Data Privacy Rights in Smart City Governance: Challenges and Policies

1. Saeid Karami*: Assistant Professor, Department of Private Law, Payame Noor University, Tehran, Iran
2. Mohammadreza Mohammadkhani: PhD Student in Development Management, Department of Public Administration, Allameh Tabatabai University, Tehran, Iran
3. Abolfazl Salehsadr: Master, Jurisprudence and Fundamentals of Islamic Law, Tehran University, Tehran, Iran

*Correspondence: karami.t54@pnu.ac.ir

Abstract

The present study was conducted with the aim of identifying the framework of data privacy rights and the legal challenges faced by citizens as a critical instrument in the governance of the emerging smart city ecosystem. Although understanding the various dimensions of the transformative phenomenon of artificial intelligence in urban management requires comprehensive interdisciplinary research, the importance of safeguarding citizens' fundamental rights and fostering their participation as a core pillar of governance in smart cities has rendered the examination of its legal aspects increasingly essential. Accordingly, the research question addresses the nature of data privacy rights and the challenges to citizens' rights in smart city governance. In terms of purpose, this research is applied, and with respect to its methodological approach, it is descriptive-analytical, with data collected through a library-based method. The findings present a novel framework of citizens' concerns regarding data sensitivity as well as the purposes for which data are utilized, which facilitates the identification of fundamental data privacy challenges. The overall conclusion of the study indicates that the rapid and sometimes unpredictable development of emerging technologies, in addition to necessitating increased attention to technical factors, requires appropriate legislative measures to address existing legal gaps and deficiencies based on the proposed framework. Furthermore, by adopting a responsible artificial intelligence approach in smart city governance, it is necessary to design and implement national policies and programs that take into account the identified challenges, alongside regulatory measures targeting both actors and subjects within the urban environment, in order to ensure the protection of citizens' fundamental rights.

Keywords: Smart City, Privacy, Citizens' Rights, Artificial Intelligence, Governance

Received: 21 September 2025
Revised: 18 November 2025
Accepted: 21 November 2025
Published: 01 December 2025

Citation: Karami, S., Mohammadkhani, M., & Salehsadr, A. (2025). Data Privacy Rights in Smart City Governance: Challenges and Policies. *Legal Studies in Digital Age*, 4(4), 1-17.

1. Introduction

Politicians and scholars of management science have called the nineteenth century the century of empires, the twentieth century the century of nation-states, and the twenty-first century the century of cities. According to the latest report of the United Nations Population Fund, more than half of the world's population currently lives in urban areas, and it is projected that

approximately 66 percent of the world's population will live in an urban environment by 2050 (United Nations, 2014). This imposes additional pressure on climate, energy, the environment, and living conditions. In the United Kingdom alone, 82.9 percent of the population lived in an urban area in 2019, and this trend has continued to increase (Lewis, 2016). With the enormous growth of the urban population, cities face numerous challenges and problems, including environmental risks, unfavorable transportation conditions, and economic threats such as unemployment. If this situation signifies the intensification of urban problems and issues together with the growing demand for services, the first and most important institution raised for addressing and responding to these issues is urban management. In fact, the increase in urbanization and urban transformations throughout the world in recent decades has generated unprecedented challenges for urban management policy (Bugge & Voigt, 2008). If the reasons for the failure to implement projects in the path of sustainable development in a metropolis such as Tehran are considered, it becomes clear that the administrative framework and organizational structure of the municipality have been affected by multiple variables and have not sufficiently benefited from transparency and accountability in managerial decision-making, vision formulation, teamwork, expert processes, compliance with law, public interests, and similar matters (Eslami & Alizadegan, 2019). Under such conditions, the key role of urban governance becomes evident, and the challenges facing citizens require urban governance to take steps in the field of smartification and access to managerial information for the development of urban affairs, because, as will be discussed, the smart city relies on open data, information sharing through integrated systems, transparency, and accountability while respecting individual privacy (Zuiderwijk et al., 2012). At this level of urban governance, urban planners and managers have turned to modern technologies and advanced networks, and in recent years they have used artificial intelligence and the Internet of Things to support "smart city" solutions in solving complex urban problems and optimizing city administration. In 2017, Cisco announced a one-billion-dollar investment in smart cities (Cui et al., 2018). China, as the world's most populous country, alone has more than 200 ongoing smart city projects (Li et al., 2015). The use of the Internet of Things has increased in recent years, and figures from the global Statista platform indicate that by 2030 there will be more than 29 billion Internet of Things devices worldwide (Lewis, 2016).

Predictably, a city's infrastructure is embedded with billions of devices that can benefit citizens through various applications such as intelligent transportation systems, smart government, smart healthcare, smart environments, and smart homes. Managers of smart cities and communities can improve citizens' quality of life by properly using artificial intelligence to analyze data for the optimal use of urban resources, better management of infrastructure networks and other essential devices, improvement and control of traffic and urban transportation, prediction and mitigation of flood, fire, and other natural disaster risks, assistance to police in better addressing crime and establishing security, and improvement of service quality, health, and public welfare. Smart city technologies can even contribute to increasing environmental sustainability and reducing environmental damage by controlling climate change, intelligently monitoring wastewater and waste, and reducing greenhouse gas emissions in cities.

Smart cities collect and analyze large volumes of data to achieve smartification objectives, including process automation, service quality improvement, and better decision-making. In other words, these datasets are the feature that makes cities and communities "smart." However, over the past decade, the increasing spread of sensors and data-collection machines in smart cities by the public and private sectors has created democratic challenges surrounding artificial intelligence and the protection of citizens' digital rights, especially privacy protection and personal ownership.

The collection of citizens' data becomes a source of privacy concerns when it includes personally identifiable information. Smart city technologies that collect residents' data, unique identifiers, and personally identifiable information, such as names, usernames, passwords, account numbers, addresses, emails, telephone numbers, credit card numbers, smart card identifiers, license plates, and faces, in order to provide access to everyday life services create attractive targets for cybercriminals. In addition, every internet-connected device involved in receiving or transmitting smart city data is a potential security vulnerability that threatens cybersecurity in the protection of residents' data privacy. Privacy advocates also raise the concern that urban managers share collected data with private-sector partners for secondary use, such as commercial data mining, monetization, compensation for the costs of deploying smart city technologies, or other purposes. For example, analysis of specific data about individuals, such as location and travel history, purchasing patterns, and consumer information, to determine what type of customer a person is may in some cases lead to discriminatory pricing. Some opponents of smart city technologies

warn that smart cities and communities violate individual privacy and infringe civil liberties through government surveillance, whereas the primary condition for the success of any smart program is respect for human dignity, rights, and civil freedoms. Observance of this fundamental condition determines the level of citizens' participation in urban managers' decision-making as well as their trust in the usefulness of new technologies. From the perspective of governance and policy, gaining citizens' trust for full participation in smartification and for improving efficiency and quality of life is highly important. Therefore, in recent years, numerous calls to support citizens' digital rights have led to the emergence of countless reports, manifestos, organizations, projects, and political declarations in various national, transnational, regional, and global contexts. In 2018, the city councils of Barcelona, Amsterdam, and New York established the Cities Coalition for Digital Rights as an international alliance of people-centered global smart cities to promote citizens' digital rights on a global scale, which has so far included 60 cities worldwide. This program is a strategic index supported by the United Nations Human Settlements Programme, which explicitly supports the coalition as an innovative and strategic urban network for full formation and sustainable urban development (Calzada, 2021), because for the sustainable development of a smart city, citizens must be treated as trusted partners. The effects of failing to ensure the subjective and objective security of the privacy of participants in the smart city may sometimes be very severe. For example, falsified healthcare data may lead to the wrong prescription of medication, which may ultimately have serious health consequences for the patient; in such a case, citizens may resort to reactive regulations that guarantee their security and privacy. Moreover, without a secure system and a stable financial environment, key businesses that strengthen the smart city cannot confidently invest in creating smart technologies and entering the smart city market. In such a situation, the economic costs of smart city development will become very high and unsustainable.

Therefore, planning to secure the smart city is of very high importance, because it will have undeniable negative consequences. But are technical solutions sufficient to achieve this objective? What is the role of urban managers as macro-level policymakers of smart cities in protecting citizens' privacy? Given the rapid and pervasive development of emerging technologies, what framework can be drawn for individual privacy so that policymakers and urban managers can consider and use it in balancing the benefits of applying artificial intelligence with privacy challenges and risks in smart city governance?

To answer these questions, the following hypotheses are considered in this research:

Smart cities, alongside their many social and economic opportunities, create democratic challenges surrounding citizens' rights, including the security of individuals' data privacy, because they rely on open data and the sharing of information from integrated systems by the public and private sectors.

From the perspective of governance and policy, gaining citizens' trust as the main participants in the smartification of cities and respecting human dignity, rights, and civil freedoms are undeniable necessities for full participation in this process and for increasing efficiency and sustainable development of the smart city.

The rapid and pervasive development of emerging technologies, on the one hand, and the unpredictable and inconsistent nature of citizens' perceptions, on the other, have made it necessary to establish a specific framework for continuous review, planning, and timely action by the actors and subjects in this field.

The use of technical factors to create immunity for data privacy in smart cities is not sufficient; rather, it requires measures and instruments, including policies, programs, regulations, and procedures, that can guarantee citizens' legal rights in the protection of their privacy.

In view of the above hypotheses, and in order to answer these questions, the present study first explains the concept and key propositions of the smart city and privacy. Then, by outlining the privacy framework in the smart city and its position in international legal institutions and Iran's statutory laws, it examines the most important risks and concerns related to citizens' privacy. Finally, by offering policy recommendations in this field, it seeks to take an effective step toward addressing the stated challenges and creating an appropriate basis for achieving smart city objectives.

2. Background and Research Method

Given the emerging nature of artificial intelligence in Iran and its application in urbanization, the scope of studies conducted to outline citizens' privacy in smart cities has been limited to examining the foundations of citizens' privacy security in the smart city and the outlook of the harms facing it. In the study by Hakim and Ebrahimian (2023), the jurisprudential and legal dimensions of the deprivation of citizen security in artificial intelligence were examined, and by analyzing jurisprudential and

legal opinions, the theory was proposed that anyone who deprives citizens of security and peace through artificial intelligence tools is a combatant and corruptor on earth and, in the event of such action, deserves the imposition of the punishment prescribed for combatants (Hakim & Ebrahimian, 2023). Seddighi et al. (2021), through library studies and a fuzzy Delphi survey of organizational experts, identified three issues—the lack of secure communication, insecure protocols and application programming interfaces, and legislation—as the main cybersecurity threats in the process of smartifying the city of Tehran, and they presented corrective measures and preventive arrangements for each of them (Seddighi et al., 2021). Zakerinia (2023) examined the nature of civil liability arising from artificial intelligence in Iranian law and the laws of European Union member states and, by analyzing statutory laws and conducting a comparative study of European regulations, identified operators of high-risk artificial intelligence systems as having strict liability, which, in cases of multiplicity, becomes joint and several liability. In addition, by examining the Iranian legal system, the study considered the liability of artificial intelligence to have the nature of a special liability based on the act of another and customary attribution, and in cases of multiplicity, shared liability (Zakerinia, 2023).

Considering the initiation and significant progress of the smartification process in developed countries, the existing literature in foreign research is broader. A large volume of this research concerns technological challenges and the presentation of technical solutions. Some other studies have addressed the social nature of smart cities and individuals' rights to privacy protection.

Based on two case studies, Stanciulescu (2021) evaluated the digitalization strategies of Romanian cities for optimizing the relationship between citizens and public services and examined the rights and responsibilities of citizens and local authorities in observing fundamental rights. This is because, during the process of applying smart technologies, every city faces the problem of finding a fair balance between respect for human dignity and citizens' rights, on the one hand, and facilitating access to high-quality services through professional technologies, on the other. The study concludes that the three actors in this field—local authorities, companies involved in city smartification, and citizens—must find a means of cooperating with one another in order to identify the best innovative solutions that benefit all (Stanciulescu, 2021). In a study aimed at explaining the close and important relationship between smart cities and data privacy, Johnson (2023) first explains the types of data collected by smart city technology, the reasons for collecting these data, and the sensitivity of these data in relation to residents' privacy. In the next stage, the study describes the most important privacy concerns associated with smart cities. It also raises other concerns that smart cities and communities should consider alongside privacy protection. Finally, it recommends solutions that balance and address these concerns. These include the recommendation that Congress should pass comprehensive federal data privacy legislation; state legislators should establish laws for accountability and transparency in law enforcement use of smart city data, such as surveillance cameras and gunshot detection technology; governments should regulate and enforce privacy and cybersecurity laws for private companies with which they partner to provide smart city applications; and they should not require third parties to hand over users' sensitive personal data as a condition of operation (Johnson, 2023).

The present study, with an inductive view of the research conducted on citizens' privacy in smart cities, seeks to theorize a framework for examining individuals' privacy concerns in smart cities, based on the assumption that from a governance perspective, people's privacy concerns must be recognized in order to maintain their support and participation in the further development of smart cities. Achieving this objective, in addition to technical solutions, requires macro-managerial measures, including policymaking and attention to the regulation and implementation of comprehensive rules and procedures that can guarantee citizens' legal rights in this field. Accordingly, in terms of its scale in the field of governance and policymaking, its presentation of a framework for privacy security challenges in smart cities, and its comprehensive and up-to-date examination of Iran's legal system, the subject of this research possesses research innovation in comparison with existing studies. In terms of purpose, the present study is applied, and in terms of approach, it is descriptive-analytical in a case-study manner; its data and information were collected through the documentary library method. The applied nature of this research lies in the fact that using its findings and ideas in the continuous comparative assessment of smart city issues in national and international spaces creates an applied need for a more theoretical and situational understanding of privacy concerns in these cities and a deeper understanding of the empirical relationship among data, objectives, and technology for the governors and managers of these cities. With this approach, first, through the library method and the study of documents, credible scientific databases, the latest findings of global technology research centers, and documents of international institutions, including United Nations supporting

documents, as well as the re-examination of Iran's statutory laws, and through a case study of the legal status of citizens' data privacy as one of the most important pillars of smartification, the study attempts, with a descriptive-analytical approach, to outline a novel framework of data privacy in order to achieve a clear understanding of the most fundamental privacy challenges in the smart city. In addition, by using a qualitative method and deductive and inductive reasoning based on the research findings, and by analyzing the outlined framework and challenges, it presents policy solutions for decision-makers and provides the basis for operational planning by urban managers in order to create a balance between the benefits of applying artificial intelligence and privacy threats.

3. Theoretical Foundations of the Research

3.1. The Concept of the Smart City

The purpose of proposing the concept of the smart city may be regarded as achieving sustainable economic development and improving citizens' quality of life. A review of the literature shows that the main axis of the smart city is the advancement of information and communication technology, because a smart city is distinguished from an ordinary city by technology and innovation. With this approach, many definitions exist for smart cities, ranging from definitions that focus exclusively on infrastructure to those that place greater emphasis on empowering citizens and communities to function intelligently. At the 2014 forum, the International Telecommunication Union defined the smart city as follows: "A smart sustainable city is an innovative city that uses information and communication technologies and other means to improve quality of life, efficiency of urban operations and services, and competitiveness, while ensuring that it meets the needs of present and future generations with respect to economic, social, and environmental aspects" (Lea, 2017). This definition emphasizes that the smart city is not merely a city that uses new technologies, but rather an interconnected ecosystem composed of multiple components, including citizens, urban managers, local companies, and industrial and social groups.

As noted, the role of citizens' participation in the realization of the smart city and the important position of governance in providing the basis for and managing this key factor remove the concept of the smart city from exclusive limitation to the application of smart technologies and present a multidimensional definition. Attention to these three essential components as enabling factors of the smart city is necessary for explaining this concept: technological factors, human factors centered on citizens, and institutional and organizational factors, meaning elements that make collective action possible, such as policies and regulations in the field of governance. These factors guide six characteristics: economy, mobility, environment, citizens, living, and governance, as shown in Table 1. These have been widely formulated in the studies of researchers (Giffinger et al., 2007).

Table 1. Characteristics of the Smart City

Characteristic	Description	Author
Smart citizen	As the largest source of urban development and the driving force for achieving smart city objectives, equipped with the knowledge and education required in the field of technology to make better use of social infrastructure and to cultivate creativity and collective intelligence while preserving individual privacy.	(Gil-Garcia et al., 2015)
Smart governance	A structure based on integrated urban governance, with policymaking directed toward public participation, interaction with governmental and private actors, cooperation, and open access to information data while preserving citizens' privacy through the use of hardware and software infrastructure of information and communication technology by means of data exchange, service integration, and urban management communications.	(Giffinger et al., 2007)
Smart economy	A knowledge-based economy, entrepreneurship and digital business, public-private partnerships, and international relations in the form of electronic trade and commerce by using the capacities of secure technologies and innovations.	(Cunha et al., 2016)
Smart mobility	Networked urban transportation resources based on information and communication technology for managing demand flow and population mobility and creating better access for citizens in order to promote social inclusion and avoid the isolation of modern urban neighborhoods.	(Benevolo et al., 2016)
Smart environment	Attractive natural conditions, resource management, and sustainable environmental protection efforts through technology in order to reduce the adverse effects of urbanization, with emphasis on smart energy and information-and-communication-technology-centered energy networks, pollution control in urban systems, green homes, and the management of urban waste and wastewater systems.	(Braun et al., 2018); (Giffinger et al., 2007)
Smart living	Improvement of the urban lifestyle through the standards of a safe and healthy society, such as the safety of citizens' housing, access to health and educational resources, high-quality social services, strengthening of social capital, and creation of a sense of belonging to society among individuals.	(Cunha et al., 2016); (Giffinger et al., 2007)

Source: (Romani et al., 2023)

As can be seen, because smart city initiatives are realized through citizens' participation, human factors are more important than other factors and components of the smart city. Therefore, in summary, a smart city can be described as a city in which efforts are made to use information and communication technology together with human capital to solve urban problems, improve intra-city processes, and enhance citizens' quality of life. In examining the components of the smart city, the concept of security and privacy permeates all the characteristics proposed for the entire structure.

3.2. Citizens' Data Privacy

The concept of privacy was first considered a fundamental right by the European Convention on Human Rights in 1950 and was established as "respect for private life" (Cui et al., 2018). Since then, numerous efforts have been made to explain the concept of privacy in a way that adapts to every new change in reality. Article 12 of the Universal Declaration of Human Rights states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."

The Executive Regulation of the Law on Publication and Free Access to Information, approved by the Council of Ministers on November 12, 2014, in paragraph (c) of Article 1, provides a comprehensive definition of privacy as the domain of an individual's personal life that the individual expects others not to violate without his or her consent or prior notification, or except by law or by judicial authorities; this includes bodily privacy, entry, observation, eavesdropping, and access to an individual's personal information through a computer, mobile phone, letter, residence, vehicle, and that part of privately rented places such as hotels and ships, as well as what is legally considered the private professional activity of any natural or legal person, such as commercial documents, inventions, and discoveries.

Considering that the infrastructure of a smart city includes thousands of devices and applications for improving processes and providing benefits to citizens, the vulnerabilities of this smart system cause the use of devices and applications to face numerous problems concerning security and privacy, because they not only collect a wide range of sensitive information from individuals and the city's social circles, but also control urban facilities and affect citizens' lives. Therefore, the existence of objective security and the protection of data privacy in the context of the smart city are vital factors for the development of subjective security and citizens' trust. Accordingly, and as a result of the increasing reliance of public and private institutions on digital interactions with citizens and consumers, research on data privacy protection has grown significantly over recent decades. Several national and international organizations, such as the Organisation for Economic Co-operation and Development, have identified privacy as a key policy, regulatory, and legal challenge of the twenty-first century, which, in the field of individuals' personal data, includes data collection, storage, management, access, retention, and security (Oecd, 2011).

In fact, this is not a single concept, but rather a set of practices or principles that organizations and governments follow to protect personal data or personally identifiable information (Van Zoonen, 2016). According to the United States National Institute of Standards and Technology, personally identifiable information is any information about an individual maintained by an agency, including:

Any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records.

Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information (National Institute of & Technology, 2015).

3.3. Urban Governance

One of the key and widely used concepts in the management of smart cities is the term urban governance. One of the most important international references for better understanding urban governance is United Nations documents, which in recent years have placed this concept at the center of their studies and missions. In 1996, at the second conference of the United Nations Human Settlements Programme in Istanbul under the Habitat urban agenda, this organization adopted as its slogan the global campaign for establishing good urban governance (Unchs, 2000). According to the definition provided in the United Nations Human Settlements Programme, urban governance is:

"A set of methods for planning and managing the public affairs of cities by public institutions and private entities. This type of governance is a continuous process through which conflicting or opposing interests are reconciled and transformed into participatory action for city administration" (Dameri, 2017).

According to this definition, urban governance includes formal institutions, informal practices, and citizens' social capital.

The World Bank also provided a definition of governance in 1995 as follows:

"Governance is a set of institutional and individual, public and private methods for managing people's common affairs. It is a continuous process that leads to the harmonization of diverse or conflicting interests and consequently to the adoption of participatory actions. Governance includes formal institutions and systems established to guarantee the implementation of law, as well as informal contracts and agreements of people and institutions in pursuit of their interests" (Bugge & Voigt, 2008).

The report of the Commission on Global Governance, which is in fact the main reference for definitions provided regarding governance, states:

"Governance is the sum of the many ways individuals and institutions, public and private, manage their common affairs" (Unchs, 2000).

Governance also includes the services that governments provide for the activities of citizens (Eslami & Alizadegan, 2019).

Therefore, it can be said that urban governance means the influence of all influential pillars of the city on city management through all mechanisms that move, with the participation of public and private participants, toward the advancement of the city and its citizens.

4. Theoretical Literature at the Global Scale

Given the importance of data privacy, the European Union announced its view on the use of artificial intelligence on April 8, 2019. The requirements stated in some of these expressions indicate the importance of citizens' security and privacy:

Human participation and oversight: Artificial intelligence devices must facilitate the existence of certain reasonable societies by supporting the involvement of human agents and by observing fundamental rights, without reducing, limiting, or endangering human autonomy.

Robustness and safety: Artificial intelligence that we can trust requires algorithms to be sufficiently secure, reliable, and robust so that the functioning of artificial intelligence devices does not encounter errors or inconsistencies throughout the entire period.

Respect for private life and data governance: Citizens must have full control over their data, and data must not be used to discriminate against them.

Transparency: The traceability of artificial intelligence systems must be guaranteed.

Diversity, non-discrimination, and equality: Artificial intelligence devices must take into account a set of human abilities, competencies, and needs and ensure access.

Social and environmental well-being: Artificial intelligence devices must be used to accelerate positive social change and to benefit sustainable development and environmental responsibility.

Responsibility: Mechanisms must be established to ensure responsibility for artificial intelligence services and their actions (Stanciulescu, 2021).

In addition, one of the committees established under the Council of Europe under the title of the Committee on Artificial Intelligence for Europe has designed several documents addressing both the promotion of artificial intelligence and the risks associated with specific uses of this new technology. Among these are Artificial Intelligence for Europe (European Commission, 2018), the policy document on artificial intelligence, the European approach to excellence and trust (European Commission, 2020a), the European framework on the ethical aspects of artificial intelligence, robotics, and related technologies (European Commission, 2020b), the proposal for a regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (European Commission, 2021), and the ethics guidelines for trustworthy artificial intelligence (European Commission, 2019). One of the most important issues considered in these

documents is the need to develop safe and responsible artificial intelligence, preserve privacy, comply with existing laws and policies, and align with countries' values (Akbari et al., 2023).

In 2022, the United Nations, in the document "Principles for the Ethical Use of Artificial Intelligence," emphasized the right to privacy and the protection of personal data in data governance mechanisms. This document also emphasizes that organizations must have appropriate oversight mechanisms, impact assessments, audits, and due diligence, including whistleblower protection, to ensure accountability for the impacts of the use of artificial intelligence systems throughout their life cycle. Governance structures must be created or strengthened in such a way that ethical and legal responsibility and accountability for decisions based on artificial intelligence are attributed to humans or legal persons at every stage of the artificial intelligence system's life cycle (United Nations, 2022).

In the United States, the presentation of proposed laws in the field of artificial intelligence regulation has begun through the leadership of research institutes and public organizations. These institutes have designed proposals in the field of this technology with the aim of creating a legal outlook for companies operating in the United States, because no formal national or state law has yet been enacted in the field of artificial intelligence systems (Schreck et al., 2023). Among the institutions active in this field, in particular, the National Institute of Standards and Technology, the Federal Trade Commission, and the Food and Drug Administration have issued documents on artificial intelligence that emphasize features such as safety, resilience, explainability and interpretability, privacy, minimum bias, transparency, and accountability in artificial-intelligence-based systems. In October 2022, a plan titled the Blueprint for an AI Bill of Rights was published at the White House, which was a general policy and roadmap with four main axes:

Axis 1: The use of algorithms must not lead to discrimination and must be designed and used for all individuals.

Axis 2: Individuals must be protected against data misuse, and there must be oversight of how data related to individuals are used.

Axis 3: All individuals must know that an automated system is being used and how and why this automated system produces results that affect them.

Axis 4: Individuals must have the right to be controlled or not controlled by artificial intelligence systems (Friedler, 2022).

In China, the state Artificial Intelligence Governance Committee published a document with the aim of setting out ethical norms for the use of artificial intelligence in China. This document provides guidelines for the use and protection of personal information, human control and responsibility in artificial intelligence, and avoidance of monopolies related to artificial intelligence (National New Generation Artificial Intelligence Governance Professional Committee, 2021).

In Iran, Articles 22, 23, and 25 of the Constitution of the Islamic Republic of Iran refer to the importance of protecting citizens' privacy.

Article 22 of the Constitution states that the dignity, life, property, rights, and residence of individuals are protected from violation except in cases permitted by law. Article 23 of the Constitution also prohibits the investigation of beliefs, and Article 25 prohibits the inspection, non-delivery, recording, and disclosure of telephone conversations, disclosure of telegraphic and telex communications, censorship, non-transmission and non-delivery of such communications, wiretapping, and any kind of surveillance, except by order of law.

On December 15, 1982, the founder of the Islamic Revolution, Imam Khomeini, taking into account the policy of Islam, issued an eight-article decree addressed to the three branches of the government of the Islamic Republic, and in the sixth paragraph of this decree, he prohibited and criminalized unauthorized entry into individuals' personal domain.

The Electronic Commerce Law, approved on January 7, 2004, in Articles 58 to 65 of Chapter Three, explicitly addresses the subject of individuals' privacy in the context of electronic transactions under various headings, including protection of personal data messages, protection of authors' rights and copyright, protection of trade secrets, and protection of trade names. In Articles 71 to 76 of this law, a violator of individuals' privacy is considered a criminal and deserving of punishment. Even in Article 78 of the law, private and public institutions that cause damage to persons are held responsible for compensation.

In 2004, the Law on Respect for Legitimate Freedoms and Protection of Citizens' Rights was approved by the Islamic Consultative Assembly concerning the rights of accused persons before law enforcement officers and judicial authorities; however, it did not directly address the issue of individuals' privacy.

The Law on Publication and Free Access to Information, approved by the Islamic Consultative Assembly on January 24, 2010, in Chapter Four titled "Protection of Privacy," Articles 14 and 15, prohibits institutions' requests to access information about natural persons that would involve unlawful disclosure of personal information. Article 16 states: "Where it is established for institutions subject to this law, on the basis of legal documents, that providing the requested information endangers individuals' life or health or entails financial or commercial damage to them, they must refuse to provide the information."

In addition, the Islamic Penal Code criminalizes offenses against individuals' dignity. For example, Article 669 of the Taazirat and Deterrent Punishments section of this law, amended on May 12, 2020, states:

"Whenever a person threatens another in any manner with murder, bodily harm, damage to honor, financial harm, or disclosure of a secret concerning that person or his or her relatives, whether or not the person thereby demands money or property or demands the performance or omission of an act, he or she shall be sentenced to flogging of up to 74 lashes or imprisonment from one month to one year."

The legislator's explicit position regarding the punishment of a person who violates individuals' life, property, dignity, and secrets indicates the degree of importance of citizens' privacy, whether this violation of dignity occurs in the objective space or in cyberspace. As Article 17 of the Computer Crimes Law, approved in 2009, also states: "Anyone who, by means of computer or telecommunication systems, publishes or makes available to others another person's private or family sound, image, film, or secrets without his or her consent except in legal cases, in such a way that causes harm or is customarily considered a violation of dignity, shall be sentenced to imprisonment from 91 days to two years, or to a fine from five million rials to forty million rials, or to both punishments."

In the Iranian Charter of Citizens' Rights, approved on December 19, 2016, quality of life along with security, protection of human dignity, and immunity of privacy are explained. Article 13 of this Charter states that every citizen has the right to enjoy life, property, dignity, legal, judicial, occupational, social, and similar forms of security. No authority may, in the name of providing security, violate or threaten the legitimate rights and freedoms of citizens and their dignity and honor. Illegal measures in the name of public security, especially intrusion into people's privacy, are prohibited. Article 31 also grants citizens the right to access their personal information collected and stored by persons and institutions providing public services and emphasizes that private information related to individuals cannot be made available to others except by law or with the consent of the individuals themselves. This content is also expressed in Articles 38 and 39 of the Charter of Citizens' Rights.

The right to protection of citizens' personal data and privacy, cybersecurity, and communication and information technologies is referred to in Article 35 of the Charter, and the prohibition of inspection, collection, processing, use, and disclosure of letters, whether electronic or non-electronic, personal information and data, as well as other postal correspondence and telecommunications such as telephone, fax, radio, and private internet communications and similar matters, is explicitly stated in Article 37 of this document.

In Article 14, this Charter obliges the authorities and officers responsible for providing public security to address any unlawful infringement of citizens' freedom and security, and in Article 42, it holds perpetrators of violations of citizens' dignity and privacy in media and public platforms and those causing material or moral damage to them responsible and obliged to compensate for the damage.

The National Data and Information Management Law, approved on November 1, 2022, makes policymaking and the approval of macro-level strategies for the system of production, maintenance, processing, access, integration, exchange, and security of national data and information, with the aim of increasing governance capacity, conditional upon the protection of security, safeguarding of citizens' privacy, and observance of confidentiality of persons' data and information. It assigns the implementation of protective and security measures in this field to the agencies and institutions subject to this law and to service providers under sectoral regulators responsible for producing, maintaining, or processing data and information, and states that violators or those disrupting processing and exchange or refusing to implement this law are subject to the punishments provided in Article 9 of the law.

The Seventh Five-Year Progress Plan of the Islamic Republic of Iran (2024–2028), which, after approval by the Expediency Discernment Council, was notified by the Islamic Consultative Assembly to the government on June 26, 2024, in Articles 75, 103, and added Article 16, emphasizes compliance with Article 25 of the Constitution and the National Data and Information Management Law regarding observance of confidentiality considerations and protection of privacy and citizens' rights.

Nevertheless, given the high importance of privacy and the rapid and sometimes unpredictable development of emerging technologies such as artificial intelligence and the Internet of Things, on the one hand, and the dispersion and insufficiency of existing laws and regulations in both public law and private law, on the other, the drafting of a comprehensive and up-to-date law for protecting citizens' data privacy has become even more necessary.

5. Research Findings

5.1. Data Privacy Framework

Because smart cities rely on the collection and analysis of data and information, this reliance, despite the many opportunities it offers for improving citizens' quality of life, can also entail threats and concerns for data privacy protection. Although there is still no specific empirical research on how people experience their privacy in smart cities, by reviewing some studies (Van Zoonen, 2016), it is possible to outline a framework for this hypothesis. The hypothetical status of this framework does not prevent its usability, and it can serve as a sensitive tool for policymakers and urban managers in the smart city so that they may take privacy concerns into account in their policymaking and operational decision-making. It also provides a set of hypotheses for academic researchers to conduct further research on privacy concerns in smart cities. Understanding this framework is based on recognizing the type of data involved and the purpose of collecting and using the data.

5.2. Types of Data

Although explicit definitions of personal data or personally identifiable data exist in international laws and regulations, individuals themselves are less sensitive about some of what is considered personal data. Various international surveys have shown that people consider medical, financial, and civil data to be highly sensitive, whereas an individual's nationality, gender, or age are considered less problematic (Van Zoonen, 2016). However, no research has examined how people feel about the collection of non-personal data such as traffic flow or air quality, and there is little reason to expect that people would be concerned about it. These data reveal nothing about specific individuals and therefore usually fall outside the scope of privacy concerns. Nevertheless, there is growing concern about the possibility of combining apparently non-personal data with highly personal data in citizen or consumer profiles, but individuals' concerns differ. For example, people differ in their sensitivity to social media updates or consumption patterns; for some individuals, such data are highly private, while for others they are unproblematic (Eurobarometer, 2011).

5.3. Data Purposes

Research on privacy concerns shows that individuals assess the purpose for which data are used and weigh the benefits that providing their data may offer them. For example, in the case of medical services or commercial benefits, most people are willing to share their data with the organization requesting them. However, they calculate the relationship between the amount of data requested and the benefits received in the data exchange and request. A complicating factor for citizens and consumers in assessing the purpose of data collection arises from the concern that their data may be used for purposes other than those for which they were originally collected.

An example of public suspicion about secondary use of citizens' data can be seen in the data-sharing plan of the National Health Service in England. This plan came under attack when it appeared that medical records held by general practitioners were being shared not only with other health and care institutions, but also with commercial third parties, especially health insurance companies (Van Zoonen, 2016). According to a British newspaper, more than 700,000 people opted out of the plan as a result of the controversy (Dominiczak, 2015).

5.4. The Fourfold Framework Model

Based on the study conducted on two dimensions of privacy concerns related to types of data and purposes of data use, a 2 × 2 privacy framework can be outlined, identifying four possible types of sensitivity that people may have regarding smart city

data (Figure 1). This model shows, on the one hand, that individuals consider certain data more personal and sensitive than others, and on the other hand, that individuals' privacy concerns differ according to the purposes of use.

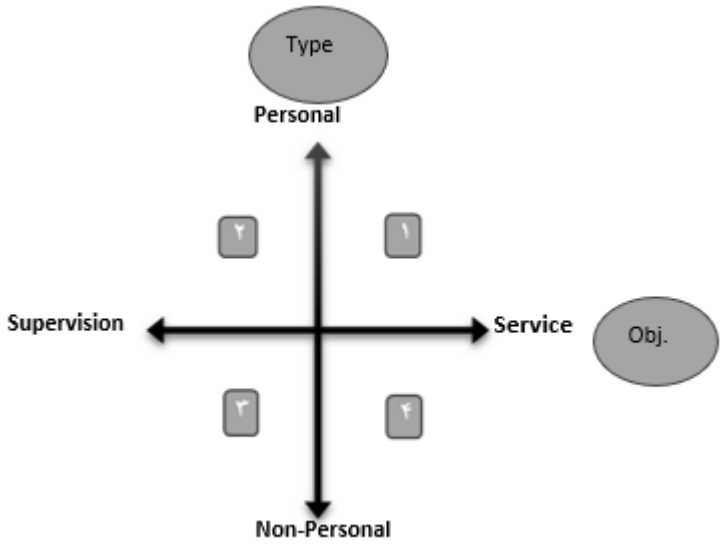

Figure 1: Fourfold Model of the Privacy Framework

5.5. Personal Data for Service Purposes

The data collected and recorded about citizens that fall in the first quadrant of the framework include information that people consider more sensitive in relation to the use of social and economic care, such as civil status, including birth, death, and marriage, housing, elections, or employment. In the digital age, this quadrant has expanded through data resulting from online transactions between urban services and citizens and from the social media behavior of residents and visitors. Urban managers collect and use these data to monitor residents' demographic patterns, assess the quality of interaction with them, and analyze civic mood. The purpose of these data is to support urban management and planning, improve urban services, and support local citizens. The privacy challenge in this quadrant is usually moderate because, first, this type of data is part of urban management and is rarely subject to civil concerns. Second, because of the service purpose, citizens experience a positive exchange between providing personal data and receiving social benefits. Nevertheless, especially in the latter case, there is a continuous risk that these data practices may move into the second quadrant, where highly personal data are used for surveillance purposes.

5.6. Personal Data for Surveillance Purposes

This quadrant includes personal data collected for surveillance purposes. This section includes all police data, ranging from minor violations to stop-and-search and criminal offense data, as well as data from city managers, such as public transportation data. Software innovations have added another layer to these data, for example, the use of facial recognition software to analyze images captured by closed-circuit cameras. Clearly, all these data are directly personal, and citizens often experience such data as highly sensitive. The combination of highly personal data collected and used for purposes of government surveillance and control has made this quadrant a contested quadrant.

5.7. Non-Personal Data for Surveillance Purposes

The data in this quadrant concern all data that cannot be linked to an individual and are used for surveillance and control purposes. Such data are obtained from the aggregation and combination of survey and registration data in the city, often used in combination with geographic information systems. Examples include data obtained from monitoring traffic flows, public transportation, crowds, sports, and event management through infrared cameras, closed-circuit cameras, or thermal sensors. These data may not automatically be considered sensitive because they do not measure individuals, but rather populations or non-personal flows of vehicles. For example, through postal-code-based data, police statistics, and housing and business

information, certain urban areas can be identified as areas with high risks of economic or social unrest. Many developments in preventive policing and the identification of neighborhoods or streets with a high risk of crime are achieved on this basis (Perry, 2013). All these data can be analyzed in a way that makes it possible to identify any citizen, thereby transforming non-personal data into personal data. For example, individuals can be identified in a crowd through facial recognition software, and location data profiling can be performed so precisely that the identification of individual households becomes possible. Accordingly, this creates civic, political, and individual suspicion and forms an unstable policy arena. In the United States, many civil organizations have protested against local police agencies that possess preventive software and have argued that its algorithms are derived from police biases and perpetuate racist and prejudiced profiling (Koss, 2015).

5.8. Non-Personal Data for Service Purposes

A large portion of current smart city technologies and collected non-personal data is used for the direct benefit of the urban environment, citizens' welfare, and more efficient urban operations. These include monitoring systems for weather and air quality, noise, smart waste management, and energy systems. Urban public health policies increasingly use such indicators, for example, identifying areas with high air pollution or noise pollution and correlating them with patterns of specific diseases (Erdem et al., 2015). The data used for these applications are about objects rather than individuals and therefore may have lower sensitivity. All data that cities currently make available through their open-data portals also fall within this quadrant, because privacy regulations prevent cities from publishing any other type of data (Zuiderwijk et al., 2012). The combination of non-personal data with service purposes appears to make this quadrant harmless for policies and government, because security breaches and data misuse are unlikely to have direct and significant effects on citizens. Nevertheless, here too, privacy concerns arise from more precise profiling methods that may make it possible to re-identify individuals from large-scale and anonymized data (Kitchin, 2014).

5.9. Data Privacy Challenges

Considering the framework described above, as well as studies conducted in smart cities on how data collected from citizens of these cities are used, several challenges can be observed. The most important challenges for privacy can be divided into three categories: data cybersecurity, secondary use of data, and government surveillance (Johnson, 2023).

5.10. Data Cybersecurity

The immunity of privacy protection when using smart city data is of very high importance. Entities that collect individuals' personal data have a responsibility to keep those data secure from unauthorized access. Data breaches can, and often do, result in individuals' personal information falling into the wrong hands, including criminals and even foreign state-sponsored hacking groups, and they often impose significant economic losses. The average cost of a public-sector data breach in 2022 was slightly more than two million dollars (Johnson, 2023).

Smart cities and communities are usually vulnerable to cyberattacks because of their use of Internet of Things devices. The potential security risk of Internet of Things devices has been well documented since their introduction, and many stakeholders and experts have emphasized the need for stronger security protections (Klein, 2021); (Hall, 2018). These devices often connect to the internet and give attackers an entry point to other devices that are not secure. Another factor affecting governments' vulnerability to cyberattacks is the amount of data, especially sensitive data, that they collect from their employees and citizens, which is true even without the collection of smart city data. Many large-scale cyberattacks target governments. Governments also control critical infrastructure, which is another valuable target for attackers (Center for Strategic International Studies, 2022).

Accordingly, governments often fail to prioritize cybersecurity. Urban management institutions have limited budgets for procuring secure technologies, updating them regularly, and hiring and retaining cybersecurity experts. A survey of local

government agencies in the United States shows that almost one-third are not even able to detect that they have been hacked (Forno, 2022).

Together, these factors make smart cities and communities attractive targets for cyberattacks. The number of entities that have access to data can also increase vulnerability. For example, if a smart city or community shares certain data with a private partner, a cyberattack on either the public entity or the private partner can compromise those data.

Therefore, data security is a serious concern for smart cities and communities and must be prioritized. Effectively addressing this concern requires urban managers to exercise caution in applying smart city technologies, follow best cybersecurity practices, increase their investment in cybersecurity, update information technology devices, and require their private partners to follow the same practices.

5.11. Secondary Use of Data

The second category of major privacy challenges in smart cities and communities is secondary use and unauthorized commercial exploitation of citizens' data. For example, analysis of specific data about individuals, such as location and travel history, purchasing patterns, and consumer information, to determine what type of customer a person is may in some cases lead to discriminatory pricing. Two situations can be imagined for this type of use. In the first situation, a city can partner with a private company to pay for or provide specific smart city technologies, and in return, the company has access to data it collects from the city and the community. In the second situation, a city can sell local advertisements that do not personally target residents but instead target the broader community.

In the first situation, privacy concerns arise when a city or community shares residents' sensitive personal data with private partners, especially if there is no law or restriction on how private partners use those data and if residents have no opportunity to grant or revoke consent for data sharing.

In the second situation, cities do not need to share residents' personal information with advertisers. Unlike targeted advertising, which targets consumers based on their individual characteristics and their online purchasing or browsing history, public advertising targets the entire community.

To better protect citizens' privacy when sharing their data, smart cities can establish rules for their private partners' use of smart city data and continuously monitor implementation to ensure proper enforcement. This is similar to what is referred to below in Article 14 of the Law on Publication and Free Access to Information, approved on January 24, 2010, regarding public institutions' access to information related to individuals' privacy. Article 6 of the National Data and Information Management Law, approved on November 1, 2022, also assigns protective and security measures for safeguarding data and information and preserving the confidentiality of persons' data and information to the agencies and institutions subject to this law and to service providers under sectoral regulators responsible for producing, maintaining, or processing data and information.

5.12. Government Surveillance

As this type of privacy concern was explained in detail in the 2 × 2 framework section, governments can use smart city projects to monitor individuals. Critics of smart cities believe that although many data collected by smart cities pose little risk to individuals' privacy on their own, theoretically, governments that have access to sufficient data collected by smart city technologies can build detailed profiles of residents. For example, a widespread narrative reinforces concerns that the Chinese government uses artificial intelligence to monitor citizens' behavior and rank them through a social credit system, assessing citizens' trustworthiness on the basis of various factors, including spending habits, online activity, and lawbreaking behavior. It is noteworthy that no technologically advanced social scoring system exists in that country (Heikkila, 2022).

Despite the outlined framework and the stated challenges, it should be noted that, on the one hand, individuals' concerns and perceptions are not always highly consistent or predictable, and, on the other hand, the development of artificial intelligence technology in the smart city and the expansion of data are so rapid and pervasive that smart city governance policies and existing laws and regulations may not respond to individuals' concerns in the coming decades. Therefore, governments and managers of smart cities face a threefold challenge:

The possibility and manner of identifying future privacy concerns of citizens in relation to emerging technologies and methods of data use.

Identifying whether and how these cases fall under laws and regulations related to data privacy protection.

The necessity of presenting a specific urban policy concerning new developments that fully addresses citizens' legal concerns beyond strictly legal requirements.

6. Discussion and Conclusion

The use of emerging artificial intelligence technology in urban management and the improvement of the public sector leads to confidence and stability in governance and creates value and legitimacy for governance by increasing predictability, improving understanding of the dimensions of problems and consequences, increasing the quality, accuracy, and speed of decisions, ensuring transparency and responsiveness to citizens' needs, and creating a basis for interaction with them in order to improve citizens' satisfaction and the overall welfare of society. The full realization of the smart city depends on appropriate cooperation and collaboration between urban decision-makers and citizens. One of the most important manifestations of this cooperation is citizens' trust in the performance of the smart city. The key element in creating this trust is the immunity of privacy and the security of personal information, because if the subjective and objective security of citizens' privacy as the main participants in the smartification of cities is not ensured, the ultimate goal of the smart city will not be achieved. Cities must establish a balance between the benefits of applying emerging technologies and privacy threats in the smart city and must implement the necessary measures in the digitalization process while simultaneously observing citizens' fundamental rights and freedoms. This is because, from the perspective of governance and policy, citizens' trust is important for full participation in smartification and for increasing urban efficiency and quality of life. However, it must be noted that the use of technical factors alone is not sufficient to achieve this objective; rather, smart city measures and instruments must include policies, programs, regulations, and procedures that can guarantee citizens' legal rights in protecting their privacy.

In this regard, the present study, with a new view of the status of information privacy in international legal institutions and Iran's statutory laws, outlined the privacy framework in the smart city and examined the most important concerns of citizens and advocates of citizens' rights. Based on this study, a framework was presented for understanding individuals' privacy concerns in smart cities, and it was stated that these concerns differ according to the type of data involved and can range from personal to non-personal data and include all intermediate degrees and combinations. Concerns also differ according to the purpose for which the data are used, which can move from improving life and services in a city toward advancing surveillance and control of citizens. Then, by analyzing the fundamental challenges of data privacy protection, it was shown that the hypothetical status of the outlined framework and challenges does not prevent the use of artificial intelligence capacities in city management and can act as a sensitive tool for policymakers and operational managers in the smart city, indicating in which contexts privacy concerns may arise among their citizens. According to the studies conducted in the present research, although some of these concerns are covered by international regulations and domestic laws of the Islamic Republic of Iran concerning the processing of personal data, smart city technologies and data development are so rapid and pervasive that formal laws may fall short in the coming decades. Accordingly, it is necessary for the legislative institution, by taking into account the privacy framework outlined in this study, to take appropriate legislative measures to fill the gaps and remove existing legal defects in the procedures, rules, and regulations governing the use of artificial intelligence in urban management, as well as to draft a specific, comprehensive law and regulations on electronic information analysis, thereby providing the necessary legal bases for addressing the stated challenges in implementing smart cities. Despite the absence of a strategic or legal document specifically in the field of artificial intelligence development in the country, the "Strategic Document of the Islamic Republic of Iran in the Field of Cyberspace," approved in 2022 by the Supreme Council of Cyberspace, currently assigns the design of the system for applying emerging cyberspace technologies, including artificial intelligence, to the Vice Presidency for Science, Technology, and Knowledge-Based Economy. It has also assigned the design of the data governance system, which is a prerequisite for the comprehensive development of artificial intelligence, and the design of smart government to the Ministry of Information and Communications Technology. However, attention must be paid to the following important points: first, the enactment of laws and regulations must not prevent smart city innovations; second, laws and programs must be aligned with the long-term and comprehensive policy and strategy of artificial intelligence and directed toward gaining the trust of citizens and community stakeholders and strengthening governance; third, operationalizing these laws requires the necessary determination for implementation and follow-up by the government and city managers.

Considering that many international institutions and developed countries, such as the European Union, the United States, and China, as pioneers of artificial intelligence, have already formulated and approved comprehensive policies, laws, and guidelines for protecting individuals' information and privacy, a comparative study of existing strategies, policies, and laws can provide guidance in this field. It is obvious that the national strategy in the field of the legal and ethical dimensions of artificial intelligence and smart cities must be localized and regulated by taking into account Iran's conditions, values, and legal system, and mere imitation of the strategies and documents of other countries will not be effective. As stated in the theoretical foundations of the present study, identifying and adopting policies and developing smartification processes in cities must include three human, institutional, and technological factors in order to guide economy, mobility, environment, citizens, living, and governance as the six key characteristics of the smart city at the final point of the real expectations curve.

It should be noted that in the smart city ecosystem, attention to self-regulatory frameworks and modern supervisory frameworks precedes legislative measures. This is because, on the one hand, the rapid development of artificial intelligence and the smart city phenomenon and the uncertainties in this field, and, on the other hand, the lengthy process of legislative measures, have increased the importance of designing an up-to-date supervisory framework for monitoring and evaluating the performance of artificial intelligence and the public and private implementing sectors in the smart city. To prevent data breaches and misuse of sensitive personal data, smart cities must monitor the performance of artificial intelligence and executive actors in the public sector and their private partners to ensure that privacy and data security standards are followed and that accessible data are used only for predetermined purposes. This is because gaining citizens' public trust requires transparency in the performance of public institutions and private partners when dealing with personal data. The private sectors of the smart city must also take initiative and ensure their compliance with laws before supervisory authorities intervene, as emphasized in the National Data and Information Management Law and the Law on Publication and Free Access to Information. In this context, it must be emphasized that the up-to-dateness of supervisory mechanisms is highly important, because traditional supervisory frameworks not only lack the capacity to confront the risks and capacities of artificial intelligence, but also illustrate the early failure of policymaking in this field.

The government and smart city managers must regulate by adopting the approach of "responsible artificial intelligence" (Akbari et al., 2023), while obliging and encouraging institutions to conduct comprehensive risk assessment, implement explainable artificial intelligence models, and create algorithmic transparency mechanisms to identify possible biases and unintended consequences. The main indicator of regulation is collective legitimacy, which is achieved through transparency, participation-seeking, linkage with stakeholders and citizens, and ultimately accepting legal responsibility for decisions. This regulation requires a cross-sectoral institution in scientific, cultural, social, economic, and security terms that, while involving citizens, provides the basis for governance convergence in the development of responsible artificial intelligence. Among the most important measures of this regulatory institution, in addition to presenting general policies for artificial intelligence development, are adopting positions and evaluating social, cultural, legal, and security impacts in the field of artificial intelligence, publicly announcing them to citizens, regulating mechanisms for accountability to community stakeholders, and presenting legislative proposals in this field.

Urban managers have a duty to pursue appropriate national programs for developing the digital competencies of residents of smart cities and to educate people and other participating sectors about the benefits provided by information technology and electronic public services, as well as the correct methods of using them while preserving privacy. Accordingly, Article 107, paragraph (c), of the Seventh Five-Year Progress Plan of the Islamic Republic of Iran, in line with the formation of electronic government, obliges the country's executive agencies to prepare and implement an operational program for establishing and implementing the smartification cycle, reforming processes, and establishing a data-based governance system. In added Article 65, paragraph 3, this law also obliges the National Center of Cyberspace and the Ministry of Information and Communications Technology to draft a national program for the development of artificial intelligence in order to provide sustainable technical, social, ethical, and legal knowledge and infrastructure and to promote and increase awareness of the functions of artificial intelligence in various fields and its potential risks. The important point in this regard is the development of theorization platforms in this field, which must be activated and organized with emphasis on the philosophy of science, technology, and artificial intelligence, based on social and local values, and aligned with the general progress of the country.

Cities must prioritize cybersecurity when implementing smart technologies and use advanced protective models, such as setting desirable security requirements for procuring internet-connected devices, encrypting smart city data, implementing

controls and monitoring network access, conducting regular threat and risk assessments, and migrating to cloud computing. As far as possible, smart cities must anonymize any personal information they collect through new technologies in order to reduce the potential threat to individuals' privacy. They should also, where possible, delete stored personal data after a specified period when the data are no longer useful for their intended function. In addition to requiring the allocation of necessary budget lines in relevant administrative sectors, these measures require organizational regulations and circulars concerning attention to the improvement of technological infrastructure.

Managers of smart cities also have a duty to educate the actors and subjects of the city about the various dimensions of the smart city, regulate national policies, laws, and programs for the correct use of emerging technologies, enhance citizens' digital capabilities, develop the smart city sustainably, and, through precise control of the smartification process, supervise observance of citizens' fundamental rights and freedoms so that citizens' rights in the dimension of privacy are guaranteed.

Based on what has been stated, in addition to creating an applied need for governors and managers of the smart city to gain a deeper understanding of the empirical relationship among data, objectives, and technology, this research provides a new research framework for academic researchers to achieve a more theoretical and situational understanding of individuals' privacy concerns in these cities and makes possible the continuous comparative examination of issues in national and international contexts.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all who helped us through this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Akbari, I., Yousefi, A., & Mehraban Hallan, M. M. (2023). *Review Report on the Seventh Development Plan Bill: Sustainable Development of Artificial Intelligence in the Country*.

Benevolo, C., Dameri, R. P., & D'Auria, B. (2016). Smart Mobility in Smart City: Action Taxonomy, ICT Intensity and Public Benefits. In *Empowering Organizations: Enabling Platforms and Artefacts* (pp. 13-28). Springer International Publishing.

Braun, T., Fung, B. C., Iqbal, F., & Shah, B. (2018). Security and Privacy Challenges in Smart Cities. *Sustainable Cities and Society*, *39*, 499-507. https://doi.org/10.1016/j.scs.2018.02.039

Bugge, H. C., & Voigt, C. (2008). *Sustainable Development in International and National Law: What Did the Brundtland Report Do to Legal Thinking and Legal Development, and Where Can We Go from Here?* Europa Law Publishing.

Calzada, I. (2021). The Right to Have Digital Rights in Smart Cities. *Sustainability*, *13*(20), 11438. https://doi.org/10.3390/su132011438

Center for Strategic International Studies. (2022). *Significant Cyber Incidents*. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Cui, L., Xie, G., Qu, Y., Gao, L., & Yang, Y. (2018). Security and Privacy in Smart Cities: Challenges and Opportunities. *IEEE Access*, *6*, 46134-46145. https://doi.org/10.1109/ACCESS.2018.2853985

Cunha, M. A., Przeybilovicz, E., Macaya, J. F. M., & Santos, F. B. P. D. (2016). *Smart Cities: Digital Transformation of Cities*.

Dameri, R. P. (2017). *Smart City Implementation: Creating Economic and Public Value in Innovative Urban Systems*. Springer International Publishing.

Dominiczak, P. (2015, 2015/06/05). Nearly One Million Patients Could Be Having Confidential Data Shared Against Their Wishes.

Erdem, O., Prins, R. G., Voorham, T. A., Van Lenthe, F. J., & Burdorf, A. (2015). Structural Neighbourhood Conditions, Social Cohesion and Psychological Distress in the Netherlands. *European journal of public health*, *25*(6), 995-1001. https://doi.org/10.1093/eurpub/ckv120

Eslami, R., & Alizadegan, F. (2019). *The Right to the City*. Shahr Danesh Legal Research Institute Press.

Eurobarometer. (2011). *Attitudes on Data Protection and Electronic Identity in the European Union* (Special Eurobarometer 359 Report, Issue. https://joinup.ec.europa.eu/node/125717

European Commission. (2018). *Artificial Intelligence for Europe*. https://digital-strategy.ec.europa.eu/en/library/communication-artificial-intelligence-europe
European Commission. (2019). *Ethics Guidelines for Trustworthy AI*. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai
European Commission. (2020a). *European Framework on Ethical Aspects of Artificial Intelligence, Robotics and Related Technologies*. https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2020)654179
European Commission. (2020b). *White Paper on Artificial Intelligence: A European Approach to Excellence and Trust*. https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en
European Commission. (2021). *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206
Forno, R. (2022, 2022/03/28). *Local Governments Are Attractive Targets for Hackers and Are Ill-Prepared*. Center for Internet and Society. https://cyberlaw.stanford.edu/blog/2022/03/local-governments-are-attractive-targets-hackers-and-are-ill-prepared
Friedler, S. (2022). *Unpacking the White House Blueprint for an AI Bill of Rights*. Brookings Institution. https://www.brookings.edu/events/unpacking-the-white-house-blueprint-for-an-ai-bill-of-rights
Giffinger, R., Fertner, C., Kramar, H., Kalasek, R., Pichler-Milanovic, N., & Meijers, E. J. (2007). *Smart Cities: Ranking of European Medium-Sized Cities* (Final Report, Issue.
Gil-Garcia, J. R., Pardo, T. A., & Nam, T. (2015). What Makes a City Smart? Identifying Core Components and Proposing an Integrative and Comprehensive Conceptualization. *Information Polity*, *20*(1), 61-87. https://doi.org/10.3233/IP-150354
Hakim, S. M., & Ebrahimian, S. H. (2023). Jurisprudential and Legal Analysis of the Deprivation of Citizen Security in Artificial Intelligence. *Islamic Jurisprudence and Law Research*.
Hall, J. L. (2018). *Comments to the CPSC on the Internet of Things and Consumer Product Hazards*. https://cdt.org/wp-content/uploads/2018/06/CDT-CPSC-IoT-Comments-061518.pdf
Heikkila, M. (2022, 2022/11/29). The AI Myth Western Lawmakers Get Wrong. https://www.technologyreview.com/2022/11/29/1063777/the-ai-myth-western-lawmakers-get-wrong/
Johnson, A. (2023). *Balancing Privacy and Innovation in Smart Cities and Communities*. https://itif.org/publications/2023/03/06/balancing-privacy-and-innovation-in-smart-cities-and-communities/
Kitchin, R. (2014). *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*. SAGE Publications. https://doi.org/10.4135/9781473909472
Klein, A. (2021, 2021/07/07). *Biden Took the First Step on National Cybersecurity Standards: Congress Needs to Follow Through*. New America. https://www.newamerica.org/oti/blog/biden-took-the-first-step-on-national-cybersecurity-standards-congress-needs-to-follow-through/
Koss, K. K. (2015). Leveraging Predictive Policing Algorithms to Restore Fourth Amendment Protections in High-Crime Areas in a Post-Wardlow World. *Chicago-Kent Law Review*, *90*, 301.
Lea, R. (2017). *Smart Cities: An Overview of the Technology Trends Driving Smart Cities*.
Lewis, J. A. (2016). *Managing Risk for the Internet of Things*.
Li, Y., Lin, Y., & Geertman, S. (2015, 2015/07/07). The Development of Smart Cities in China. Proceedings of the 14th International Conference on Computers in Urban Planning and Urban Management,
National Institute of, S., & Technology. (2015). *Glossary PII*. https://csrc.nist.gov/glossary/term/PII
National New Generation Artificial Intelligence Governance Professional Committee. (2021). *Ethical Code of Artificial Intelligence of the New Generation.* https://www-most-gov-cn.translate.goog/kjbgz/202109/t20210926_177063.html?_x_tr_sl=auto&_x_tr_tl=fa&_x_tr_hl=en-US&_x_tr_pto=wapp
Oecd. (2011). *Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy, Guidance for Government Policy Makers*.
Perry, W. L. (2013). *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. RAND Corporation.
Romani, G. F., Pinochet, L. H. C., Pardim, V. I., & Souza, C. A. D. (2023). Security as a Key Factor for the Smart City, Citizens' Trust, and the Use of Technologies. *Revista De Administração Pública*, *57*, e2022-0145. https://doi.org/10.1590/0034-761220220145x
Schreck, M., Gomez, M., & Charkoudian, S. (2023). *An Overview of the Landscape for US Regulation of AI Technology*. https://www.goodwinlaw.com/en/insights/publications/2023/04/04_12-us-artificial-intelligence-regulations
Seddighi, N., Sanaei, M. R., & Ehtesham Rasi, R. (2021). Identification and Assessment of Cyber Security and Privacy Challenges in the Transition of Tehran Metropolis to Smart City Under Uncertainty. *Business Intelligence Management Studies*, *10*(38), 109-136. https://doi.org/10.22054/ims.2021.59476.1925
Stanciulescu, M. (2021). Smart Citizens, Smart Administration: Between Rights and Responsibilities. Smart Cities International Conference Proceedings,
Unchs. (2000). *Norms for Good Urban Governance*. www.UNCHS.org
United Nations. (2014). *World Urbanization Prospects*.
United Nations. (2022). *Principles for the Ethical Use of Artificial Intelligence in the United Nations System*.
Van Zoonen, L. (2016). Privacy Concerns in Smart Cities. *Government Information Quarterly*, *33*(3), 472-480. https://doi.org/10.1016/j.giq.2016.06.004
Zakerinia, H. (2023). The Nature and Basis of Civil Liability Arising from Artificial Intelligence in Iranian and EU Members' Laws. *Private Law*, *20*(1), 135-152. https://doi.org/10.22059/jolt.2023.356703.1007186
Zuiderwijk, A., Janssen, M., Choenni, S., Meijer, R., & Alibaks, R. S. (2012). Socio-Technical Impediments of Open Data. *Electronic Journal of e-Government*, *10*(2), 156-172.