Luka Pavlenishvili*

Supervision and Control of Covert Investigative Actions by the Personal Data Protection Service of Georgia

The article examines the legality and oversight of personal data processing in the context of covert investigative activities, with a focus on evaluating the effectiveness and alignment of the current control mechanisms with international standards.

Specifically, the article assesses the mandate and authority of the Personal Data Protection Service (hereafter - PDPS) in supervising and regulating such activities. This issue has gained particular significance following the enactment of Georgia's new law "On Personal Data Protection," which granted the PDPS the authority to assess the legality of data processing classified as a state secret.

***Keywords**: personal data, covert investigative activities, oversight mechanisms, Criminal Procedure Code, Law of Georgia "On Personal Data Protection".*

1. Introduction

In the digital age, where individuals leave a pervasive digital footprint, the assessment of the legality of data processing in specific cases often falls outside the strict boundaries of legal regulation. Particular attention is warranted when it comes to covert investigative activities, especially given their association with the investigation of serious or particularly serious crimes. Such investigative actions frequently involve the processing of large volumes of diverse types of data, necessitating strict compliance with both criminal procedural law and personal data protection legislation. In these cases, adherence to the principle of data minimization is crucial.

The principle of data minimization in the context of covert investigations extends beyond being a mere organizational, technical, or procedural issue;

It is important to note that while the control of covert investigative activities is not governed by the General Data Protection Regulation (GDPR), it is regulated by the Law Enforcement Directive (LED), which sets specific rules for the processing of personal data within the police and law enforcement sector. The newly enacted law "On Personal Data Protection" of Georgia, which came into force on March 1, 2024, is largely aligned with international standards, including those set forth by the LED.

The LED outlines key principles for the processing of personal data in the context of preventing, investigating, detecting, or prosecuting criminal offenses by law enforcement

* Master's Student at Ilia State University, Faculty of Law (Criminal Law). Junior Lawyer at the Legal Department of the Personal Data Protection Service of Georgia.

agencies. These principles include legality, fairness, transparency, respect for human dignity, processing for a specifically defined and legitimate purpose, data minimization, data accuracy, limited retention periods, and robust data security measures. These guidelines ensure that investigative data processing operations are necessary, proportionate, and conducted in a manner that upholds individuals' rights and freedoms.[1]

The purpose of this study is to examine the legal framework governing the oversight of covert investigative activities. The study will explore the principle of data minimization, along with best practices and methodologies that are of particular relevance following the implementation of Georgia's new law "On Personal Data Protection." Emphasis will be placed on the role of law enforcement agencies in balancing their operational needs with the protection of fundamental rights and freedoms in a democratic society.

2. Legal framework for Conducting Covert Investigative Action

The legal framework governing the interaction between covert investigative actions conducted by law enforcement agencies and the protection of personal data is inherently complex. Harmonizing this process with the law presents significant challenges, yet it is essential for safeguarding the fundamental human right to privacy.

Covert investigative actions, or operational-search measures, serve as an Ultima Ratio, allowing for the collection of evidence through various methods or techniques, naturally without prior notification to the individuals involved.[2] These actions are carried out by the Operational-Technical Agency of the State Security Service and pertain to specific crimes investigated by the authorities outlined in Article 34(1) of the Criminal Procedure Code.[3]

Unlike other investigative measures, covert investigative actions are reserved for serious or particularly serious crimes, as well as certain offenses listed under Article 143^3(2)(a) of the Criminal Procedure Code. The crimes eligible for such investigative actions include, but are not limited to:

- Crimes against health;
- Threats to life and health;
- Crimes against sexual freedom and inviolability;
- Crimes against human rights and freedoms;
- Economic crimes;
- Crimes against entrepreneurial or other economic activities;
- Crimes within the monetary and credit system;
- Crimes against public health and morality;
- Cybercrime;
- Crimes against environmental protection and the use of natural resources;
- Crimes against the constitutional order and national security of Georgia;
- Violations of the legal regime in occupied territories;
- Official misconduct.

In addition to defining these investigative actions, it is essential to consider the legitimate objectives that warrant their use, namely:

[1] Article 4 of the Law Enforcement Directive (LED).
[2] *Akubardia I.,* Control mechanisms over secret investigative actions, collection of articles - Revaz Gogshelidze 65, Tbilisi, 2022, 200.
[3] Article 34(1) of the Criminal Procedure Code of Georgia.

- Ensuring national security;
- Ensuring public safety;
- Preventing public disorder;
- Preventing crime;
- Protecting the country's economic well-being;
- Protecting the rights and freedoms of others.

The scope and intensity of covert investigative actions must be proportionate to these legitimate goals, aligning with the general requirements of international human rights law, the jurisprudence of the European Court of Human Rights (ECtHR), and other international or regional legal standards.[4]

In line with the conclusions of the Legal Issues Committee on recent legislative amendments, the ECtHR has underscored the state's discretionary power in determining the duration of covert investigative actions. Extending the timeframe for such actions to achieve legitimate objectives, including public order protection and effective crime prevention, may be justified as long as necessary, provided there is appropriate oversight and due process guarantees.[5]

Any covert investigative action conducted for a legitimate purpose is intended to gather evidence relevant to a criminal case. However, the mere necessity of obtaining such evidence or preventing a crime is not, in itself, sufficient grounds for a court to authorize such measures. The requesting party must also demonstrate that obtaining the evidence or achieving the objective through other investigative or procedural means is either impossible or would require an unreasonable level of effort.[6]

The burden of proof to meet these standards lies with the state prosecutor, who petitions the court to authorize covert investigative actions. The prosecutor's request must be considered by the court within 24 hours, after which the judge decides whether to grant or deny the request. The judge's decision is issued in four copies: two for the prosecutor, one for the court, and one copy, containing only the operative details and resolution, is delivered to the PDPS in physical form within 48 hours.

Covert investigative actions may also be conducted under urgent circumstances, in which case the prosecutor must send one copy of the resolution to the PDPS.

3. Control Over Covert Investigative Actions and Activities Carried out in the Central Bank of Electronic Communication Identifying Data

3.1. Mandate of the Personal Data Protection Service

The oversight of the legality of personal data processing in Georgia dates back to 2013. With the legislative amendments introduced in 2014, the scope of the Law of Georgia on Personal Data Protection was expanded to cover the automatic processing of data classified

[4] *Fafiashvili L., Tumanishvili G*. and others, Commentary of Criminal Procedure Code Georgia (as of October 1, 2015), Tbilisi., 2015, 428-429.

[5] Conclusion of the Committee on Legal Issues "On Amendments to the Criminal Procedure Code of Georgia" on the Law of Georgia (No. 1614-VIIIms-Xmp, 7/06/2022) regarding the motivated remarks of the President of Georgia (No. 07-1/14, 23/06/2022).

[6] *Fafiashvili L., Tumanishvili G.* and others, Commentary of Criminal Procedure Code Georgia (as of October 1, 2015), Tbilisi., 2015, 429.

as state secrets for the purposes of crime prevention, investigation, operational-search measures, and law enforcement. At that time, the Personal Data Protection Inspector was granted the authority to oversee covert investigative actions, as well as the activities conducted within the data banks of law enforcement bodies. Following further legislative changes, effective from March 31, 2015, the Personal Data Protection Inspector was empowered to supervise investigative actions outlined in Articles 136-138 and subsections "a" and "b" of Article 143^1(1) of the Criminal Procedure Code of Georgia.[7]

From 2019 to 2022, these functions were assumed by the State Inspector Service, the successor of the Personal Data Protection Inspector.

As of March 1, 2022, the mandate for overseeing such activities was transferred to the PDPS. One of its core responsibilities is the supervision and enforcement of personal data protection regulations in Georgia, including the monitoring of the legality of data processing.

In any democratic state, it is essential to ensure the legality of covert investigative activities conducted by law enforcement agencies, particularly when processing personal data or accessing identifiable electronic communication data.

3.2. Oversight Mechanism

As previously noted, one of the key functions of PDPS is to oversee activities conducted within the central database of electronic communication identification data and covert investigative actions. This oversight can be viewed as a safeguard against abuse, given that covert investigative actions are inherently sensitive and may become a tool for severe infringements on fundamental rights, which the state itself is responsible for protecting.

PDPS supervises covert investigative actions as outlined in Article 143^1(1) of the Criminal Procedure Code of Georgia and ensures compliance with the provisions set forth in Chapter XVI^1 of the same Code. To fulfill its mandate, PDPS is granted 24-hour access to the essential information and portions of court rulings authorizing covert investigative activities. In cases of urgent necessity, it also receives the essential details and portions of prosecutor's resolutions authorizing covert investigative actions, along with protocols prepared by law enforcement agencies regarding such actions.

Additionally, PDPS receives notifications from electronic communications companies regarding the transfer of personally identifiable communication data to law enforcement agencies. Upon receiving this documentation, PDPS cross-references the information with electronic systems, records the relevant data in its internal system for documenting covert investigative actions, and conducts an analysis. Beyond these mechanisms, PDPS employs electronic and specialized control systems to monitor covert investigative activities—specifically, the covert monitoring and recording of telephone communications. An electronic control system is also used to oversee activities within the central database of electronic communication identification data.[8]

Furthermore, PDPS ensures the legality of data processing within the central database of electronic communication identification data through its control system, which includes conducting checks and inspections of the data processor or authorized individual responsible for data handling.[9]

[7] Office of the Personal Data Protection Inspector 2015 Report, 34.
[8] Activity statistics of the Personal Data Protection Service for 12 months of 2023 (January-December), 7.
[9] Law of Georgia "On Personal Data Protection", 14/06/2023, Article 49, subsection "c".

3.3. Statistical Information

It is noteworthy that, in an effort to establish uniform methodologies for producing statistical data within PDPS and to introduce relevant standards, a comprehensive methodology has been developed to summarize and analyze statistical data on the Service's activities.[10]

For example, PDPS's statistics from the previous year indicate that the mechanism for halting the covert monitoring and recording of telephone communications (via the electronic control system) was employed in 76 instances. These interruptions were due to the delayed submission of court decisions (74 cases), an illegal notification of covert investigative actions initiated by the prosecutor's resolution in urgent circumstances (1 case), and the termination of a covert investigative action (1 case).

Key data points include:

- Covert monitoring and recording of telephone communications: The court considered 859 petitions, of which 87% (744) were fully approved, 9% (80) were denied, and 4% (35) were partially approved.
- Extension of telephone communication surveillance and recording periods: The court reviewed 228 petitions, approving 87% (199), partially approving 9% (21), and rejecting 4% (8).
- Covert video and/or audio recording and photography: The court evaluated 1,024 motions, fully approving 93% (952), rejecting 6.6% (68), and partially approving 0.4% (4).
- Extension of covert video and/or audio recording and photography periods: The court reviewed 120 petitions, of which 87% (105) were approved, 11% (13) were rejected, and 2% (2) were partially approved.
- Removal and fixation of information from communication channels or computer systems: The court considered 3 petitions, approving 1 and rejecting 2.
- Collection of internet traffic data: The court reviewed and approved 1 petition for the ongoing collection of internet traffic data.
- Prosecutor's resolutions on urgent covert investigative actions: PDPS received 92 resolutions, of which 83% (76) were for covert video and/or audio recording and photography, and 17% (16) were for covert telephone communication monitoring and recording. Court rulings and prosecutor's resolutions under Article 136 of the Criminal Procedure Code: Of the documents submitted, 2% were prosecutors' resolutions and 98% were court decisions, totaling 1,490 court rulings. Additionally, PDPS received 34 prosecutor's resolutions regarding urgent investigative actions under Article 136.
- Notifications to the "Operational-Technical Agency of Georgia": PDPS notified the Agency 6 times regarding ambiguities or inaccuracies in court-issued permits for

[10] Methodology for production of annual statistics on the state of personal data protection, conduct of covert investigative actions and control of activity carried out in the central bank of electronic communication identifying data, 2024.

covert telephone communication monitoring and recording (via the electronic control system).

- Monitoring through the electronic control system: No incidents were detected during the covert monitoring and recording of telephone communications.
- Data issued by the Central Bank of Identifying Data of Electronic Communication: The Operational-Technical Agency issued data 71 times, based on relevant court decisions.
- Oversight of the Central Bank of Identifying Data of Electronic Communication: No errors or incidents were detected during the oversight of activities conducted within the Central Bank.[11]

The rise in these statistics, compared to previous reports, reflects the increased efficiency of PDPS and the strengthening of its mandate. This development is a positive step forward, as an area once beyond legal oversight has now come under regulatory supervision. Notably, the 2016 report highlighted that, in six cases, a copy of the resolution was not submitted to the supervisory body. The Chief Prosecutor's Office attributed this to time constraints and the high volume of investigative actions conducted in response to urgent needs. Additionally, in the same year, three instances of late submission of resolutions were identified.[12]

3.4. Destruction of Information Obtained through Covert Investigative Action

The information obtained from covert investigative actions is destroyed by the supervisor of the relevant case investigation, the state prosecution supporter, or their superior prosecutor. This process takes place in the presence of the judge who authorized the covert investigative action or, in cases of urgent necessity, the judge who retrospectively approved the action. The destruction of such information is conducted regardless of whether the investigative activity was deemed legal or illegal. A protocol documenting the destruction of the material, signed by the responsible prosecutor and judge, is then submitted to PDPS and recorded in the court's register of covert investigative actions.[13]

The Law Enforcement Directive (LED) provides an intriguing perspective on the destruction of information gathered during covert investigative activities. According to the LED, Member States must establish appropriate time limits for the deletion of personal data and periodically review the necessity of retaining such data. The enforcement of these time limits must be ensured through procedural safeguards, which can be seen as closely aligning with the Georgian model.

4. International Standards

4.1. Regulatory Bodies

During the conduct of covert investigative actions, the subject of such actions is granted the opportunity to fully protect their rights only after the conclusion of the covert operation.

[11] Activity statistics of the Personal Data Protection Service for 12 months of 2023 (January-December), 9.

[12] 2016 report on the state of personal data protection and inspector's activities, <https://old.pdps.ge/ka/download/2870> [05.08.2024].

[13] *Akubardia I.,* Control mechanisms over secret investigative actions, collection of articles - Revaz Gogshelidze 65, Tbilisi, 2022, 228.

Therefore, it is crucial to monitor the actions of the executing body during the course of the operation. Proper oversight before notifying the subject of the investigative actions serves as the sole legal safeguard protecting individuals and third parties from potential abuse of power.

Surveillance and other covert measures are typically carried out by national security services. In Georgia, for instance, the Operational-Technical Agency operates under the State Security Service. The supervisory authorities overseeing the activities of security services vary across countries. Research documents from international bodies such as the United Nations, Council of Europe, and Venice Commission outline best practices and provide key recommendations for the establishment and effective operation of supervisory institutions.

According to a 2015 research report by the Council of Europe, no member state's supervisory system fully adheres to internationally recognized standards and principles. There is also no universally accepted model for effective oversight. However, certain practices and approaches stand out from a human rights perspective.[14] The report highlights that, within Council of Europe member states, the supervisory authorities for security services include parliamentary committees, independent supervisory institutions, courts, and quasi-judicial bodies.

4.2. Practice of the European Court of Human Rights

a. Roman Zakharov and Others v. Russia[15]

The applicant, who was the editor-in-chief of a publishing company, initiated legal proceedings against three mobile network operators, alleging interference with his right to privacy in telephone communications. He claimed that under the applicable national legislation, mobile network operators had installed equipment that allowed the Federal Security Service (FSB) to monitor telephone communications without prior judicial authorization. The applicant sought to have the equipment removed and to restrict access to telecommunications to authorized individuals only.

The national courts rejected the applicant's request, ruling that he had not provided sufficient proof that his telephone conversations had been monitored or that the mobile network operators had shared information with unauthorized parties. The court further found that the mere installation of the system or equipment did not in itself constitute a violation of the security of his communications.

Before the European Court of Human Rights, the applicant contended that Russia's system of secret surveillance of mobile phone communications did not comply with the requirements set forth in Article 8 of the European Convention on Human Rights. On 11 March 2014, the Trial Chamber relinquished jurisdiction in favor of the Grand Chamber.

In this case, the challenged legislation had a direct impact on all mobile phone service users, as it established a covert surveillance system where anyone using a national carrier's mobile service could be subject to surveillance without ever being informed. Moreover, national legislation failed to provide effective protection for individuals suspected of being

[14] Council of Europe Commissioner for Human Rights, Democratic and Effective Oversight of National Security Services, 2015, 8, <https://rm.coe.int/1680487770> [31.07.2024].
[15] *Case of Roman Zakharov v. Russia*, (Application no. 47143/06), <hudoc.echr.coe> [31.07.2024].

monitored. Therefore, assessing the relevant legislation in abstracto was justified, meaning that the applicant did not need to demonstrate a personal risk of surveillance. He was entitled to claim victim status under the Convention.

In this ruling, the issue of supervision was critical. The national legislation's ban on the registration and recording of surveillance rendered it impossible for supervisory bodies to identify cases where surveillance had been conducted without judicial authorization. Despite the fact that the competent authorities possessed the technical capability to conduct direct surveillance, this legal provision rendered any supervisory mechanism in the country ineffective, as it deprived authorities of the ability to check the legality of the surveillance.

Although the legal framework theoretically provided for some level of prosecutorial oversight, in practice, the legislation failed to establish adequate and effective safeguards against arbitrary actions.

b. Podchasov v. Russia[16]

On February 13, 2024, the European Court of Human Rights delivered its judgment in the case of *Podchasov v. Russia*, addressing the critical issue of indefinite access to electronic communication systems by law enforcement agencies, particularly regarding access to the "weak encryption mechanism" of correspondence and its content.

Under the provisions of the Code of Criminal Procedure of the Russian Federation and the Act on Operative-Investigative Activities, electronic communication companies were mandated to store communication data for one year and their content for six months. Additionally, data, including information that could assist law enforcement in deciphering communications, was to be provided to electronic communication companies upon request.

In this case, the Federal State Security Service of Russia requested that the electronic communication company "Telegram" submit system information that would enable the service to decrypt communications linked to six mobile numbers. Notably, the users of these numbers had utilized the "secret correspondence" function of the "Telegram" platform to encrypt their messages.

The complainant contended that the indefinite access granted to law enforcement authorities was in violation of Article 8 of the European Convention on Human Rights.

The Court emphasized the importance of mechanisms ensuring the privacy of electronic communications in the digital age, including encryption measures that facilitate the protection of fundamental rights. It recognized that encryption enables users to safeguard their data and prevent the disclosure of confidential information. The Strasbourg Court found the requirement to decrypt data stored within an electronic communication system to be disproportionate, as the national legislation lacked provisions for appropriate and sufficient justification.

The Court underscored that protecting personal data is vital for the realization of an individual's right to respect for private and family life. National law must provide adequate safeguards to prevent the processing of personal data that contravenes Article 8 of the Convention. Such measures are particularly crucial when data is automatically processed for law enforcement purposes. The Court further clarified that interference in areas protected by Article 8, for law enforcement reasons, must not rely solely on modern technologies in a

[16] The European Court of Human Rights made a decision on the inadmissibility of groundless and indefinite access to the electronic communication system by law enforcement agencies, see <pdps.ge/ka> [31.07.2024], referred to: Case of Podchasov v. Russia, Application no. 33696/19, 13 February 2024.

disproportionate manner. Therefore, clear and detailed rules governing data storage, usage, and access are necessary. Additionally, the duration of data retention should be proportionate to the legitimate purpose of collection.

In assessing the factual circumstances of the case, the European Court of Human Rights noted that the long-term retention of all data and metadata in the system would impact all users of Internet communications, regardless of any suspicion regarding their involvement in criminal activities. Thus, the Court determined that the requirement for data retention and access infringed upon data confidentiality and failed to provide sufficient protections for the rights of data subjects.

Consequently, the Court concluded that the national legislation, which mandated the storage of communications from all Internet users and permitted direct access by security services to electronic communication systems without adequate data protection guarantees, could not be deemed necessary in a democratic society. As a result, the Court found a violation of Article 8 of the European Convention on Human Rights.

Members of the European Parliament emphasized the necessity for both ex ante and ex post supervision, aligning with the Court's approach.[17]

c. Ekimdzhiev and Others v. Bulgaria[18]

The case of *Ekimdziev et al. v. Bulgaria* addresses the inadequacy of legal safeguards against illegality and abuse of power concerning covert surveillance, as well as the storage and access to data obtained through wiretapping.

Factual Circumstances: The plaintiffs consist of two lawyers and two non-governmental organizations associated with them. They assert that they are at risk of surveillance and interception of communications by the Bulgarian state based on their activities and the existing Bulgarian legislation on surveillance and its practical application. Notably, the plaintiffs do not claim that state authorities have conducted surveillance or wiretapping of their communications.

Evaluation by the European Court: The European Court of Human Rights reviewed the application of Bulgarian legislation regarding surreptitious surveillance, acknowledging significant improvements since its prior decision in the case of *Association for European Integration and Human Rights and Ekimdzievi v. Bulgaria*. However, the Court concluded that the legislation did not meet the minimum standards of protection against illegality and abuse of power required by Article 8 of the Convention.

A crucial aspect of the Court's evaluation pertains to the issue of supervision. It found that national legislation failed to establish clear rules governing the storage, access, review, use, communication, and destruction of communication data. Such data was retained within criminal cases, accessible to anyone, which resulted in inadequate protection and created a substantial risk of disproportionate intrusion into the personal lives or correspondence of individuals and legal entities.

[17] European Parliament Resolution of 12 March 2014 on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs (2013/2188(INI)).

[18] Case of Ekimdzhiev and Others v. Bulgaria, (Application no. 70078/12), <https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-214673%22]}> [05.08.2024].

Furthermore, the existing supervisory framework was deemed incapable of effectively assessing potential abuses of power. Although the Personal Data Protection Commission possessed the authority to examine data collection practices by communications service providers, it lacked the capacity to scrutinize the actions of public authorities with access to such data.

Consequently, the European Court determined that the current Bulgarian legislation regarding the storage and access to data obtained from communication interception did not fully comply with the requirement of "law," thus failing to ensure that any "interference" was "necessary in a democratic society." This inadequacy resulted in a violation of Article 8 of the European Convention on Human Rights.

5. Conclusion

Ensuring the inviolability of an individual's right to private life, as protected by Article 15 of the Constitution of Georgia, stands as one of the paramount responsibilities of a democratic state. This right serves as the foundation for human growth and development, allowing individuals to flourish as persons. It functions as a shield through which citizens can express their opinions, embrace individuality, and hold diverse perspectives without facing negative repercussions. Consequently, the investigative activities undertaken by law enforcement agencies, particularly covert investigative actions, necessitate meticulous oversight and various legislative safeguards. This highlights the importance of enhancing and linking the mandate of the Personal Data Protection Service to established Western practices.

This is evidenced by the annual reports and statistics published by the Service, as well as the high rate of implementation of recommendations from international organizations discussed in the article. Such accomplishments position the Personal Data Protection Service as a robust supervisory mechanism for ensuring the effectiveness of covert investigative actions.

Bibliography:

1. Law of Georgia "On Personal Data Protection", 14/06/2023;
2. Criminal Procedure Code of Georgia, 09/10/2009.
3. Article 4 of the Directive on the processing of personal data in the police sector;
4. Conclusion of the Legal Issue Committee "On Amendments to the Criminal Procedure Code of Georgia" on the Law of Georgia (No. 1614-VIIIms-Xmp, 7/06/2022) regarding the motivated remarks of the President of Georgia (No. 07-1/14, 23/06/2022);
5. *Akubardia I.,* Control mechanisms over secret investigative actions, collection of articles - Revaz Gogshelidze 65, volume, 2022, 200, 228;
6. Council of Europe Commissioner for Human Rights, Democratic and Efective Oversight of National Security Services, 2015, 8, <https://rm.coe.int/1680487770> [31.07.2024].
7. European Parliament Resolution of 12 March 2014 on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs (2013/2188(INI));
8. *Fafiashvili L., Tumanishvili G*. and others, Criminal Procedure Commentary of Georgia (as of October 1, 2015), Tb., 2015, 428-429;
9. Personal Data Protection Inspectorate Office 2015 Report, 34;

10. Statistics of the activity of the Personal Data Protection Service for 12 months of 2023 (January-December), 7, 9.Council of Europe Commissioner for Human Rights, Democratic and Effective Oversight of National Security Services, 2015, 8, <https://rm.coe.int/1680487770> [31.07.2024];
11. *Case of Roman Zakharov v. Russia*, (Application no. 47143/06);
12. *Case of Podchasov v. Russia,* Application no. 33696/19, 13 February 2024.