International Journal of Cyber Law |
Volume: 1 Issue: 4
2023

Balance Between Data Collection and Privacy in the Context of Smart Cities

Islombek Rustambekov
Tashkent State University of Law
i.rustambekov@tsul.uz

Sadokat Safoeva
Tashkent State University of Law
s.safoeva@tsul.uz

Andrey Rodionov
Tashkent State University of Law
andre-rodionov@mail.ru

Rakhmatov Uktam
Tashkent State University of Law
u.rakhmatov@tsul.uz

Abstract

The emergence of Smart Cities as a response to the need for efficient, sustainable, and livable urban environments has gained significant traction in recent years. Smart cities leverage advanced technologies to collect and analyze vast amounts of data, facilitating data-driven decision-making and improved services for residents. However, this data collection raises crucial concerns regarding privacy and the potential misuse of personal information. This article examines the global challenge of achieving a balance between data collection and privacy in the context of smart cities. It delves into the complexities surrounding urban data collection, highlighting the importance of safeguarding individuals' privacy rights. Drawing on international perspectives and best practices, this study proposes solutions to address this critical issue, including the implementation of robust data protection frameworks, privacy-enhancing technologies, and citizen-centric governance models. By striking the right balance between data collection and privacy, smart cities can harness the power of data while ensuring the protection of individuals' privacy rights in the digital age.

Keywords: Smart Cities, Data Privacy, Legal Framework, International Law, Privacy Risks

I. Introduction

The rapid growth of Smart Cities and the extensive collection of urban data have increased the need to protect people's privacy rights. While the use of data can bring numerous benefits, such as improved city planning, resource allocation, and service delivery, it also raises concerns about the potential invasion of privacy and misuse of personal information. It is critical to strike a balance between harnessing the power of data for the good of society and protecting people's privacy (Smith & Johnson, 2018; Lee, 2019). By examining existing legal provisions, we can evaluate their applicability to the collection and use of urban data and identify problems and gaps in the current legal framework [1].

In addition, this article proposes solutions to address the global problem of balancing urban data collection and privacy concerns. These decisions take into account ethical, legal and technological considerations to ensure the responsible and transparent use of urban data (Brown et al., 2020; Garcia & Martinez, 2017). The results of this study contribute to the ongoing debate about Smart Cities and data privacy, highlighting the importance of addressing a global challenge. By identifying potential solutions and examining their feasibility and effectiveness, we can pave the way for the development of laws and regulations that protect privacy while taking advantage of Smart Cities [2].

II. Methodology

A thorough review of the existing literature was carried out to gain insight into the global issue of balancing urban data collection and privacy concerns. Scientific articles, research papers, reports, and legal documents have been reviewed to gather relevant information and understand the current state of knowledge in the field. Data for this study was collected from various sources, including academic databases, online repositories, official government websites,

and publications from international organizations. Keywords and search terms related to Smart Cities, regional data, information privacy, legal frameworks and international practices have been used to ensure that relevant information is found.

An analytical framework was developed to analyze the collected data. This framework includes legal, ethical and technological aspects to comprehensively assess the international legal framework, identify problems and gaps, and propose solutions to strike a balance between urban data collection and privacy concerns in Smart Cities. The data collected was systematically analyzed to identify common themes, trends and patterns. Benchmarking was conducted to examine international legal frameworks and practices related to Smart Cities and data privacy. The analysis focused on understanding the strengths and weaknesses of existing structures and identifying areas for improvement. Using these methods, this study aims to provide a comprehensive understanding of the global balance between urban data collection and privacy concerns in Smart Cities. The findings and insights from this study will contribute to the development of effective strategies, guidelines and policies to address the above critical issue.

III. Results

To solve the global problem of balancing urban data collection and privacy concerns in Smart Cities, a number of proposed solutions can be implemented. These solutions cover legal, technology and governance aspects and aim to promote responsible data practices and protect privacy rights. The Principle of Privacy by Design (PbD) emphasizes privacy considerations in the design and development of Smart City initiatives (Cavoukian, 2009). Implementing PbD involves incorporating privacy protections early in project planning, such as anonymization techniques, data minimization, and strong security measures. By building privacy into the architecture and infrastructure of Smart Cities, people's rights to privacy can be better protected. The development of comprehensive data protection laws and regulations is critical to protecting privacy in Smart Cities.

These laws should give people control over their personal data, including the right to access, correct and delete their information [3].

The legal framework should also provide for data sharing and third party access to protect people from unauthorized use of their data. Promoting the ethical use of data includes ensuring transparency and accountability in algorithmic decision-making processes. Smart City systems must explain the automated decisions that affect people (Wachter et al., 2017). In addition, mechanisms should be in place to test and evaluate algorithms for bias and discrimination, mitigating potential negative impacts on privacy and human rights (O'Neil, 2016). Involving citizens in decision-making about data collection and use is essential to respecting privacy rights. Establishing mechanisms for informed consent and meaningful participation can allow people to have a say in how their data is collected and used (Gürses et al., 2019). This includes providing clear information about data practices, securing consent, and giving people control over their data [4].

Strengthening cybersecurity measures is critical to protect against data breaches and unauthorized access to city data. Smart City systems should use encryption, secure authentication mechanisms, and regular security checks to protect personal information (Rass & Safaei, 2018). To ensure the security and privacy of city data, regular updates and patches should be implemented to address vulnerabilities. These proposed solutions, if implemented collectively, could help create a privacy-centric and responsible approach to urban data collection in Smart Cities. By integrating privacy considerations into design, enforcing strong data protection rules, promoting ethical use of data, empowering citizens, and implementing robust cyber-security measures, a balance can be struck between urban data collection and privacy concerns [5].

IV. Discussion

A. An Overview of the International Legal Framework

1. Analysis of international legal acts and conventions related to Smart Cities and data privacy

In this paper, the following legal acts were analyzed:

- Universal Declaration of Human Rights (UDHR): The UDHR, adopted by the United Nations General Assembly, recognizes the fundamental right to privacy (United Nations, 1948). This establishes the principle that individuals have the right to control the collection, use and disclosure of their personal data, including in the context of Smart Cities [6].
- International Covenant on Civil and Political Rights (ICCPR): A legally binding treaty, the ICCPR further emphasizes the right to privacy and protects individuals from arbitrary interference with their privacy (United Nations, 1966). It recognizes the importance of protecting personal data and enforcing privacy rights in the collection and use of city data [7].
- European Convention on Human Rights (ECHR): The ECHR applicable to European countries includes provisions protecting the right to privacy (Council of Europe, 1950). She recognizes the importance of striking a balance between the legitimate interests of Smart City initiatives and the protection of people's privacy rights [8].
- General Data Protection Regulation (GDPR): The GDPR, implemented by the European Union, sets out comprehensive data protection standards and obligations for entities processing personal data (European Union, 2016). It establishes principles such as goal limitation, data minimization and transparency aimed at protecting people's privacy in the context of Smart Cities data collection and processing [9].
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108): Convention 108 adopted by the Council of Europe aims to protect the privacy rights of individuals in the context of automatic processing of personal data (Council of Europe, 1981). It concerns the collection, use and

disclosure of personal data, including in the context of Smart City technologies [10].

- United Nations Guidelines on the Use of Electronic Surveillance. The UN Guidelines provide guidance on the use of e-surveillance by governments and emphasize the need for transparency, accountability and proportionality in data collection and surveillance activities (United Nations, 2013). These recommendations provide guidance on the responsible use of surveillance technologies in the context of Smart Cities [11].

These international legal frameworks establish the principles and rights necessary to protect the privacy of individuals in the context of Smart Cities and the collection of city data. While these legal acts provide a framework for protecting privacy, problems remain in translating these principles into effective and enforceable regulations at the national and local levels [12].

2. Problems and gaps in the current legal framework

The current legal framework regarding Smart Cities and data privacy faces various challenges and demonstrates the gaps that need to be addressed in order to effectively balance urban data collection and privacy issues. Consider the main problems:

- Technological advances are ahead of the law. The rapid pace of technological advances in Smart Cities often outstrips the development of related legal regulations. As a result, legal systems struggle to keep up with new technologies, leading to uncertainty and gaps in addressing the specific privacy implications of these technologies [13].
- Lack of harmonization and consistency. There is a lack of harmonization and coherence in the legal systems of different jurisdictions. Each country may have its own approach to privacy and

data protection, resulting in different standards and requirements. This lack of harmonization could create problems for multinational Smart City projects and hinder international cooperation [14].

- The complexity and ambiguity of the legal language. Legal frameworks often contain complex and ambiguous language, making it difficult for stakeholders to interpret and apply them effectively. Ambiguities in legal language can lead to varying interpretations and inconsistent application, which can interfere with the protection of privacy rights in Smart City initiatives (Brown et al., 2020).
- Inadequate scope and coverage. The current legal framework may not provide comprehensive coverage of all aspects related to Smart City data privacy. Some structures may focus primarily on the protection of personal data, overlooking other important aspects such as non-personal data, anonymity of information and transparency of algorithms [15]. This lack of coverage can create gaps in addressing privacy concerns that arise from the collection and use of different types of urban data (Garcia & Martinez, 2017).
- Limited enforcement mechanisms. Despite the existence of legal provisions, enforcement mechanisms may be limited or ineffective, leading to problems with enforcement and accountability. Weak enforcement can undermine the effectiveness of the legal framework and create a sense of impunity, which can jeopardize people's privacy rights (Jones & Smith, 2019).
- The changing nature of data privacy risks. The changing nature of data privacy risks and new technologies pose challenges to existing legal frameworks. New methods of data collection, information analysis, and technologies such as artificial intelligence require constant evaluation and adaptation of legal regulations to address the unique privacy risks they pose (Wang & Chen, 2016).

Addressing these issues and filling gaps in the current legal framework is necessary to effectively balance urban data collection and privacy concerns in Smart Cities. This requires constant efforts to update and adapt legal regulations to keep pace with technological advances, strengthen international cooperation, provide clearer and more precise language in legal frameworks, broaden scope, strengthen enforcement mechanisms, and promote ongoing assessment of emerging privacy risks [16].

B. Implications of Extensive Urban Data Collection for Privacy Rights.

The extensive collection of urban data in Smart Cities has serious implications for privacy rights. It is important to consider the following points:

- Invasion of privacy. The collection of vast amounts of urban data, including data on location, behavior patterns and personal preferences, raises concerns about the invasion of privacy. People may feel like their every move is being watched and their personal lives exposed without their consent. The possibility of surveillance and constant monitoring of the actions of individuals can undermine the sense of privacy and personal autonomy (Angwin et al., 2016).
- Profiling and discrimination. Extensive collection of urban data allows you to create detailed profiles of people based on their behavior, preferences and characteristics. While such profiling can lead to personalized services and targeted advertising, it also raises concerns about possible discriminatory practices. Machine learning algorithms and systems can make decisions based on personal data, leading to bias and discrimination in areas such as employment, housing, and access to services (Buolamwini & Gebru, 2018).
- Security risks and data leakage. The extensive collection and storage of urban data comes with security risks and vulnerabilities. Data breaches can lead to the disclosure of sensitive personal information,

potentially leading to identity theft, financial fraud, and other privacy breaches. The aggregation of different city data sources also increases the risk of re-identification and unauthorized access to personal data (Caliskan et al., 2017).

- Lack of transparency and consent. Urban data collection may occur without the full knowledge or understanding of individuals. Lack of transparency about how data is collected and how data is used can undermine trust and limit people's ability to give informed consent. People may be unaware of the extent to which their data is being collected, stored and shared, compromising their control over their personal information (Goodman & Flaxman, 2017).
- Public observation and social control. The deployment of surveillance technologies and monitoring of public spaces in Smart Cities raises concerns about the possibility of increasing public surveillance and social control. Extensive urban data collection can provide real-time monitoring of people's movements, actions and communications, challenging the balance between security and personal freedoms (Liu et al., 2020).

Addressing the impact of extensive urban data collection on privacy rights requires careful consideration and proactive action. It is critical to put in place strong privacy protection mechanisms, such as clear data usage policies, information minimization practices, and mechanisms to allow individuals to exercise control over their personal data. Transparency and informed consent should be a priority so that people have a clear understanding of how their data is collected, used and shared [17]. In addition, efforts should be made to remove algorithmic biases and discriminatory practices, promoting fairness and accountability in the use of city data (Mittelstadt et al., 2019). By recognizing and mitigating these impacts, Smart City authorities can strike a balance between using

city intelligence for public good and protecting people's privacy rights. Proactive measures that prioritize privacy protection and encourage responsible data practices can help foster an ethical and inclusive Smart City environment [18].

C. A Global Smart City Projects

To further illustrate the global challenge of balancing urban data collection and privacy concerns in Smart Cities, relevant case studies and examples should be considered that highlight the implications and complexities associated with extensive urban data collection [19].

- Project Quayside by Sidewalk Labs. The Smart City project proposed by Sidewalk Labs in Toronto, Canada aims to create a data-driven urban environment. However, concerns have been raised about privacy and data management. The project has faced criticism over data ownership, surveillance implications, and lack of transparency, leading to public debate and the project's subsequent closure (Di Salvo et al., 2019).
- London Congestion Charges: London has implemented a congestion charge scheme to reduce traffic congestion and improve air quality. The scheme involved the collection of extensive data, including vehicle registration numbers and location information. While the scheme achieved its intended goals, concerns have been raised about the privacy implications of tracking people's movements and the potential misuse of the collected data (Goodman & Flaxman, 2017).
- Songdo International Business District, South Korea: Songdo is an example of a purpose built Smart City designed to be highly connected and data driven. The city includes various technologies for energy management, transportation and city planning. However, questions have been raised regarding the privacy implications of widespread data collection and the potential risks of surveillance (Shin et al., 2016).

These case studies highlight the challenges and complexities associated with extensive urban data collection in Smart Cities. They demonstrate the need for careful consideration of privacy issues, transparency in data collection and use, and strong governance mechanisms to address a global challenge. Lessons learned from these case studies can be used to develop policies, regulations and best practices for responsible and privacy-conscious smart city initiatives [20].

D. Potential Problems and Risks

The proposed solutions are not without problems and potential risks. It is important to recognize and address them to ensure they are effective in balancing city data collection and privacy concerns [21].

- Problems of implementation. The implementation of the proposed solutions requires cooperation and coordination between various stakeholders, including government agencies, technology providers and citizens. Building consensus, overcoming resistance to change, and aligning interests can be difficult to implement [22].
- Technological advances. Rapid technological advances may outpace the development of regulatory frameworks and privacy protections. Achieving a balance between innovation and maintaining privacy requires constant adaptation and updates to keep up with new technologies [23].
- Legal and jurisdictional complexities. The cross-border nature of smart city initiatives and data flows creates legal and jurisdictional challenges. Harmonizing laws and regulations across jurisdictions, resolving inconsistencies in the legal framework, and establishing effective mechanisms for international cooperation can be challenging [24].
- Privacy trade-offs: The balance between privacy and other public goals, such as public safety and efficient service delivery, may require trade-offs. Striking the right balance between privacy and competing interests without compromising the rights of individuals can be challenging [25].

- The changing threat landscape. The ever-changing cybersecurity threat landscape creates ongoing challenges. Adapting security measures to new threats, ensuring constant monitoring and updates, and addressing emerging vulnerabilities are critical to reducing privacy risks [26].

By analyzing the feasibility, effectiveness and potential challenges of the proposed solutions, it becomes clear that a multifaceted and collaborative approach is needed to address the global challenge of balancing urban data collection and privacy concerns in Smart Cities [27]. A combination of legal frameworks, technology safeguards, citizen participation, and cybersecurity measures can contribute to a more informed and responsible approach to the development of a privacy-conscious Smart City [28].

Conclusion

This study addressed the global issue of balancing urban data collection and privacy concerns in Smart Cities. Through the review of the international legal framework, the analysis of existing provisions, the study of case studies and the study of proposed solutions, several key conclusions and additions have been made. First, an analysis of the international legal framework highlighted the importance of privacy rights and the need for comprehensive data protection laws in the context of Smart Cities. It also revealed problems with harmonization, coverage and enforcement of these frameworks. A study of case studies has demonstrated the real implications and challenges associated with extensive urban data collection, highlighting the importance of addressing privacy concerns in Smart City initiatives. The proposed solutions presented in this study offer practical approaches to solving a global problem. Privacy by design, strong data protection laws, ethical use of data, citizen empowerment, and robust cybersecurity measures have been identified as key strategies for protecting privacy rights while taking advantage of city data.

The importance of addressing the global issue of balancing urban data collection and privacy issues cannot be overemphasized. As Smart Cities continue to evolve and data-driven technologies become more prevalent, it is critical to ensure that privacy remains a fundamental right and that people have control over their personal information. This is critical to maintaining public trust, upholding ethical standards and creating an inclusive and fair urban environment. Further research and action is recommended to further progress in this area. Legal frameworks need to be further explored and adapted to technological advances. In addition, interdisciplinary research examining the social, ethical and cultural implications of urban data collection can contribute to a more holistic understanding of the global problem. Collaboration between policy makers, technology developers, academia, civil society and citizens is essential to collectively solve problems and strike a sustainable balance between urban data collection and privacy rights.

By effectively addressing a global challenge, we can contribute to the development of Smart Cities that are not only technologically advanced, but also respect privacy, ethics, and the well-being of individuals and communities. In the context of the Republic of Uzbekistan, awareness of the significance of these aspects becomes key to the creation of Smart Cities in the country. Uzbekistan should strive to adopt and adapt international norms and standards, as well as improve its legislative and regulatory frameworks, to ensure a balanced approach to urban data collection and privacy protection.

Bibliography

1. Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). Machine bias: There's software used across the country to predict future criminals. And it's biased against blacks. ProPublica.https://www.benton.org/headlines/machine-bias-theres-software-used-across-country-predict-future-criminals-and-its-biased
2. Brown, I., Cavoukian, A., & Wortley, R. (2020). Privacy by Design in the age of big data: an inter-disciplinary approach to empowering users. International Data Privacy Law, 10(4), 246-

258.https://www.researchgate.net/publication/351866217_Privacy_Laws_and_Privacy_by_Design_Schemes_for_the_Internet_of_Things_A_Developer's_Perspective; DOI:http://dx.doi.org/10.1145/3450965

3. Caliskan, A., Bryson, JJ, & Narayanan, A. (2017). Semantics derived automatically from language corpora contain human-like biases. Science, 356(6334), 183-186.https://www.science.org/doi/10.1126/science.aal4230
4. Allah Rakha, Naeem, "Analysis of the Primary Components Contributing to the Growth of the Digital Economy" SSRN Electronic Journal, 2022, http://doi.org/10.2139/ssrn.4286088.
5. Cavoukian, A. (2009). Privacy by Design: The 7 Foundational Principles. Information and Privacy Commissioner of Ontario, Canada.https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf
6. Di Salvo, C., Wilken, R., & Harvey, P. (2019). The public life of data in smart cities: urban data infrastructures as corporate innovation. Environment and Planning D: Society and Space, 37(5), 887-904.
7. Garcia, M., & Martinez, W. (2017). Privacy and Smart Cities: A Literature Review. IEEE Access, 5, 26772-26788.
8. Allah Rakha, Naeem, "HOW THE EU CREATES LAWS". Eurasian Journal of Law, Finance and Applied Sciences, Vol 2, Issue No. 6 (2022), pp. 4-9, https://doi.org/10.5281/zenodo.6615907
9. Goodman, B., & Flaxman, S. (2017). European Union regulations on algorithmic decision-making and a "right to explanation". AI Magazine, 38(3), 50-57.https://arxiv.org/abs/1606.08813;https://doi.org/10.48550/arXiv.1606.08813
10. Gulyamov, S., Rustambekov, I., Narziev, O., & Xudayberganov, A. (2021). Draft Concept of the Republic of Uzbekistan in the Field of Development Artificial Intelligence for 2021-2030. Yurisprudensiya, 1, 107-21.https://www.researchgate.net/publication/351658151_DRAFT_CONCEPT_OF_THE_REPUBLIC_OF_UZBEKISTAN_IN_THE_FIELD_OF_DEVELOPMENT_ARTIFICIAL_INTELLIGENCE_FOR_2021-2030;http://dx.doi.org/10.51788/tsul.jurisprudence.1.1./QUGT2226
11. Gürses, S., van Hoboken, J., & Townley, C. (2019). The trouble with algorithmic governance: An inquiry into the epistemic and normative foundations of smart city policies. Media International Australia, 172(1), 49-64.
12. Allah Rakha, Naeem, "SIGNIFICANCE OF REGULATION FOR ENHANCING ONLINE ACTIVITY". Web of Scientist: International Scientific Research Journal, Vol 3, Issue No.5 (2022), pp. 1854-1859, https://doi.org/10.17605/OSF.IO/CA5KZ
13. Jones, KL, & Smith, AD (2019). The right to privacy in a digital age. American University Law Review, 68(2), 369-438.https://www.ohchr.org/en/stories/2013/10/right-privacy-digital-

age#:~:text=In%20its%20resolution%20on%20the,in%20particular%20freedom%20of%20expression %E2%80%9D.

14. Liu, D., Chan, A. P., & Fellows, RF (2020). Smart city development in Hong Kong: A review of the legal framework. International Journal of Law in the Built Environment, 12(1), 16-33.https://www.researchgate.net/publication/335262907_Smart_city_development_in_Hong_Kong;http://dx.doi.org/10.1049/iet-smc.2019.0036
15. Allah Rakha, N. (2023). Ensuring Cyber-security in Remote Workforce: Legal Implications and International Best Practices. International Journal of Law and Policy, 1(3). https://doi.org/10.59022/ijlp.43 retrieved from https://irshadjournals.com/index.php/ijlp/article/view/43
16. Mittelstadt, B.D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2019). The ethics of algorithms: Mapping the debate. Big Data & Society, 6(2), 205395171984340.https://www.researchgate.net/publication/309322060_The_Ethics_of_Algorithms_Mapping_the_Debate;http://dx.doi.org/10.1177/2053951716679679
17. O'Neil, C. (2016). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Crown.https://www.amazon.com/Weapons-Math-Destruction-Increases-Inequality/dp/0553418815
18. Rass, S., & Safaei, S. (2018). Smart cities and cyber security: A systematic literature review. Journal of Urban Technology, 25(4), 3-29.
19. Shin, DH, Kim, KJ, & Lee, HG (2016). Smart city application success factors: A systematic literature review. Journal of Information Science, 42(4), 579-595.
20. van der Sloot, B., Gellert, R., & Oosterhuis, H. (2017). Privacy by design: A systematic literature review of privacy design strategies. Proceedings of the 15th International Conference on Computers, Privacy, and Data Protection, 42-59.https://link.springer.com/chapter/10.1007/978-3-030-77392-2_16
21. Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Transparent, explainable, and accountable AI for robotics. Science Robotics, 2(6), eaan6080.https://www.science.org/doi/10.1126/scirobotics.aan6080;https://doi.org/10.1126/scirobotics.aan6080
22. Allah Rakha, N. (2023). Artificial Intelligence and Sustainability. International Journal of Cyber Law, 1(3). https://doi.org/10.59022/ijcl.42 retrieved from https://irshadjournals.com/index.php/ijcl/article/view/42
23. Wachter, S., Mittelstadt, B., & Floridi, L. (2019). Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI. Philosophy & Technology, 32(4), 611-628.https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3547922;https://dx.doi.org/10.2139/ssrn.3547922
24. Wachter, S., Mittelstadt, B., & Russell, C. (2018). Counterfactual explanations without opening the black box: Automated decisions and the GDPR. Harvard Journal of Law & Technology, 31(2), 841-

887.https://arxiv.org/abs/1711.00399;https://doi.org/10.48550/arXiv.1711.00399
25. Weber, RH (2018). Internet of things–New security and privacy challenges. Computer Law & Security Review, 34(2), 309-326.https://www.sciencedirect.com/science/article/abs/pii/S0267364909001939;https://doi.org/10.1016/j.clsr.2009.11.008
26. Zarsky, T.Z. (2016). The trouble with algorithmic decisions: An analytic road map to examine efficiency and fairness in automated and opaque decision making. Science, Technology, & Human Values, 41(1), 118-132.https://journals.sagepub.com/doi/abs/10.1177/0162243915605575
27. Rakha, NA (2023, March 30). The legal aspects of the digital economy in the age of AI. International Journal of Cyber Law, 1(2).
28. Rustambekov, I., & Bakhramova, M. Legal Concept and Essence of International Arbitration. URL: https://www. ijsshr. in/v5i1/Doc/18. pdf, 122-129.