

Biometric Surveillance and Tracking in Georgia

The mass arrests of protest participants in Georgia between 2024 and 2026 brought into sharp focus the scale and purpose of the state’s surveillance infrastructure. As of April 2026, the Ministry of Internal Affairs (MIA) operates a network of 9,822 cameras integrated into the ‘Safe City, Safe Region, Safe Country’ programme — a figure that includes 7,233 general-vision cameras and 2,589 licence-plate recognition devices, according to the MIA’s own published data.¹ This infrastructure is integrated with automated facial recognition technology supplied by multiple vendors and capable of real-time biometric matching against government databases.

CCTV Camera concentrations in Tbilisi correspond to documented protest assembly points and established march routes. Public procurement records, reviewed by the Organised Crime and Corruption Reporting Project (OCCRP), show that from December 2024, MIA units and Tbilisi municipality together procured surveillance cameras and related licences worth approximately USD 1.2 million, including 251 Dahua Technology cameras with AI-powered facial recognition capabilities.²

The consequence has been the post-factum identification and arrest of protest participants — in some cases weeks or months after the demonstrations concerned. This pattern is consistent with the use of surveillance for deterrent purposes rather than the narrowly tailored regulation of public order.

I. Targeting peaceful protesters

Protest-related arrests documented since 2024 have relied, in whole or in part, on biometric matching carried out through the ‘112’ unified video surveillance system operated by the MIA. The system integrates CCTV camera feeds with automated facial recognition software and cross-references outputs against government databases of personal photographs. The legal authority for this processing derives from interior ministerial orders.

That legal basis does not satisfy the ‘quality of law’ standard established by the European Court of Human Rights and applied to biometric data processing under Article 8 of the European Convention on Human Rights (ECHR). The relevant ministerial orders and the Law on Police together provide insufficient safeguards governing the scope, conditions, retention, oversight and use of biometric data processing. The processing of biometric data on the basis of a ministerial order that rests on so vague a statutory delegation does not constitute a sufficiently accessible, precise, or foreseeable legal basis within the meaning of Article 8(2) ECHR. The European Court of Human Rights (the Court) and Convention 108+ classify this type of data as sensitive data warranting heightened protection.³

¹ https://112.gov.ge/?page_id=1660&lang=en

² OCCRP, Georgia’s Surveillance Surge: Chinese Cameras Spark Protest Crackdown Fears, 28 March 2025, available at <https://www.occrp.org/en/news/georgias-surveillance-surge-chinese-cameras-spark-protest-crackdown-fears>

³ Convention 108+ and Protocols, available at <https://www.coe.int/en/web/data-protection/convention108-and-protocol>

The Council of Europe (CoE) Guidelines on Facial Recognition (adopted by the Committee of Ministers in 2021) are explicit that the deployment of facial recognition for law enforcement purposes requires,⁴ at minimum:

- a clear and specific legal basis;
- a necessity and proportionality assessment;
- a prohibition on use against persons exercising fundamental rights including the right to peaceful assembly;
- and independent supervisory oversight.

The available evidence indicates that these safeguards are either absent or insufficiently guaranteed in the Georgian legal framework. The deployment of a highly intrusive biometric surveillance system against participants in peaceful demonstrations — in the absence of any individualised public safety risk justifying such processing — raises serious concerns regarding compatibility with Articles 8 and 11 of the European Convention on Human Rights.

The documented use of post-factum facial recognition to identify and arrest protest participants produces a significant chilling effect on the exercise of the rights to privacy and peaceful assembly, a factor that the European Court has repeatedly recognised as relevant when assessing compliance with Articles 8 and 11.

Where individuals know, or reasonably believe, that participation in a demonstration will result in biometric identification and potential sanction, the effective exercise of the right to peaceful assembly is structurally impaired. The same logic applies with greater force where the surveillance infrastructure is visibly concentrated at protest locations and its use against demonstrators is publicly documented.⁵

II. Ineffectiveness of the personal data protection institutions

Failure to Act During the Protest Period

During the mass protests of 2024 to 2026, the Personal Data Protection Service, established o6 2022 pursuant to EU association commitments and CoE recommendations as an independent supervisory authority for personal data protection, demonstrably failed to fulfil its mandate.

In February 2025, the Georgian Young Lawyers' Association (GYLA) formally called on the Service to examine the legality of the MIA's use of facial recognition surveillance systems against protest participants.⁶ The institution failed to respond substantively to that request.

⁴ Council of Europe, Guidelines on Facial Recognition (2021), available at [G](#)

⁵ Amnesty International and more than 170 organisations call for a ban on biometric surveillance, 7 June 2021, available at <https://www.amnesty.org/en/latest/press-release/2021/06/amnesty-international-and-more-than-170-organisations-call-for-a-ban-on-biometric-surveillance/>

⁶ GYLA calls on the Personal Data Protection Service to Study the Practice of Using Facial Recognition Cameras by the MIA, 10 February 2025, available at <https://gyla.ge/en/post/saia-mowodeba-sheswavlil-iqnes-amomcnobi-kamerebis-gamoyenebis->

Individuals subjected to arbitrary CCTV surveillance and the alleged seizure of personal electronic devices following protest-related arrests similarly received no response to their complaints from the agency.

The Service's silence in the face of documented, large-scale biometric processing of participants in peaceful demonstrations — precisely the category of processing Convention 108+ and the CoE's facial recognition guidelines treat as requiring the highest level of scrutiny — represents a failure of institutional function that preceded and contributed to the conditions enabling the abuses described in section above.

Abolishing Personal Data Protection Service

On 17 November 2025, the Parliament of Georgia — comprised predominantly of Georgian Dream party members — announced the abolition of the Personal Data Protection Service, effective 2 March 2026. The announced justification was institutional optimisation and resource rationalisation. The Service's functions were transferred to the State Audit Office (SAO).⁷

The timing and surrounding circumstances indicate that the reform weakens independent oversight over the personal data protection at a time of expanding state surveillance powers. Established as an independent supervisory authority for personal data protection, the Service had the functional equivalent of a national data protection authority (DPA) within the meaning of Convention 108+.

While the practical independence of the Service from government was consistently criticised as insufficient from its inception, it constituted the only institutional body with a formal mandate to investigate complaints of unlawful processing by state authorities. Its abolition sent a strong institutional signal to any successor body about the consequences of independent action.

The transfer of functions to the State Audit Office, to a constitutional body with a mandate focused on the audit of public finances with the mandate not designed for the adjudication of individual data protection complaints or the investigation of surveillance practices, in itself, raise questions about effectiveness of this decision. Convention 108+, Article 15 requires contracting parties to establish supervisory authorities that are independent and possess effective investigative and corrective powers. The formal transfer of data protection functions to a general audit body, without equivalent structural independence or specialist competence, raises serious questions about whether Georgia will continue to meet that obligation in substance rather than merely in form.

[praqtika?fbclid=IwY2xjawIWnJZleHRuA2FlbQIxMAABHZfCGJS9gjpJIuI1VGrR3s79jk-TLSUbkNMbp-6jsdVIqwCKe38Usd71UQ_aem_-F9e-mSiFa--jdObuKZC_Q](https://www.parliament.ge/en/media/news/adamianis-uflebata-datsvisa-dasamokalakointegratsiiskomitetmapersonalurmonatsemtadatsvisshesakhebkanonshitsvlilebameoremosmenitganikhila)

⁷ Parliament of Georgia, The Human Rights and Civil Integration Committee deliberated on the Draft Law on Personal Data Protection for the II reading, 02 December 2025, available at <https://www.parliament.ge/en/media/news/adamianis-uflebata-datsvisa-dasamokalakointegratsiiskomitetmapersonalurmonatsemtadatsvisshesakhebkanonshitsvlilebameoremosmenitganikhila>

III. Conclusion

The mass biometric surveillance of peaceful protesters, the dismantling of independent data-protection oversight, and the expansion of State access to sensitive personal data together breach Georgia's international commitments in the field of personal data protection, freedom of assembly and expression.