

Protection of Personal Data In "Mystery Shopper" Operations: Human Rights Proportionality

 Davlatov Bahodir Akbar o'gli

Doctoral student, Academy of Law Enforcement, Uzbekistan

Received: 26 Mar 2026 | Received Revised Version: 22 April 2026 | Accepted: 04 May 2026 | Published: 31 May 2026

Volume 08 Issue 05 2026 | Crossref DOI: [10.37547/tajpslc/Volume08Issue05-09](https://doi.org/10.37547/tajpslc/Volume08Issue05-09)

Abstract

This article analyzes issues of personal data protection and human rights proportionality in the context of the "mystery shopper" method. The application of this method in the digital age creates new legal challenges. The legal framework for collecting, storing, and using personal data in mystery shopper operations is analyzed in the context of foreign experience and Uzbekistan legislation, with relevant proposals and recommendations developed.

Keywords: Mystery shopper, personal data, human rights, anti-corruption, digital era, principle of proportionality, data protection.

© 2026 Davlatov Bahodir Akbar o'gli. This work is licensed under a Creative Commons Attribution 4.0 International License (CC BY 4.0). The authors retain copyright and allow others to share, adapt, or redistribute the work with proper attribution.

Cite This Article: Davlatov Bahodir Akbar o'gli. (2026). Protection of Personal Data In "Mystery Shopper" Operations: Human Rights Proportionality. *The American Journal of Political Science Law and Criminology*, 8(05), 48–51. <https://doi.org/10.37547/tajpslc/Volume08Issue05-09>

1. Introduction

The "mystery shopper" (mystery shopper) institution is widely used in world practice as one of the effective methods of combating corruption. This method serves to identify unlawful actions of civil servants during service delivery, and to expose bribery and other corrupt behaviors.

However, with the rapid development of digital technologies, "mystery shopper" operations have become increasingly complex, collecting ever more data. These operations, carried out with the help of hidden video cameras, audio recordings, hidden cameras, and biometric data, are effective in identifying corruption on one hand, but on the other hand pose serious threats to citizens' personal lives and rights to data protection.

The theme of the international conference — "Ensuring the Rule of Law in the Digital Age: Innovation, Human Rights and Security Proportionality" — requires illuminating precisely this contentious issue. This article analyzes the legal mechanisms for ensuring proportionality between personal data protection and human rights in "mystery shopper" operations.

2. The "Mystery Shopper" Institution And The Personal Data Problem

2.1. The Nature of the "Mystery Shopper" Method and Digital Transformation

"Mystery shopper" is a method whereby a specially trained person visits a service point in the guise of an ordinary customer and covertly observes and records the behavior of the employee or official. While in its

traditional form this method was based on the personal memory and written report of the observing agent, the digital age has fundamentally transformed it .

Today, "mystery shopper" operations use the following digital tools: hidden video cameras and microphones; GPS trackers; mobile applications on smartphones; artificial intelligence-based analytical systems; biometric data recording technologies. These tools increase the effectiveness of operations, but at the same time create the risk of mass collection of personal data.

2.2. Classification of Collected Data and Legal Problems

The data collected in "mystery shopper" operations can be divided into three main groups.

The first group — data of the operation subject (the official being inspected): photographs, video clips, voice recordings, actions within the scope of official authority. This data constitutes the main targeted object of the operation.

The second group — data of incidentally encountered third parties: other customers, employees, or persons who fall within the range of surveillance equipment. These individuals are unaware of the operation and have not consented to the collection of their data.

The third group — the "mystery shopper's" own data: the agent is also exposed to the risk of being observed or identified during the operation, which raises the issue of ensuring their safety.

The core of the legal problem is connected with the question of whether the actions of an official within the scope of their duties can be recognized as public information, or whether they should be protected as the individual's private data. This issue has found different solutions in each legal system.

3. International Legal Standards and Foreign Experience

3.1. International Normative Framework

According to Article 12 of the Universal Declaration of Human Rights, no one shall be subjected to arbitrary interference with their privacy, family, home or correspondence, nor to attacks upon their honor and reputation. This norm establishes important limitations in "mystery shopper" operations against officials as well.

Article 8 of the European Convention on Human Rights

guarantees the right to respect for private life and stipulates that state interference is permissible only when "necessary" — that is, on the basis of the principle of proportionality. The EU General Data Protection Regulation (GDPR) 2016/679 is considered the most modern and comprehensive normative instrument in this field.

Applying GDPR principles to "mystery shopper" operations gives rise to the following requirements: existence of a lawful basis; purpose limitation in data collection; data minimisation; accuracy; storage limitation; and integrity and confidentiality.

3.2. Experience of Foreign States

German Experience.

In Germany, "mystery shopper" operations are regulated on the basis of the Federal Data Protection Act (BDSG) and GDPR rules. According to the practice of Bundesgerichtshof (BGH) courts, the admissibility of covert surveillance results as evidence requires verification of their conformity with the provisions of the Grundgesetz (Constitution) concerning personal inviolability.

US Experience.

In the US, alongside federal data protection legislation (Electronic Communications Privacy Act, Privacy Act), there are specific standards for conducting "mystery shopper" oversight of government authorities. Ombudsmen and inspection offices actively use this method for anti-corruption purposes.

The experience of Northern European countries (Denmark, Sweden, Norway) shows that these states have developed a clear and comprehensive legal basis for "mystery shopper" operations, agents are pre-certified by authorized bodies, and an independent audit of collected data is conducted.

4. The Principle of Proportionality: Analysis and Criteria

4.1. The Content of the Principle of Proportionality

The principle of proportionality is one of the fundamental postulates of modern legal philosophy, requiring that a reasonable ratio be established between state coercive measures and their outcomes. In the practice of the Court of Justice of the European Union, proportionality is assessed through three criteria:

suitability of the measure; necessity of the measure — i.e., the absence of other, less restrictive methods; and the benefits of the measure outweighing its harm (proportionality *stricto sensu*).

Applying these criteria to "mystery shopper" operations shows that: first, the method is suitable for identifying corruption; second, in some cases less invasive methods (such as documentary oversight) also exist; third, the volume and scope of collected data must be proportionate to the specific objective.

4.2. Anti-Corruption and Privacy

On one hand, there is the state's obligation to effectively combat corruption (UN Convention Against Corruption, Article 5). On the other hand, every person's right to private life, confidential personal data, and protection is guaranteed by the constitutions of all democratic states in the world.

In resolving this contradiction, the principle of fair balance applies: surveillance data must be collected only as proof of corruption, using the least invasive method of documentation; data of third parties must be promptly deleted; access to collected data must be limited; and independent oversight must be established.

5. Proposals And Recommendations For Improving Uzbekistan Legislation

5.1. Analysis of the Current Legal Framework

In Uzbekistan, the legal framework related to the "mystery shopper" institution is still in the process of being formed. The Law on Personal Data adopted in 2019 establishes general norms, but the issue of personal data in "mystery shopper" operations is not clearly regulated. The Law on Combating Corruption (2017) and relevant norms of the Civil Code exist, but they need to be adapted to digital "mystery shopper" operations.

5.2. Proposed Reforms

In the legislative sphere:

It is necessary to develop a separate normative document on the procedure for conducting "mystery shopper" operations, the volume of collected data, and their protection; to introduce a mechanism for obtaining an independent judicial sanction for conducting operations; and to establish an obligation to automatically delete third-party data.

In the institutional sphere:

It would be appropriate to grant the Anti-Corruption Agency powers of prior oversight of "mystery shopper" operations; to organize training seminars and webinars for "mystery shoppers", and conduct mandatory data protection training for employees of authorized bodies; and to introduce a system for auditing the use of operation results.

In the technological sphere:

It is proposed to register covert surveillance equipment in a state registry; to establish standards for encrypting and digitally sealing collected data; and to apply the chain of custody principle to operations.

6. Conclusion

The "mystery shopper" institution continues to be an effective tool for combating corruption. However, in the context of the digital age, the application of this method is giving rise to new and complex problems in the field of human rights and personal data protection.

Based on the foreign experience and international standards analyzed in this article, it was established that: the principle of proportionality is the central criterion for legally justifying "mystery shopper" operations; the volume of collected data must not exceed the specific objective of the operation; the protection of third parties' rights requires special guarantees; and independent oversight mechanisms ensure the legitimacy of the institution.

For Uzbekistan, adapting the "mystery shopper" institution to the requirements of the digital age will, on one hand, increase the effectiveness of the fight against corruption, and on the other, preserve the primacy of human rights. This is an important condition for implementing the rule of law principle in digital public administration.

References

1. UN Convention Against Corruption (UNCAC), 2003.
2. EU General Data Protection Regulation (GDPR), 2016/679.
3. Universal Declaration of Human Rights, 1948, Article 12.
4. European Convention on Human Rights, 1950, Article 8.
5. Law of the Republic of Uzbekistan on Personal Data, 2019.

6. Law of the Republic of Uzbekistan on Combating Corruption, 2017.
7. Transparency International. (2023). *Mystery Shopper Methodology in Anti-Corruption Monitoring*. Berlin.
8. European Data Protection Board. (2022). *Guidelines on Personal Data Protection in Investigative Operations*. Brussels.
9. OECD. (2021). *Digital Government and Anti-Corruption: Leveraging Technology for Integrity*. Paris.
10. Bundesdatenschutzgesetz (BDSG), Germany, 2018.
11. Investigatory Powers Act 2016, United Kingdom.
12. Nikiforov, A. (2022). *Mystery Shopping as a Tool of Anti-Corruption Policy: Comparative Analysis*. // *Journal of Public Administration*, Vol. 14, № 2. pp. 45–67.
13. Solove, D.J. (2008). *Understanding Privacy*. Harvard University Press.
14. Bennett, C.J., Raab, C.D. (2020). *The Governance of Privacy: Policy Instruments in Global Perspective*. MIT Press.
15. Finn, A., & Kayandé, U. (1999). *Unveiling a mystery: Mystery shopping concerning the service effort*. *Journal of Retailing*, 75(2), 195–217.