The urgency ranking of legal levers also stabilized with high consensus (Kendall's $W = 0.74$, $p < 0.01$), prioritizing the Smart City Act first, followed by refinements to PPP and concession laws. As one expert from the Ministry of Digital Transformation (E3) articulated, 'The Act sets mandates and interoperability guardrails – without it we risk fast but fragmented deployments'. This was echoed by a respondent from the EU integration office (E9), who noted, 'Front-loading a framework law eases EU acquis alignment and reduces donor transaction costs'. Based on expert consensus, we propose drafting and adopting a comprehensive Smart City Act as a foundational legislative piece, ensuring it integrates EU digital acquis principles from its inception.

Data protection and privacy are crucial for building public trust. Experts recommend mandatory Data Protection Impact Assessments (DPIAs) and oversight by Data Protection Officers (DPOs) for municipal systems processing personal data, achieving a median consensus score of 7. For non-personal urban data in public-private partnerships (PPPs), there is strong support for an 'open by default' policy (Kendall's $W = 0.79$, $p < 0.01$). An expert (E1) noted, 'Open when non-personal; controlled when risk is higher – always with a DPIA and a public decision trail'. The evidence supports requiring DPIAs for personal data and adopting 'open by default' principles for non-personal data to enhance transparency.

For PPPs, experts suggested a 'Dubai-with-guardrails' model, prioritizing open standards and interoperability to avoid vendor lock-in (Kendall's $W = 0.68$, $p < 0.01$). An expert (E7) warned against lock-in, stating that 'escrow interfaces, open APIs, and step-in rights are essential'. Our analysis suggests developing standardized PPP contracts that mandate open standards, interoperability, municipal ownership of non-personal data, and clear exit strategies to ensure public benefit.

Citizen participation and inclusion are vital for the legitimacy and sustainability of reconstruction efforts. While there was lower consensus on specific mechanisms (Kendall's $W = 0.56$, $p < 0.01$), a strong demand emerged for a 'National Inclusion Package', rated with a median score of 7. This package should include digital literacy programs, accessible interfaces for all demographics, and formal public feedback channels. An expert from the Government Office for European and Euro-Atlantic Integration (E5) stated, 'Inclusion is essential for democratic stability and EU accession. Our smart cities must reflect this'. Drawing on expert consensus, we propose creating a 'National Digital Inclusion Package' that includes digital literacy initiatives, accessible design standards for smart city applications, and mechanisms for diverse citizen participation in planning and oversight. Table 3 summarizes the key quantitative findings from the expert elicitation.

Table 3: Key findings from the expert elicitation on smart city governance

Governance Lever	Round 1 Median (IQR)	Round 2 Median (IQR)	Round 2 Consensus (Kendall's W)
A. Legal Readiness			
Need for a Smart City Act	6 (1)	7 (0)	0.74
B. PPP Safeguards			
Mandate Open Standards in Contracts	6 (1)	7 (1)	0.68
C. Data Governance			
Mandatory DPIAs for Personal Data	6 (1)	7 (1)	N/A
'Open by Default' for Non-Personal Data	N/A	N/A	0.79
D. Citizen Inclusion			
Need for a National Inclusion Package	6 (1)	7 (1)	0.56

Note: Likert items are scored on a 1–7 scale, where seven is 'strongly agree'. A higher Kendall's W indicates stronger consensus on rankings.

Source: The authors

Beyond governance structures, citizen acceptance requires demonstrable benefits. International research emphasizes that smart city success depends not only on material improvements (service efficiency, cost savings) but also on citizens' 'sense of gain' – feelings of fairness, inclusion, and empowerment. For Ukraine, procurement decisions must balance rapid deployment with visible community benefits and transparent accountability mechanisms. The quantitative results of the expert elicitation are visualized in Figure 3.

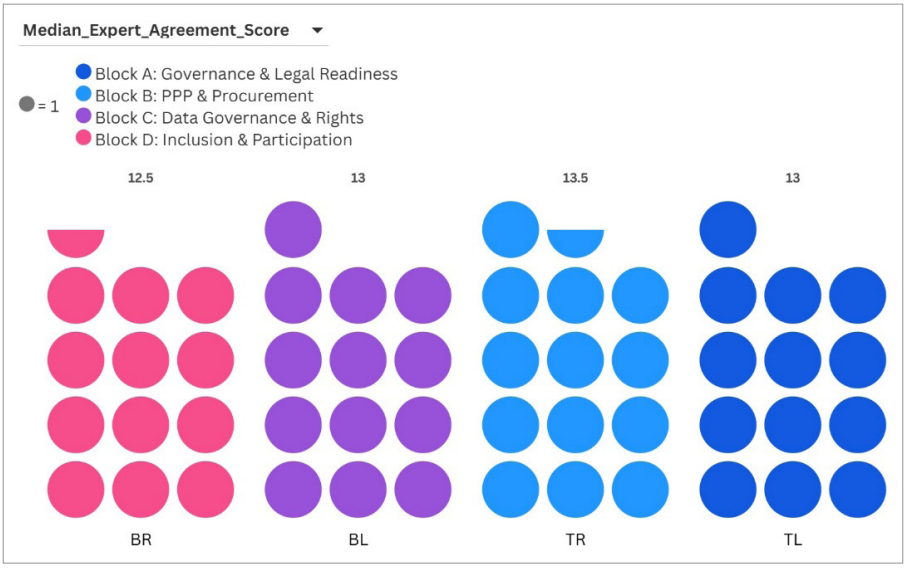


Figure 3: Expert consensus on key governance priorities

Source: The authors

Expert findings highlight the need for concrete actions to build citizen-centric smart cities that protect human rights in the digital realm. This involves integrating a rights-based approach throughout the technology lifecycle, from planning to oversight. Municipalities should conduct mandatory Human Rights Impact Assessments (HRIAs) alongside Data Protection Impact Assessments (DPIAs) for technologies that could impact privacy, freedom of expression, or non-discrimination, such as facial recognition and predictive policing systems.

6. Discussion and conclusion: navigating the trade-offs of smart reconstruction

Ukraine's urban reconstruction presents both a governance challenge and an opportunity to embed resilient, democratic principles into digital infrastructure. This analysis reveals four critical trade-offs requiring principled navigation while providing empirical validation for the study's core hypotheses.

Validation of research hypotheses. The findings provide strong support for both research hypotheses. Regarding H1, expert elicitation demonstrates overwhelming consensus (Round 2 median = 7, IQR = 0) that Ukraine needs a comprehensive Smart City Act before large-scale deployments. The current fragmented legal landscape – characterized by outdated data protection laws (2010), absence of AI/IoT liability frameworks, and overlapping municipal mandates – undermines interoperability and citizen trust, validating the hypothesis. Without a principle-based framework aligned with EU digital acquis (GDPR, NIS2, DGA, AI Act), Ukraine risks perpetuating ad-hoc initiatives with limited scalability and significant vendor lock-in. Regarding H2, the PPP risk-allocation matrix (Table 2) and expert consensus on contractual safeguards confirm that poorly governed partnerships erode public value through vendor lock-in, data ownership ambiguities, and accountability gaps. However, the 'Dubai-with-guardrails' model – emphasizing mandatory interoperability (Kendall's $W = 0.68$, $p < 0.01$), open-by-default non-personal data (Kendall's $W = 0.79$, $p < 0.01$), and municipal ownership – demonstrates that well-structured PPPs can accelerate reconstruction without compromising citizen rights. This validates H2: legal safeguards on data ownership, transparency, and accountability are essential preconditions for ethical smart city development.

Core trade-offs. Centralization vs. autonomy: A hybrid approach based on EU subsidiarity – central standards (Smart City Act, 'GovTech-lite' agency), enabling local innovation – resolves this tension. Speed vs. deliberation: Phased implementation allows rapid infrastructure restoration parallel to deliberate governance development, preventing lock-in while addressing urgent needs. Innovation vs. regulation: Outcome-focused GDPR/NIS2-aligned rules with regulatory sandboxes enable innovation within rights-respecting boundaries. Security vs. openness: Risk-based governance reconciles these: strict controls for sensitive systems coexist with open-by-default non-personal data publication.

Limitations. This study's constraints include: expert elicitation (n = 10) providing informed judgment rather than representative data; comparative analysis relying on secondary sources, limiting granularity; assumptions about continued EU integration; potential for technology evolution to outpace proposed mechanisms; dependence on political will and resources beyond analytical scope; and scoring methodology representing evaluative assessments rather than empirical measurements. Future research should pursue longitudinal pilot tracking, citizen surveys, cost-benefit analysis, comparative post-conflict studies, and technical feasibility assessments.

Roadmap. We propose a sequenced implementation: 0–12 months – enact the Smart City Act, establish the National Coordination Council, issue mandatory procurement guidance; 12–24 months – create the GovTech-lite centre, launch 2–3 city pilots; 24–36 months – refine legislation, amend PPP laws, invest in capacity-building and digital literacy. The sustainable path combines enforceable Civic-data-rights, Open-data-first defaults, and Proprietary-with-guardrails discipline. This framework attracts investment through clear rules, protects citizens by embedding rights from inception, and sustains innovation by preventing vendor lock-in. Ukraine's reconstruction will define whether smart cities serve democratic values or undermine them. The choice is not speed versus safeguards – it is building enduring systems or replicating failures requiring costly future dismantlement.

Statements and declarations. The authors declare the absence of any conflict of interest in this study.

Acknowledgements. The authors thank the anonymous senior civil-service experts who generously contributed their time and insights to this research.

Data availability statement. The detailed methodological protocol, the complete questionnaire for the expert elicitation (including definitions provided to participants), and the scoring rubrics for the comparative governance analysis (Figure 1) are available as supplementary materials in two annexes, archived on Zenodo at https://doi.org/10.5281/zenodo.17249168.

References:

1. Avdieieva, T., 'Cameras with Facial Recognition on City Streets: Is It Legal?', Centre for Democracy and Rule of Law, 2025, [Online] available at https://cedem.org.ua/en/analytics/cameras-facial-recognition/, accessed on September 29, 2025.
2. Barns, S., 'Smart Cities and Urban Data Platforms: Designing Interfaces for Public Life', 2018, *City, Culture and Society*, vol. 12, pp. 5–12, DOI: 10.1016/j.ccs.2017.09.006.
3. Cabinet of Ministers of Ukraine, 'Concept for the Development of the Digital Economy and Society of Ukraine for 2018-2020', Order No. 67-r of January 17, 2018, [Online] available at https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text, accessed on September 29, 2025.

4. Calzada, I., *Smart City Citizenship*, Cambridge, Massachusetts: Elsevier Science Publishing, 2021.
5. Cardullo, P. and Kitchin, R., 'Being a Citizen in the Smart City: Up and Down the Scaffold of Smart Citizen Participation in Dublin, Ireland', 2019, *GeoJournal*, vol. 84, pp. 1–13, DOI: 10.1007/s10708-018-9845-8.
6. Clement, J., Ruysschaert, B. and Crutzen, N., 'Smart City Strategies – A Driver for the Localization of the Sustainable Development Goals?', 2023, *Ecological Economics*, vol. 213, pp. 1–17, DOI: 10.1016/j.ecolecon.2023.107941.
7. Cowley, R., Joss, S. and Dayot, Y., 'The Smart City and Its Publics: Insights from Across Six UK Cities', 2018, *Urban Research & Practice*, vol. 11, no. 1, pp. 53–77, DOI: 10.1080/17535069.2017.1293150.
8. Dunayev, I., Gavkalova, N. and Kud, A., 'Designing a Platform-Based Model of Civic Participation within the Smart-City Concept for Post-War Ukrainian Cities', 2023, *Eastern-European Journal of Enterprise Technologies*, vol. 4, no. 13(124), pp. 46–56, DOI: 10.15587/1729-4061.2023.285448.
9. European Parliament and Council, *Directive (EU) 2019/1024 on Open data and the re-use of public sector information*, 2019, Official Journal of the European Union, [Online] available at https://eur-lex.europa.eu/eli/dir/2019/1024/oj/eng, accessed on September 29, 2025.
10. European Parliament and Council, *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*, 2022a, Official Journal of the European Union, [Online] available at https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng, accessed on September 29, 2025.
11. European Parliament and Council, *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, 2016, Official Journal of the European Union, [Online] available at https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng, accessed on September 29, 2025.
12. European Parliament and Council, *Regulation (EU) 2022/868 on European data governance (Data Governance Act)*, 2022b, Official Journal of the European Union, [Online] available at https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng, accessed on September 29, 2025.
13. European Parliament and Council, *Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, 2024, Official Journal of the European Union, [Online] available at http://data.europa.eu/eli/reg/2024/1689/oj, accessed on September 29, 2025.
14. Government of Dubai, Law no. (22) of 2015 Concerning the Regulation of Partnerships Between the Public and Private Sectors in the Emirate of Dubai, 2015.
15. GovTech Singapore, 'Singapore Smart Nation', 2025, [Online] available at https://www.smartnation.gov.sg/, accessed on September 29, 2025.
16. Greenfield, A., *Radical Technologies: The Design of Everyday Life*, London: Verso, 2018.
17. Isin, E. and Ruppert, E., *Being Digital Citizens*, London: Rowman & Littlefield International, 2015.
18. Kitchin, R., 'Making Sense of Smart Cities: Addressing Present Shortcomings', 2015, *Cambridge Journal of Regions, Economy and Society*, vol. 8, no. 1, pp. 131–136, DOI: 10.1093/cjres/rsu027.

19. Kuzior, A., Pidorycheva, I., Liashenko, V., Shevtsova, H. and Shvets, N., 'Assessment of National Innovation Ecosystems of the EU Countries and Ukraine in the Interests of their Sustainable Development', 2022, *Sustainability*, vol. 14, no. 14, pp. 1–22, DOI: 10.3390/su14148487.
20. Law of Ukraine 'On Personal Data Protection' no. 2297-VI of 1 June 2010, Verkhovna Rada of Ukraine, [Online] available at https://natlex.ilo.org/dyn/natlex2/r/natlex/fe/details?p3_isn=87898, accessed on September 29, 2025.
21. Law of Ukraine 'On the Basic Principles of Ensuring Cybersecurity of Ukraine' no. 2163-VIII of 5 October 2017, Verkhovna Rada of Ukraine, [Online] available at https://zakon.rada.gov.ua/laws/show/2163-19#Text, accessed on September 29, 2025.
22. Lee, Y., Han, S. and Cho, Y., 'Navigating the Path to Smart and Sustainable Cities: Insights from South Korea's National Strategic Smart City Program', 2025, *Land*, vol. 14, no. 5, pp. 1–23, DOI: 10.3390/land14050928.
23. March, H. and Ribera-Fumaz, R., 'Barcelona: From Corporate Smart City to Technological Sovereignty', 2018, in Karvonen, A., Cugurullo, F. and Caprotti, F. (eds.), *Inside Smart Cities: Place, Politics and Urban Innovation*, London: Routledge, pp. 227–242.
24. Marot, B., *Developing Post-War Beirut (1990–2016): The Political Economy of 'Pegged Urbanization'*, Geography, McGill University, 2018.
25. Meijer, A. and Bolívar, M.P.R., 'Governing the Smart City: A Review of the Literature on Smart Urban Governance', 2016, *International Review of Administrative Sciences*, vol. 82, no. 2, pp. 392–408, DOI: 10.1177/0020852314564308.
26. Ministry of Digital Transformation of Ukraine, 'Diia Platform', [Online] available at https://diia.gov.ua, accessed on September 29, 2025.
27. Municipality of Sarajevo, 'Official Website', [Online] available at https://www.sarajevo.ba, accessed on September 29, 2025.
28. Nam, T. and Pardo, T.A., 'Conceptualizing Smart City with Dimensions of Technology, People, and Institutions', Proceedings of the 12th Annual International Conference on Digital Government Research, New York: ACM, 2011, pp. 282–291, DOI: 10.1145/2037556.2037602.
29. OECD, 'Measuring Smart City Performance in COVID-19 Times: Lessons from Korea and OECD Countries', 2021, Proceedings from the 2nd OECD Roundtable on Smart Cities and Inclusive Growth, [Online] available at https://www.oecd.org/en/publications/measuring-smart-city-performance-in-covid-19-times-lessons-from-korea-and-oecd-countries_72a4e7db-en.html, accessed on September 29, 2025.
30. Oliukha, V.H., 'Legal Basis for the Implementation of the Smart City Concept in Ukraine', 2024, *Analytical and Comparative Jurisprudence*, vol. 6, pp. 339–344, DOI: 10.24144/2788-6018.2024.06.55.
31. Seoul Metropolitan Government, 'Official Website of the Seoul Metropolitan Government', [Online] available at https://english.seoul.go.kr, accessed on September 29, 2025.
32. UN-Habitat, 'Centering People in Smart Cities: A Playbook for Local and Regional Governments', 2021, United Nations Human Settlements Programme, [Online] available at https://unhabitat.org/sites/default/files/2021/11/centering_people_in_smart_cities.pdf, accessed on September 29, 2025.
33. UN-Habitat, 'International Guidelines on People-Centred Smart Cities', UN-Habitat, 2025, [Online] available at https://unhabitat.org/international-guidelines-on-people-centred-smart-cities, accessed on September 29, 2025.

34. UNESCO, 'Revive the Spirit of Mosul', 2020, Paris: United Nations Educational, Scientific and Cultural Organization, [Online] available at https://www.unesco.org/en/revive-mosul, accessed on September 29, 2025.
35. Verkhovna Rada of Ukraine, Law Draft 'On Personal Data Protection' no. 8153 (registered 25 October 2022), [Online] available at https://itd.rada.gov.ua/billinfo/Bills/Card/40707, accessed on September 30, 2025.
36. Verkhovna Rada of Ukraine, Resolution no. 4065-IX of 20 November 2024 'On Adopting as A Basis the Draft Law of Ukraine 'On Personal Data Protection' (reg. no. 8153)', [Online] available at https://zakon.rada.gov.ua/go/4065-IX, accessed on September 30, 2025.
37. Voorwinden, A., 'The Privatised City: Technology and Public-Private Partnerships in the Smart City', 2021, *Law, Innovation and Technology*, vol. 13, no. 2, pp. 439–463, DOI: 10.1080/17579961.2021.1977213.
38. Wernick, A. and Artyushina, A., 'Future-Proofing the City: A Human Rights-Based Approach to Governing Smart City Technologies', 2023, *Internet Policy Review*, vol. 12, no. 1, pp. 1–23, DOI: 10.14763/2023.1.1695.
39. World Bank, *Public-Private Partnership Legal Resource Center*, Washington, D.C., 2020, [Online] available at https://ppp.worldbank.org/, accessed on September 29, 2025.