# SMART CITIES PROJECT AND ITS EVALUATION IN THE CONTEXT OF LEGAL REGULATION OF CYBERSECURITY

**Kamran Khalilov***

**Abstract**

*The expanding integration of digital technologies into the physical and administrative layers of modern cities has brought the smart city model to the forefront of urban development strategies. These environments rely on sensor-based infrastructures, interconnected operational systems, and continuous data circulation, forming complex digital ecosystems that reshape how public services function and how urban resources are managed. Yet the same technological density that enables efficiency also amplifies exposure to security breaches, intrusive data practices, and governance uncertainties. This study explores the legal dimensions of safeguarding these digitally dependent urban systems, with particular attention to how cybersecurity requirements intersect with data protection, infrastructural reliability, and the rights of city residents. Drawing on international regulatory experience, especially European approaches that integrate cybersecurity obligations with structured data protection rules, the article evaluates the capacity of Azerbaijan's existing legal instruments to respond to the risks associated with smart city development. A comparative legal assessment reveals several gaps in national legislation, including fragmented responsibilities, limited procedural safeguards, and the absence of tailored norms for high-interconnectivity urban systems. Although Azerbaijan has established a baseline framework for information security and personal data handling, the operational complexity of smart infrastructures requires more adaptive, technically grounded, and enforceable regulatory measures. The article concludes by outlining direction-specific recommendations intended to strengthen legal resilience, refine cybersecurity governance, and support the secure and accountable development of smart city initiatives.*

**Keywords**: *smart cities, cybersecurity governance, regulatory analysis, data protection, digital urban systems, Azerbaijan.*

## *I. Introduction*

The rapid pace of urbanization, coupled with the growing complexity of metropolitan infrastructures and the widespread integration of digital technologies into everyday life, has transformed the "smart city" concept from a theoretical model into a practical urban development paradigm. Smart cities rely on the deployment of information and communication technologies (ICT), sensor networks, big data analytics, and artificial intelligence to optimize the functioning of transportation systems, public utilities, energy distribution, municipal governance, and a wide range of public services. This technologically enhanced model, however, inherently requires the continuous collection, processing, and interconnection of large volumes of data, thereby introducing substantial legal, ethical, and cybersecurity challenges [16].

The increasing digitalization of urban environments heightens the vulnerability of smart city ecosystems to cybersecurity incidents, unauthorized data access, system manipulation, and privacy violations. As international research demonstrates, highly interconnected infrastructures, particularly those involving real-time monitoring, integrated control systems, and automated decision-making processes can expand attack

* PhD Candidate in Law, Criminal Procedure Department of the Faculty of Law, Baku State University, email: kamran.khalilov.isa@bsu.edu.az

surfaces and expose residents to new forms of risk. Consequently, the development and operation of smart cities must be supported by robust legal frameworks that establish clear standards for data governance, cybersecurity safeguards, accountability mechanisms, and the protection of individual rights.

In Azerbaijan, the introduction of smart city and smart village policies has been formalized through governmental directives, reflecting the country's broader agenda of digital transformation and sustainable urban development. These initiatives aim to incorporate advanced technologies into public administration and urban infrastructure, yet their effectiveness largely depends on the adequacy of existing legal and regulatory structures concerning cybersecurity and data protection. Although national legislation establishes a foundational framework for information security and personal data governance, questions remain regarding its capacity to address the complex risk landscape associated with smart city environments, particularly in the context of large-scale sensorization, algorithmic decision-making, and cross-system interoperability.

Given these dynamics, this article aims to examine the regulatory dimensions of smart city development through the lens of cybersecurity and data protection. By analyzing international norms with particular emphasis on European Union regulatory approaches alongside Azerbaijan's national legislation and strategic policies, the study evaluates existing frameworks, identifies structural gaps, and explores opportunities for harmonization. The article proceeds by outlining the conceptual and technological underpinnings of smart cities, examining their threat landscape, assessing the legal safeguards required for secure and rights-respecting implementation, and offering a comparative review of international and domestic regulatory models. This analytical framework contributes to a more comprehensive understanding of how smart city initiatives can be implemented in a manner that is technologically efficient, legally coherent, and aligned with fundamental principles of security, transparency, and human rights [4].

The study is based on a combination of primary legal texts and secondary academic literature to analyze the legal and regulatory dimensions of smart city cybersecurity and data protection. Primary materials include Azerbaijan's national legislation, such as the Law on Personal Data (2010) [18], the Strategy of the Republic of Azerbaijan on Information Security and Cybersecurity for 2023–2027, [26] and related national standards governing digital infrastructure and ICT security. European Union legal frameworks were also considered, including the General Data Protection Regulation (GDPR, 2016/679) [10], the NIS2 Directive (2022/2555) [11] on the security of network and information systems, and the EU Cybersecurity Act (2019/881) [12]. In addition to legal texts, academic publications and institutional reports providing insights into smart city technologies, cybersecurity, and comparative legal frameworks were utilized. This combination ensures that both technological and legal dimensions of smart cities are considered in a comprehensive manner.

The methodology relies on comparative legal analysis, focusing on identifying and evaluating how existing laws address the challenges posed by smart city ecosystems. Legal provisions from Azerbaijan and the European Union were reviewed to assess the coverage of cybersecurity governance, data protection obligations, institutional responsibilities, and enforcement mechanisms. Each provision was coded according to its scope, level of obligation, mechanisms for compliance, and alignment with technological requirements. The study also developed a framework for comparison that

examines the adequacy of national legislation relative to international standards, highlighting gaps in accountability, risk management, and operational applicability.

The collected information was synthesized using both tabular and thematic approaches. Tabular analysis allowed for direct comparisons of specific legal provisions, while thematic synthesis helped identify broader patterns, structural gaps, and potential areas for reform [13]. This approach made it possible to evaluate not only whether Azerbaijani legislation addresses cybersecurity and data protection concerns, but also how it aligns with EU best practices, particularly regarding citizen rights, infrastructure security, and institutional coordination. By combining qualitative assessments of legal content with quantitative consideration of the comprehensiveness of regulations, the study produced evidence-based insights applicable to policymakers, urban planners, and cybersecurity professionals.

Overall, this approach provides a structured yet flexible methodology that bridges technology, law, and governance. It enables a clear understanding of how smart city initiatives can be supported by adaptive and enforceable legal frameworks capable of addressing the complexity of highly interconnected urban systems while ensuring compliance with both national requirements and international standards.

*II. Understanding smart cities as a reality of the modern digital world.*

A smart city is an urban development model in which information and communication technologies (ICT), sensor systems, analytical platforms, and digital decision-making tools are employed to optimize city management and service delivery. In this model, urban infrastructure elements operate in a coordinated manner, utilizing real-time data to improve efficiency, transparency, and accountability in governance. The core objective of smart cities is to enhance public services, increase resource efficiency, boost social welfare, and support sustainable urban growth [13].

Smart cities are complex socio-technical systems that integrate technological, social, and institutional dimensions. They are not merely collections of advanced technologies, but also ecosystems that facilitate data-driven governance, citizen participation, and inter-agency collaboration [15]. This comprehensive approach distinguishes smart cities from traditional urban frameworks and highlights the critical interplay between technology, policy, and human factors. The essence of smart cities lies in their capacity to provide coordinated and adaptive services based on large-scale data collection and analysis [7]. Integrated infrastructures enable predictive planning and real-time adjustments across sectors such as transportation, energy, public utilities, and emergency management. For instance, intelligent traffic management can optimize signal timings based on congestion patterns, energy grids can dynamically balance supply and demand, and public safety responses can be adjusted using real-time information.

Furthermore, smart city initiatives aim to enhance social engagement by enabling citizens to participate in decision-making through digital platforms and improving access to e-government services. Therefore, the essence of smart cities encompasses technological innovation, social dynamics, and institutional governance [3].

Smart cities represent an extensive framework that brings together multiple structural and functional components. According to a report issued by the European Parliament, and based on Cohen's conceptualisation, smart cities encompass six principal dimensions. These include smart people, smart governance, smart economy, smart mobility, smart environment, and smart living [6, pp. 131-132]. Within this framework,

smart living particularly emphasizes an urban setting in which residents can maintain their daily lives with no anxiety regarding personal security. Ensuring that individuals can move freely at any hour without fear for their safety, and that they can communicate effortlessly with others, stands as an essential requirement—and indeed a necessity—for a smart-living model free from security concerns [14, pp. 126].

For such an environment to emerge, smart security systems must deliver services that protect residents from adverse environmental conditions, accidents, and crime. These systems include technological infrastructures that secure urban spaces and roadways, rely on data analytics to identify individuals who threaten public safety through biometric technologies, reduce operational errors of security units, and provide large-scale warning mechanisms capable of disseminating alerts during potential natural disasters. Central to smart security is the capacity to anticipate potential security problems before they occur, enabling authorities to take pre-emptive measures based on proactive assessments. When incidents do occur, smart systems should ensure rapid information flows, enabling timely interventions. Equally important is enhancing the responsiveness of emergency-management systems and shortening reaction times through optimization techniques [21, p. 117]. Beyond crime prevention, smart security also entails the establishment of early-warning systems rooted in environmental monitoring, the protection of residents from crime and accidents, and the preservation of food and product safety, all of which contribute to healthier living conditions [4, p. 60].

Within smart cities, the creation of integrated governance models which supported by camera networks and digital urban security systems—aims to ensure efficient management of resources, risk, and operational processes under the supervision of law-enforcement bodies. Smart systems are expected to identify incidents, protect the security of collected data, archive high-volume audiovisual materials, and maintain an open architecture capable of future upgrades. Smart-security technologies include burglary-prevention mechanisms, alarm and access-control systems, advanced surveillance devices, fire-monitoring and response systems, disaster-tracking and warning technologies, suspicious-individual detection, under-vehicle scanning tools, dynamic video-search systems, crowd-density analysis, license-plate recognition, and biometric-based suspect identification, among other integrated applications [22, pp. 4-5].

The widespread adoption of such systems in smart cities aims to reduce crime rates by ensuring robust monitoring and identification capabilities. Biometric identification through smart-camera networks and license-plate recognition systems facilitates the prevention of criminal incidents. Placing biometric identification cameras at city entrances, major squares, and strategic intersections supports timely apprehension and transfer of offenders to judicial authorities [23]. Advanced urban-monitoring systems, real-time data-processing infrastructures, and persistent environmental sensors constitute essential elements for maintaining the livability of cities and ensuring the continued functioning of other smart-city technologies. Smart security technologies in this context may include: 1) Urban security systems capable of integrating environmental monitoring, road-safety functions, and product-safety mechanisms; 2) An integrated platform combining cloud-based large-scale data storage, retrieval architectures, intelligent video analytics, biometric systems, and advanced data-processing tools; 3) Enhanced bandwidth capacity to support diverse security applications and ensure seamless operation of smart systems, providing security personnel with reliable, science-

based decision-support mechanisms that minimize operational errors and guarantee effective functioning of the overall security architecture [1, pp. 17-18].

A secure smart-city environment depends on strong coordination among all urban stakeholders. The mere installation of digital and communication infrastructures does not suffice; without the integration of human, technological, and institutional components, the smart-security model remains incomplete. Therefore, residents, public institutions, civil-society organizations, businesses, and private security providers must cooperate within a shared governance mechanism. Smart-security mechanisms should be supported through highly sensitive systems, including mobile devices and complementary communication tools that enable continuous connectivity with central command units. Ensuring uninterrupted access to these centers in all conditions fosters residents' confidence in the system and strengthens public trust. As cities evolve into smart urban environments, smart-security technologies assume a critical role in safeguarding environmental sustainability, supporting disaster resilience, preventing human-induced disruptions, and reinforcing economic viability for future generations [19, pp. 102-103].

In summary, the categorization of smart cities highlights the multidimensional nature of urban digital transformation. Functional focus determines sector-specific objectives and investment priorities, technological maturity reflects system integration and automation capacity, and strategic alignment ensures that legal and institutional frameworks support secure, efficient, and citizen-centric urban development. Recognizing these dimensions is essential for developing robust legal and cybersecurity frameworks that accommodate the evolving complexity of smart city ecosystems.

*III. Assessment of smart cities in the context of the cybersecurity concept.*

The integration of advanced technologies into urban ecosystems has elevated cybersecurity to a core pillar of contemporary urban safety. Within this framework, the smart security paradigm necessarily incorporates cybersecurity, as the uninterrupted delivery of urban services and the protection of personal data depend on resilient and secure digital infrastructures. In smart cities, virtually all data flows, operational processes, and administrative functions are mediated through cyber-systems. Consequently, as cities increasingly adopt smart technologies, concerns related to security vulnerabilities have intensified [8, p. 492].

Cybersecurity constitutes a critical challenge due to the growing potential for cyber-attacks targeting essential sectors of smart cities. Importantly, cybersecurity encompasses not only deliberate threats such as industrial espionage and cyberterrorism, but also unintended disruptions resulting from user errors, equipment malfunctions, and natural disasters. Even a single vulnerability may enable an attacker to infiltrate a network, gain access to control software, or alter system configurations in ways that destabilize critical infrastructures [24].

Ensuring the protection of personal data in smart cities cannot be achieved solely through stringent preventive measures. Although technical safeguards are indispensable, long-term system security ultimately depends on continuous testing and proactive vulnerability assessment. Cybersecurity specialists must therefore approach the system from the viewpoint of a potential adversary, systematically evaluating weak points in order to anticipate and prevent cybersecurity breaches. Intelligent firewalls and security software capable of detecting digital footprints constitute essential components of this infrastructure. While professional expertise is necessary for establishing initial

cybersecurity systems, municipalities must also cultivate in-house information security specialists to ensure sustainable protection [17].

The growing demand for digital services has prompted city administrations to provide free public Wi-Fi access; however, unsecured public networks pose significant threats to data privacy. Evaluating smart-city cybersecurity exclusively through the lens of internet access would be incomplete, as smart technologies permeate diverse aspects of daily life. Nevertheless, free and uncontrolled Wi-Fi remains a major vulnerability: lack of authentication impedes the identification of perpetrators in cyber-related incidents. Introducing minimal fees or requiring identity verification and password authentication may mitigate risks and enhance traceability. Such mechanisms could also offset some of the financial burden of providing public connectivity [20].

To safeguard smart cities against emerging threats, cybersecurity systems must be developed within a structured and comprehensive framework. Key considerations in the planning phase include the following:

A. Privacy, secure and resilient network connectivity:

If citizens perceive that smart technologies do not adequately protect their personal information, they are likely to avoid using them. Therefore, integrating privacy protections in accordance with user consent is fundamental. Otherwise, public trust and acceptance of smart-city technologies will erode. Smart-city infrastructures rely on interconnected systems that enable real-time data exchange. Establishing networks with robust intrusion detection and resistance to unauthorized access is essential for system continuity.

B. System complexity and security services:

Smart cities represent a "system of systems," featuring highly interconnected and interdependent components. As a result, the number of security vulnerabilities may exceed the number of subsystems. To mitigate these risks, sophisticated cryptographic and multi-layered security models are required. Simpler system architectures are inherently easier to compromise. Ensuring cybersecurity requires cost-effective, high-performance security services staffed by qualified experts. From initial installation to ongoing maintenance, smart-city infrastructures must be supported by skilled personnel.

C. Smart data management and system usability and operational continuity:

As personal data are collected through smart meters, smartphones, electric hybrid vehicles, and sensor networks, privacy concerns become increasingly prominent. A central challenge lies in establishing identity and privacy management mechanisms that span the entire system. Smart security systems depend on the coordinated functionality of numerous components. A single attack, for example, unauthorized reconfiguration of a device or impersonation of another system element may disrupt service availability. Therefore, maintaining continuous usability is vital [8, p. 493]. Emergency response planning and key management (Robust Encryption):

Even though the objective is to eliminate vulnerabilities entirely, security breaches remain inevitable. Comprehensive emergency response plans are therefore indispensable, as rapid reaction capability is crucial during crisis events. Strong encryption requires highly scalable key-management systems. Because smart cities involve millions of interconnected devices spanning multiple institutions, authentication, authorization, interoperability, and performance must be upheld at exceptionally high standards [2].

In light of these principles, the effective implementation of cybersecurity in smart cities requires adherence to foundational governance norms: privacy-by-design, accurate threat identification, strong stakeholder participation, transparency, risk minimization, attack-

surface reduction, defense-in-depth, restricted access privileges, least-privilege enforcement, strategic ambiguity where necessary, and robust backup and recovery systems. Ultimately, cybersecurity frameworks must remain adaptive, future-oriented, and capable of integrating emerging technologies to ensure long-term resilience and societal awareness.

*IV. EU legal and regulatory framework for smart city cybersecurity.*

The European Union has developed a robust legal and regulatory framework designed to ensure the cybersecurity and data protection of smart city ecosystems. At the core of this framework is the General Data Protection Regulation (GDPR, 2016/679), which sets stringent requirements for the collection, processing, and storage of personal data, including that obtained from urban IoT devices, sensors, and digital public services (European Commission, 2016). GDPR enforces principles such as lawfulness, fairness, transparency, data minimization, and purpose limitation. Moreover, it grants citizens fundamental rights to access, rectify, or delete their data, obliging public authorities and private operators to adopt privacy-by-design and privacy-by-default approaches in smart city applications. This regulation forms the cornerstone of personal data protection, ensuring that citizens' privacy is preserved in increasingly digitized urban environments [27].

Complementing GDPR, the NIS2 Directive (2022/2555) establishes a comprehensive set of obligations for network and information system security across essential and digital services sectors. The directive covers critical infrastructures that are central to smart city functionality, such as energy distribution, water supply, transportation networks, healthcare, and public administration systems. It mandates that operators implement risk management measures, report incidents promptly to national authorities, conduct security audits, and establish contingency and continuity plans. NIS2 thus addresses the operational resilience of smart cities, emphasizing proactive cybersecurity governance and inter-organizational coordination.

The EU Cybersecurity Act (Regulation 2019/881) further reinforces this framework by introducing a voluntary EU-wide cybersecurity certification scheme for ICT products, services, and processes (European Parliament, 2019). This mechanism provides standardized criteria to evaluate the security level of technologies used in urban environments, enabling public administrations and private operators to select solutions with verified security assurances. Certification also encourages transparency and accountability, while building trust between citizens, service providers, and municipal authorities.

In addition to formal legal instruments, the European Union Agency for Cybersecurity (ENISA) plays a pivotal role in supporting smart city cybersecurity (ENISA, 2020) [9]. ENISA provides practical guidelines, threat analyses, risk assessment frameworks, and sector-specific recommendations. Its guidance emphasizes a risk-based and context-sensitive approach to cybersecurity, advocating the integration of security measures into urban planning, the continuous monitoring of digital infrastructures, and collaboration among municipalities, private operators, and research institutions. ENISA also highlights emerging threats such as ransomware attacks, IoT vulnerabilities, and systemic risks arising from interdependent infrastructures, thereby enabling EU member states to implement preemptive measures.

Furthermore, EU cybersecurity policies promote harmonization across member states to avoid regulatory fragmentation, which is particularly relevant in the context of cross-border smart city projects and shared digital infrastructures. Initiatives such as the EU Cybersecurity Strategy for the Digital Decade outline long-term objectives for secure and

resilient digital transformation, including investment in cybersecurity research, capacity building, and public-private partnerships. By aligning legal obligations, technical standards, and strategic planning, the EU framework provides a multidimensional approach to safeguard smart cities against both technical and socio-legal risks [5].

Overall, the EU legal and regulatory framework demonstrates a systematic integration of personal data protection, infrastructure resilience, and cybersecurity governance. By combining binding regulations, voluntary certification schemes, and expert guidance, it ensures that smart cities can operate efficiently, protect citizens' rights, and withstand cyber threats. The EU approach serves as a model for implementing coordinated, enforceable, and adaptive legal frameworks that underpin the sustainable and secure development of urban digital ecosystems.

*V. Cybersecurity governance and regulatory framework for smart cities development in the Republic of Azerbaijan*

Cybersecurity considerations have become a structural and indispensable component of smart-city development in Azerbaijan, where digital transformation is increasingly embedded into public governance, infrastructure management, and urban planning. The country's political commitment to this transformation was formally articulated through the Presidential Decree of 19 April 2021 on the preparation of the Smart City and Smart Village concepts. This decree functions not merely as a planning document but as a strategic mandate that requires public authorities to adopt technology-based governance models relying on pervasive data collection, interconnected sensor infrastructures, and algorithmic decision-support mechanisms. As a consequence, cybersecurity and data-protection obligations are no longer auxiliary elements but rather intrinsic components of national urban-development policy.

Azerbaijan's foundational information-law framework, primarily the 1998 Law "On Information, Informatization and Protection of Information", predates contemporary cyber-physical architectures but nonetheless provides the conceptual backbone for information governance, delineating responsibilities for protecting information systems, regulating access to data, and defining liability for breaches. However, the evolution of smart-city systems, which operate through high-density IoT devices, cloud-based platforms, open APIs, and machine-learning–driven analytics, places pressure on this earlier legislative framework. Its general principles remain relevant, but technological realities now require substantial modernization to reflect distributed architectures, encrypted data flows, sensor-based environmental monitoring, and autonomous system interactions.

Complementing the general information-law framework is the Law "On Personal Data," which constitutes the core of Azerbaijan's data-protection regime. Smart-city ecosystems inevitably produce extensive personal data, including biometric identifiers (e.g., facial-recognition data), real-time geolocation metrics, behavioural patterns derived from transit-card or sensor usage, and high-resolution video streams captured by intelligent surveillance systems. While the Law "On Personal Data" establishes fundamental obligations such as purpose limitation, data-processing controls, and requirements for consent, it was drafted in a period preceding the mass deployment of municipal IoT networks. As a result, the law's existing rules are increasingly strained by the scale, granularity, and continuous nature of data processing inherent in smart-city infrastructures. Anticipated amendments to the law therefore represent an opportunity

for alignment with international standards and for embedding stronger accountability mechanisms into municipal digital governance.

A major regulatory turning point occurred with the Cabinet of Ministers Decision No. 229 of 17 July 2023, approving the Rules for Ensuring the Security of Critical Information Infrastructure (CII). This decision brings Azerbaijan closer to global cybersecurity governance practices by defining critical information infrastructures broadly and establishing binding obligations for operators across essential sectors, including energy, finance, telecommunications, transportation, water management, and e-government platforms. Smart-city infrastructures, particularly intelligent transport systems, unified municipal platforms, emergency-response networks, and public-utilities monitoring, either constitute or interact directly with these critical infrastructures [25]. Consequently, this Rules have a substantial regulatory effect on smart-city development: operators are required to conduct continuous risk assessments, establish technical and organizational defence mechanisms, report cybersecurity incidents in accordance with national protocols, undergo mandatory audits, and maintain internal rapid-reaction units structurally analogous to sectoral CERTs. As smart-city infrastructures grow in scale and complexity, a larger proportion of their subsystems will fall under the jurisdiction of CII regulation, intensifying the need for standardized technical governance.

Despite these normative advances, Azerbaijan's current cybersecurity ecosystem reflects a structural imbalance between strategic ambition and institutional capacity. The National Information Security and Cybersecurity Strategy for 2023–2027 emphasizes resilience, coordinated cyber-defence, international cooperation, and talent development, signalling an advanced conceptual grasp of national priorities. Yet municipal authorities and local service operators, key actors in smart-city implementation, often lack adequate cybersecurity expertise, standardized operational procedures, and financial resources necessary for maintaining secure digital infrastructures. This discrepancy is particularly concerning because smart-city ecosystems operate as interconnected networks: a single point of weakness in local infrastructure can generate cascading disruptions affecting transport-flow optimization, emergency communications, utility distribution, environmental monitoring, and numerous citizen-facing digital services. In this sense, cybersecurity shortcomings at the municipal level represent systemic vulnerabilities, not isolated administrative challenges.

The rapid expansion of smart-city infrastructures also broadens the national attack surface. The increasing number of IoT endpoints introduces vulnerabilities in device management, firmware updates, authentication procedures, and encryption protocols. Inadequate network segmentation can allow attackers to pivot laterally across municipal systems, potentially compromising multiple layers of urban infrastructure. Moreover, smart-city platforms depend heavily on data centralization, which, while beneficial for efficiency, magnifies the consequences of any data breach. The large-scale processing of biometric, geolocation, and behavioural data also presents significant privacy risks, including unauthorized profiling, re-identification, and potential misuse by unauthorized third parties. As algorithmic and AI-enhanced services expand, these concerns become more pressing, requiring transparent governance, algorithmic accountability, and explicit safeguards preventing discriminatory or opaque decision-making.

Nevertheless, Azerbaijan has unique opportunities to shape a secure and internationally competitive model of smart-city governance. The existence of a regulatory regime for critical infrastructure provides a solid foundation for imposing robust

cybersecurity requirements on all major urban-service providers. The national prioritization of smart cities enables the state to systematically promote "security by design" principles across public procurement, infrastructure planning, and digital-service architecture. The strengthening of national CERT structures and the emergence of sector-specific cybersecurity groups signal the development of institutional capacity necessary for coordinated incident response. At the level of data governance, the forthcoming modernization of personal-data regulation could introduce explicit safeguards for automated decision-making, biometric-data governance, and AI-based municipal systems, enhancing public trust and improving compliance with international norms.

To fully materialize these opportunities, several systemic measures are essential. First, Azerbaijan's information-law framework must be technologically updated to incorporate explicit cybersecurity standards for IoT devices, municipal cloud platforms, authentication mechanisms, encryption protocols, and data-retention cycles. Second, cybersecurity competencies at the municipal level must be significantly strengthened through dedicated funding, technical training, and the establishment of localized incident-response teams. Third, all smart-city procurement processes should embed mandatory cybersecurity-impact assessments, risk analyses, and periodic independent audits. Fourth, personal-data governance should be enhanced through clearer purpose-limitation rules, stricter oversight of biometric and video-analytics systems, expanded rights for data subjects, and transparent communication about data usage. Finally, public participation and awareness should be integrated into smart-city planning, ensuring that citizens understand how their data are collected, processed, and protected.

Taken together, these developments position Azerbaijan at a critical juncture. The state has established a sophisticated regulatory and strategic foundation for secure smart-city development, but the effectiveness of these instruments will depend on coherent implementation, inter-institutional coordination, and the modernization of legacy laws. If legal reforms, capacity-building initiatives, and robust governance mechanisms evolve in parallel with ongoing infrastructure deployment, Azerbaijan has the potential to emerge as a regional leader in secure, rights-respecting, and resilient smart-city governance.

*VI. Conclusion and Recommendations.*

The rapid global transition toward smart-city ecosystems signifies a fundamental reconfiguration of how states conceptualize urban governance, public-service delivery, and infrastructure management. Smart-city projects built upon the integration of IoT networks, sensor-based monitoring, cloud computing, real-time analytics and automated control systems transform cities into continuously functioning digital organisms. While such systems promise efficiency, sustainability and improved quality of life, their reliance on interconnected platforms and expanded data flows exposes them to unprecedented cybersecurity and privacy risks. These risks are not confined to isolated systems; vulnerabilities in even a single component may cascade across entire urban infrastructures, affecting essential public services, critical information infrastructure, and citizen trust. Therefore, the evolution of smart-city initiatives necessarily requires a parallel evolution of legal, institutional and technical mechanisms for cybersecurity regulation.

From a regulatory perspective, the smart-city paradigm blurs traditional boundaries between municipal service provision, national cybersecurity governance, and data-protection law. As cities become cyber-physical environments, legal frameworks must adapt to govern integrated networks where security, privacy, interoperability and

accountability are deeply intertwined. The experience emerging across jurisdictions including the developing framework in Azerbaijan demonstrates that successful smart-city deployment depends not merely on technological adoption but on the robustness of cybersecurity law, risk-management procedures, cross-sector coordination and enforceable data-governance norms. Without such structures, efficiency-oriented digitalisation can inadvertently create large-scale systemic vulnerabilities.

Azerbaijan has already signalled strategic intent, notably through the Presidential Decree launching Smart City/Smart Village concepts and the recent national Strategy on Information Security and Cybersecurity, and has introduced CII rules that bring many urban systems under formal security obligations. These steps provide a strong foundation; however, translating policy into resilient, rights-respecting smart-city practice requires a package of targeted, feasible interventions at legal, institutional, technical and social levels.

Summarizing the above, this article puts forward the following proposals for the legal regulation of cybersecurity, especially in the smart cities project in the Republic of Azerbaijan:

1. To minimise systemic vulnerabilities, smart-city projects would benefit from embedding security-by-design principles throughout their lifecycle. This includes integrating clear security and data-protection criteria into public procurement documentation, encouraging the use of independently validated security controls, and ensuring that vendors provide long-term support, secure update mechanisms, and transparent documentation. Such an approach aligns with global best practices that prioritise early-stage risk identification rather than post-deployment remediation.

2. Given the interdependence of municipal IoT systems, transportation platforms, energy grids and public-service data flows, Azerbaijan may consider forming a coordinated governance mechanism that maintains an updated inventory of smart-city assets, their criticality, and cross-sector dependencies. A dynamic mapping of digital infrastructure, complemented by sector-specific resilience plans and secure information-exchange protocols, would strengthen oversight and reduce regulatory blind spots.

3. Smart-city operations are heavily localized, and timely incident response is essential for preventing cascading failures. Creating municipal-level CERT or incident-response units that operate in close coordination with the national CERT/SOC would enhance rapid detection, containment and recovery capabilities. Periodic joint exercises, standardized escalation procedures and capacity-building programmes would ensure consistent competence across regions, including in newly developed smart-village areas.

4. As smart-city environments rely extensively on biometric systems, continuous location data and AI-enabled analytics, the regulatory framework may be enhanced through clearer rules on data sensitivity, retention, system interoperability and algorithmic accountability. Introducing mandatory cybersecurity-impact and privacy-impact assessments before deployment, alongside transparent oversight of automated decision-making, would help maintain public trust and ensure compliance with fundamental rights. Harmonising these rules with Azerbaijan's long-term digitalisation strategies would support both innovation and responsible governance.

**References:**

1. Ador, S.S. Smart City Security Solution. PhD Thesis. Brac University, Bangladesh, 2019.
2. AlDairi, A., & Tawalbeh., L. Cyber Security Attacks on Smart Cities and Associated Mobile Technologies, Procedia Computer Science, Volume 109, 2017, Pages 1086-1091.

URL: https://doi.org/10.1016/j.procs.2017.05.391 (last access: 29.06.2025).

3. Allwinkle, S.; Cruickshank, P. Creating Smarter Cities: An Overview. Journal of Urban Technology, 2011, Vol. 18, No. 2, pp. 1–16.

4. Anthopoulos, L.G. Understanding Smart Cities: A Tool for Smart Government or an Industrial Trick? Switzerland: Springer, 2017.

5. Batty, M.; Axhausen, K.W.; Giannotti, F., et al. Smart Cities of the Future. The European Physical Journal Special Topics, 2012, Vol. 214, pp. 481–518.

URL: https://doi.org/10.1140/epjst/e2012-01703-3 (last access: 29.06.2025).

6. Bilici, Z.; Babahanoğlu, V. Smart City Applications and the Case of Konya. Journal of Academic Approaches, 2018, Vol. 9, No. 2, pp. 124–139.

7. Caragliu, A.; Del Bo, C.; Nijkamp, P. Smart Cities in Europe. Journal of Urban Technology, 2011, Vol. 18, No. 2, pp. 65–82.

URL: https://doi.org/10.1080/10630732.2011.601117 (last access: 29.06.2025).

8. Elmaghraby, A. (2014). Cyber security challenges in Smart Cities: Safety, security & privacy. Journal of Advanced Research, Volume 5, Issue 4, 491-497.

9. ENISA. Cybersecurity in Smart Cities. European Union Agency for Cybersecurity, 2020.

URL: https://www.enisa.europa.eu/publications/cybersecurity-in-smart-cities (last access: 29.06.2025).

10. European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR). — Brussels, 2016.

11. European Union. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). — Brussels, 2022.

12. European Union. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the EU Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act). — Brussels, 2019.

13. Giffinger, R.; Fertner, C.; Kramar, H.; Kalasek, R.; Pichler-Milanović, N.; Meijers, E. Smart Cities: Ranking of European Medium-Sized Cities. Vienna: Vienna University of Technology, Centre of Regional Science, 2007.

14. Govada, S.; Rodgers, T. Smart Metropolitan Regional Development. In: Vinod Kumar, T.M. (ed.). Towards Smarter Regional Development of Hong Kong Within the Greater Bay Area. Singapore: Springer, 2019, pp. 101–174.

15. Hashem, I.A.T.; Chang, V.; Anuar, N.B. The Role of Big Data in Smart City. International Journal of Information Management, 2016, Vol. 36, No. 5, pp. 748–758.

URL: https://doi.org/10.1016/j.ijinfomgt.2016.05.002 (last access: 29.06.2025).

16. Khalilov K.I. Legal basis of combating cybercrime: current problems and solutions // Uzhhorod National University Herald. Series: Law. — 2025. — № 91 (4). — P. 291–300.

URL: https://visnyk-pravo.uzhnu.edu.ua/article/view/344203 (last access: 29.06.2025).

17. Komninos, N. Intelligent Cities: Innovation, Knowledge Systems and Digital Spaces. London: Routledge, 2013.

18. Law of the Republic of Azerbaijan on Personal Data / Adopted on 11 May 2010; Unified Electronic Database of Legal Acts of the Ministry of Justice of the Republic of Azerbaijan (in Azerbaijani / *"Fərdi məlumatlar haqqında" Azərbaycan Respublikasının*

*Qanunu // 11 may 2010-cu ildə qəbul edilmişdir - Azərbaycan Respublikası Ədliyyə Nazirliyinin Hüquqi Aktların Vahid Elektron Məlumat Bazası*).

URL: https://e-qanun.az/framework/19675 (last access: 29.06.2025).

19. Lizarralde, G.; Chmutina, K.; Bosher, L.; Dainty, A. Sustainability and Resilience in the Built Environment: The Challenges of Establishing a Turquoise Agenda in the UK. Sustainable Cities and Society, 2015, Vol. 15, pp. 96–104.

20. Nam, T.; Pardo, T.A. Conceptualizing Smart City with Dimensions of Technology, People, and Institutions. Proceedings of the 12th Annual International Digital Government Research Conference, 2011, pp. 282–291.

21. Novotný, R.; Kuchta, R.; Kadlec, J. Smart City Concept, Applications and Services. Journal of Telecommunications System and Management, 2014, Vol. 3, No. 2, pp. 1–8.

22. Özay, B. Yeni Kent Yönetimi Yaklaşımı ve Çözümler — Örnek Proje İzmir Kent Güvenlik Yönetimi.

URL: http://www.emo.org.tr/ekler/9aa8e2608db2a72ek.pdf (last access: 29.06.2025).

23. Örselli, E.; Akbay, C. Teknoloji ve Kent Yaşamında Dönüşüm: Akıllı Kentler. Uluslararası Yönetim Akademisi Dergisi, 2018, Vol. 2, No. 1, pp. 228–241.

24. Örselli, E.; Bilici, Z.; Babahanoğlu, V. Akıllı Vatandaş, Akıllı Kentler ve Türkiye. ICPESS 2018, Proceedings Vol. 1, Political Studies, pp. 1–14.

25. "Rules for ensuring the security of critical information infrastructure in the Republic of Azerbaijan" / Approved by Decision of the Cabinet of Ministers of the Republic of Azerbaijan dated 17 July 2023; Unified Electronic Database of Legal Acts of the Republic of Azerbaijan (in Azerbaijani / *"Azərbaycan Respublikasında kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi qaydaları"nın təsdiq edilməsi haqqında Azərbaycan Respublikası Nazirlər Kabinetinin Qərarı // 17 iyul 2023-cü ildə qəbul edilmişdir - Azərbaycan Respublikası Ədliyyə Nazirliyinin Hüquqi Aktların Vahid Elektron Məlumat Bazası*).

URL: https://e-qanun.az/framework/54651 (last access: 29.06.2025).

26. Strategy of the Republic of Azerbaijan on Information Security and Cybersecurity for 2023–2027 / Approved by Decree of the President of the Republic of Azerbaijan dated 28 August 2023; Unified Electronic Database of Legal Acts of the Republic of Azerbaijan (in Azerbaijani / *"Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023 – 2027-ci illər üçün Strategiyası"nın təsdiq edilməsi haqqında" Azərbaycan Respublikası Prezidentinin Sərəncamı // 28 avqust 2023-cü ildə qəbul edilmişdir - Azərbaycan Respublikası Ədliyyə Nazirliyinin Hüquqi Aktların Vahid Elektron Məlumat Bazası*).

URL: https://e-qanun.az/framework/55045 (last access: 29.06.2025).

27. Zanella, A, N. Bui, A. Castellani, L. Vangelista and M. Zorzi. Internet of Things for Smart Cities, in IEEE Internet of Things Journal, 2014, Vol. 1, No. 1, pp. 22-32,

URL: doi: 10.1109/JIOT.2014.2306328 (last access: 29.06.2025).

**Date of receipt of the article in the Editorial Office: 03.07.2025**
**Date of acceptance for publication: 25.12.2025**