



Personal Data for Surveillance:

Remote Facial Recognition and Emerging Surveillance Practices in Georgia

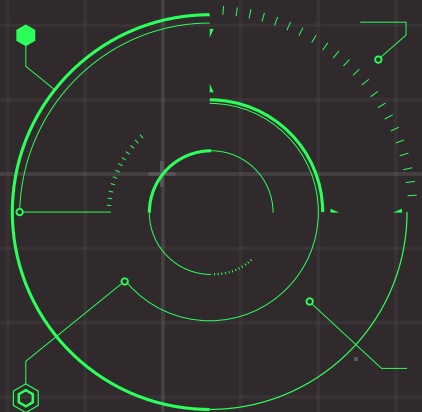


Table of Contents

1. Executive Summary	3
2. Background	6
3. The Chilling Effect of Surveillance on Freedom of Expression	11
4. The Infrastructure Behind Chilling Effect: How Russian Facial Recognition was Built and Deployed	19
4.1 A decade in the making facial recognition surveillance layer	19
4.2 How facial recognition works in practice: cameras, software, and identification	24
4.3 How law formalizes surveillance	29
4.4 Procured from Moscow: The Strategic Risk of Georgia's Surveillance Vendor	31
5. Emerging Surveillance Practices: A First Look on Elections, the Church, and Mental Health Issues	35
5.1 Personal Data for Social Control: Electoral Practices	35
5.2 Personal Data for Social Control: Faith and the Orthodox Church	41
5.3 Personal Data for Social Control: Mental Health Records	45
6. Conclusion	50

1. Executive Summary

In October 2024, Georgian Dream claimed victory in parliamentary elections whose results the opposition, the president, and international organisations and observers refused to accept. Later in November, Georgian Dream halted the EU accession process. Protests began that night and have not stopped since.

This report examines how Georgia's surveillance apparatus has been turned against its own citizens, to silence demonstrations. It documents the facial recognition system procured from a Moscow-based company with institutional ties to Russian security services, the six layers of state data that can be combined around any individual, the structured use of fines, legal escalation, and retroactive enforcement to make public protest economically and socially costly. At its center is the chilling effect, the process by which people do not need to be arrested or identified to change their behavior, the awareness that they might be is enough. But protest monitoring is one application of a broader logic. The same infrastructure and the same instinct for control extend into elections, where personal data is used to pressure and mobilize voters - as well as into the Orthodox Church, used as a vehicle for political surveillance, and into mental health records, weaponized to discredit and pressure individuals. Each is examined here as part of how a surveillance state quietly consolidates itself across different domains of public and private life.

Key findings:

General

- Georgian authorities are in the active development phase of a mass surveillance infrastructure. Personal data held across multiple state agencies is being used or may be used for social control - via protest monitoring, elections, religious institutions, and mental health records.
- Georgia's surveillance infrastructure was not built for the 2024 protests - it was already in place. The demonstrations revealed a system thirteen years in the making, since 2013.
- Authorities implemented structured, sequential mechanisms to produce a chilling effect among demonstrators. Legal amendments provided the framework; remote facial recognition provided the operational backbone.
- According to interviewees with demonstrators, the chilling effect has reduced both the visible scale of demonstrations and the willingness of protesters to participate in the future.

Vendor and Strategic Risk

- The Ministry of Internal Affairs has procured its facial recognition system from Papillon AO, a Moscow-based company whose products serve primarily Russian law enforcement and Russian proxy states - despite a wide market of alternatives available in democratic countries.
- Five upgrades over eleven years, direct training of ministry operators by Russian personnel on Georgian territory, and a perpetual licence signed in October 2024 may constitute an institutional partnership, not a vendor relationship. As of April 2026, a core component of Georgian state security infrastructure remains under the legal jurisdiction of the country that occupies Georgian territory.

Technical Capabilities

- The Polyface software gives the ministry unlimited operator access and is capable of running searches against pre-loaded photos from social media and other external sources - a feature the ministry explicitly requested, indicating cross-platform surveillance as an intended use.
- The system supports three modes of operation: automatic tracking of all individuals in frame, manual operator-directed observation, and watchlist-based alerting for pre-identified activists.
- The software does not only identify who someone is - it can reconstruct a full protest history: when a person arrived, how long they stayed, what was the movement of a person, and how many times they returned. Once identified at one protest, the system can locate them across every other recorded event.

Chilling Effect

- According to interviews with demonstrators, because fines arrived weeks or months after the fact, attending a protest may have stopped being a temporary act and become, in their accounts, a permanent and searchable record.
- The interviews point to behavioural changes both at protests and in everyday life: demonstrators describe rerouting their commutes, moving communication to encrypted platforms, limiting their protest expression, and avoiding camera-dense areas during ordinary daily activity.
- Each time demonstrators adapted, the legal framework appears to have caught up. What was tolerated one month was penalised the next, producing successive rounds of withdrawal rather than a single break.

- Face masks, adopted as protection, made the protest environment feel unrecognisable and tense, according to several interviewees. Demonstrators could not identify friends or read the crowd, and the act of self-protection became its own source of anxiety.
- Interviewed demonstrators broadly report that the fear of identification caused them or people they knew to stop attending protests or significantly reduce participation - and that it continues to constrain their willingness to demonstrate in the future.

2. Background

On October 26, 2024, Georgian Dream, a party that had governed Georgia since 2012, claimed victory in parliamentary elections held under a newly introduced fully proportional system.¹ International observers documented voter intimidation and irregularities with electronic voting machines.² Georgia's president by that time, Salome Zourabichvili, refused to recognize the results and called for an international investigation.³ All four opposition coalitions that cleared the electoral threshold rejected the outcome and declined their parliamentary mandates.⁴ On November 28, the European Parliament adopted a resolution declaring the elections neither free nor fair and calling for a re-run within a year.⁵ That same day, Prime Minister Kobakhidze announced the suspension of EU accession talks until at least 2028⁶ - a direct breach of a constitutional obligation that requires every public body to advance accession,⁷ in a country where 89 percent of the population supports EU membership.⁸

Protests began that evening on Rustaveli Avenue. Demonstrators demanded new elections. By December 3, they had spread to at least 37 cities in Georgia and 40 abroad^{9,10}. The government's response was physical: water cannons, rubber bullets, documented beatings by police and informal violent groups. The Public Defender's Office recorded 282 cases of physical abuse.¹¹ At least 486 people were detained in November and December alone.¹² The demonstrations continued. As of June 3, 2026, they are still ongoing - 552 consecutive days.

1. Civil.ge, 'Key Points of Newly Adopted Constitution' (27 September 2017), <https://old.civil.ge/eng/article.php?id=30474> (25 May 2026)

2. Council of Europe, 'Georgia: elections marred by uneven playing field, pressure and tension, but voters offered a wide choice, say international observers' (27 October 2024), <https://shorturl.at/voWUW> (25 May 2026)

3. Deutsche Welle, 'Georgian President Salome Zourabichvili rejects election results | DW Interview (Uploaded 28 October, 2024), https://youtu.be/Ut_sWcJEvR0?si=4hKXUx8ZBUMJ_9XY (25 May 2026)

4. The Guardian, 'Georgia's pro-EU opposition calls for protest over 'rigged' election result' (27 October 2024), <https://www.theguardian.com/world/2024/oct/27/georgias-pro-eu-opposition-calls-for-protest-over-rigged-election-result> (25 May 2026)

5. European Parliament resolution of 28 November 2024 on Georgia's worsening democratic crisis following the recent parliamentary elections and alleged electoral fraud (2024/2933(RSP)), https://www.europarl.europa.eu/doceo/document/TA-10-2024-11-28_EN.html (25 May 2026)

6. Euronews, 'Georgian prime minister suspends EU membership talks until end of 2028' (28 November 2024), <https://shorturl.at/PoTZP> (25 May 2026)

7. Constitution of Georgia (Tbilisi 1995), <https://matsne.gov.ge/en/document/view/30346> (25 May 2026).

8. IRI, 'IRI Georgia Poll Finds Support for EU Accession High, Weariness of Russian Presence, Lack of Faith in Political Parties' (25 April 2023), <https://shorturl.at/dVkbJ> (25 May 2026)

9. ForSet, <https://shorturl.at/KOK3p> (25 May 2026)

10. ForSet <https://shorturl.at/r7fgQ> (25 May 2026)

11. Radiotavisupleba, 'Number of opened cases - 0. Violence by law enforcement officers during protests has not been investigated even after 6 months' (28 May 2025), <https://shorturl.at/mjgNJ> (25 May 2026)

12. Radiotavisupleba, 'Number of opened cases - 0. Violence by law enforcement officers during protests has not been investigated even after 6 months' (28 May 2025), <https://shorturl.at/mjgNJ> (25 May 2026)

Between late 2024 and early 2026, the legal framework around protest tightened steadily - sharper fines, new penalties for face coverings, formal powers for biometric identification, and eventually criminal liability for sidewalk demonstrations.

The legal framework escalated in steps.¹³ The fine for blocking a road rose from 500 GEL to 5,000 GEL and to 15,000 GEL for repeat actions. Wearing a face mask at a protest was penalized at 2,000 GEL. February 2025 amendments to the administrative code gave authorities formal powers to photograph individuals and conduct biometric identification of suspected administrative violators, providing legal grounding for practices already underway.¹⁴ By March 2026, blocking a sidewalk could result in criminal charges and imprisonment and the assembly required pre-registration and state approval. Transparency International Georgia assessed that freedom of assembly had been factually abolished.¹⁵

Before December 2024	Road-blocking fine: 500 GEL
↓	
13 December 2024 – 6 February 2025	Road-blocking fine raised to 5,000 GEL; organizer fine 15,000 GEL; face-mask penalty 2,000 GEL introduced
↓	
February 2025	Administrative code amended to give police formal powers of biometric identification - putting a legal basis under identification practices that were already in use.
↓	
July 2025	Non-payment of fines becomes punishable by imprisonment (15–30 days); fine appeals restricted to courts only
↓	
16 October 2025	Face coverings and obstructing movement become administrative detention offenses (up to 15–60 days); repeat offenses carry criminal imprisonment (1–4 years)

Table 1: *The escalation of restrictive laws against demonstrators*

Georgia’s surveillance infrastructure was not built for the 2024 protests - it was already in place. The demonstrations revealed a system thirteen years in the making. The state purchased its first large crowds surveillance software in 2013 and the spending on surveillance technologies increased thirteenfold between 2019 and 2024, with the largest

13. Socialjustice.org.ge, ‘Systematic analysis of legislative changes adopted against protests’ (27 December 2024), <https://shorturl.at/jnUeJ> (25 May 2026)

14. Socialjustice.org.ge, ‘Systematic analysis of legislative changes adopted against protests’ (27 December 2024), <https://shorturl.at/jnUeJ> (25 May 2026)

15. Transparency Georgia, ‘De Facto Abolition of Freedom of Assembly – A Law Turned into a Repressive Mechanism’ (4 November 2025), <https://shorturl.at/EOAZp> (25 May 2026)

increase between 2023-2024.^{16,17} The scale of that expansion has since been confirmed by the government itself. In April 2026, incoming vice-premier Mamuka Mdinaradze stated publicly that the volume of information flowing into the State Security Service had grown thirtyfold in a single year - wiretapping included.¹⁸ *“Yes, wiretapping has also increased - but on the basis of court orders,”* he said, adding that court orders themselves had grown 2 to 2.5 times. He framed it as an achievement, and promised it would accelerate.

The expansion was not invisible to the public. A 2023 CRRC Georgia survey found that 44 percent of the population believed the government was monitoring them in at least one form - phone calls, social media, informants, or physical surveillance.¹⁹ Opposition supporters were 25 percentage points more likely than ruling-party supporters to hold that belief. The infrastructure described in this report was already shaping behavior before it was deployed against demonstrators.

By 2024, the infrastructure that made identification possible was largely already there. It operates across several institutions each holding a different piece of the same person. For the purposes of this report, we have categorised these holdings into layers, grouped by the function each serves in the identification and enforcement chain.

The capture layer: the Ministry of Internal Affairs and its subordinate units hold the visual record:

- CCTV footage from public surveillance networks²⁰
- Facial recognition data processed through Polyface software, procured from Papillon, a Moscow-based company with documented ties to Russian security services²¹
- Automatic number plate recognition data²²
- Body and vehicle camera footage from the Patrol Police
- Mobile communication metadata via lawful interception

16. Agreement on state procurement N934 (4 September 2013), <https://tenders.procurement.gov.ge/public/library/files.php?mode=contract&file=71996> (25 May 2026)

17. A. Akhmedova, New challenge: Chinese surveillance cameras in Georgia, (Tbilisi 2025), <https://civicidea.ge/%E1%83%90%E1%83%AE%E1%83%90%E1%83%9A%E1%83%98-%E1%83%92%E1%83%90%E1%83%9B%E1%83%9D%E1%83%AC%E1%83%95%E1%83%94%E1%83%95%E1%83%90-%E1%83%A9%E1%83%98%E1%83%9C%E1%83%A3%E1%83%A0%E1%83%98-%E1%83%A1/> (25 May 2026)

18. Imedinews, Mamuka Mdinaradze on the State Security Service's performance: "If a year ago the flow of information was at X level, today this figure has increased thirtyfold. This includes an increase in wiretapping as well, though only on the basis of a court order, (23 April 2026), <https://shorturl.at/WljeU> (25 May 2026)

19. OC Media, 'Datablog | Do Georgians feel like they are being spied on by the government?' (13 June 2023), <https://oc-media.org/datablog-do-georgians-feel-like-they-are-being-spied-on-by-the-government/> (29 May 2026)

20. 'Video Surveillance System' https://112.gov.ge/?page_id=280 (29 May 2026)

21. On.ge 'Georgia Uses Russian Artificial Intelligence to Investigate Crimes' (24 January 2023), <https://go.on.ge/34xo> (29 May 2026)

22. 'Video Surveillance System' https://112.gov.ge/?page_id=280 (29 May 2026)

- The Public Safety Management Center 112 holds nationwide video surveillance feeds²³

The cameras feeding this system are manufactured primarily by Hikvision and Dahua - Chinese companies sanctioned by the United States and legally obliged under Chinese law to share data with the state.

The reference layer: footage is useful only when a face can be matched to an identity. The Public Service Development Agency, under the Ministry of Justice, holds:

- Facial images for the entire Georgian population²⁴
- The national ID and passport registry²⁵
- Population registry including address and family links²⁶

This is what converts an image into an actionable identity. A Ministry of Internal Affairs response obtained by Rights Georgia confirms that this data is integrated into the Ministry's unified information bank, giving Polyface direct access to civil-registry photographs when it runs a match.²⁷ Mass identification at protests is possible not because demonstrators are in a police watchlist, but because every adult citizen is already in the registry the system queries.

The intelligence layer: the State Security Service maintains:

- Communications interception data
- Surveillance records on activists, journalists, and political actors
- Intelligence files on protests and civic activity
- Biometric identifiers collected through covert means

The relational and locational layer: telecommunications operators (Magti, Silknet, Cellfie) hold:

- Subscriber identity and call detail records²⁸
- Mobile location data via cell tower geolocation²⁹

23. Minister of Internal Affairs of Georgia, Order No. 108, On the Approval of the Statute of the Legal Entity of Public Law (LEPL) – Public Safety Management Centre “112” under the Ministry of Internal Affairs of Georgia (27 December 2019). <https://police.ge/departments/sazogadoebrivi-usaftrkheobis-martvis-tsentr-112/33?locale=ka> (29 May 2026)

24. ‘Personal Data Protection’ <https://shorturl.at/kWETV> (29 May 2026)

25. Minister of Internal Affairs of Georgia, Order No. 462, On the Approval of the Statute of the Legal Entity under Public Law (LEPL) – Service Agency of the Ministry of Internal Affairs of Georgia (28 November 2019). <https://www.matsne.gov.ge/ka/document/view/4714514?publication=0> (29 May 2026)

26. Minister of Internal Affairs of Georgia, Order No. 462, On the Approval of the Statute of the Legal Entity under Public Law (LEPL) – Service Agency of the Ministry of Internal Affairs of Georgia (28 November 2019). <https://www.matsne.gov.ge/ka/document/view/4714514?publication=0> (29 May 2026)

27. Mass Surveillance: Accountability of the Personal Data Protection Service, (2025), <https://drive.google.com/file/d/1JLS6kZJS6jyxfHhH0Wqpg2IL8MvJCex9/view> (25 May 2026)

28. Magticom, ‘Privacy Policy’ <https://docs.magticom.ge/contract/latest/privacy-policy> (29 May 2026)

29. Ibid

- Device identifiers
- Internet usage metadata

Combined with protest footage, this enables network mapping - reconstructing who was present, when, or who was in contact with whom.

The political and welfare layers: the Central Election Commission holds the unified voter registry with identification data and address information. The Ministry of Health and Social Service Agency holds healthcare records, social assistance files, disability status, and welfare program data. These datasets are not, on their own, surveillance instruments. Their inclusion here reflects the structural risk: combined with the capture, reference, and financial layers, they would allow political behaviour and economic vulnerability to be aligned on the same person.

These layers are described separately here, but they are not separate in practice. The Internal Affairs Ministry's own records show that civil-registry data is already integrated into its matching system.³⁰ Other integrations are likely; they are simply not yet documented.

No single agency constitutes the significant threat. The threat is their combinability - the capacity to align these datasets around the same individual and for wider social control. Protest monitoring is one application of that logic. The same infrastructure for social control could extend into elections, welfare distribution, mental healthcare, and other domains of Georgian life examined in this report. That infrastructure was already in place in November 2024, when demonstrations began. The chapters that follow examine what that produced - beginning with the people who encountered it first.

30. Order of the Ministry of Internal Affairs of Georgia, On the Approval of the Strategy for the Development of Intelligence-Led Policing (ILP) (2021–2025), (11 July 2021), <https://info.police.ge/uploads/63f38bcd3981f.pdf> (25 May 2026)

Chapters 3 and 4 draw on interviews, investigation, and editorial collaboration with AlgorithmWatch, originally published in “Seen and Silenced: How Russian Surveillance Software Suppresses Georgian Civilians Rights”, available at <https://algorithmwatch.org/en/russian-surveillance-face-recognition-georgia/>, licensed under CC BY 4.0. Some passages are reproduced or adapted from that piece.

Source: AlgorithmWatch, CC BY 4.0

3. The Chilling Effect of Surveillance on Freedom of Expression

A chilling effect on freedom of expression becomes possible with the awareness that participation in public life carries an unpredictable personal cost. When people begin calculating the risks before showing up, adjusting their routes, limiting what they say, the effect has already taken hold. What follows documents how that process unfolded in Georgia: the penalties that made surveillance consequential, the visible shift in protest participation, self-censorship and behavioral changes among demonstrators, and fear of showing up.

From December 2024 onward, authorities used surveillance footage and facial recognition to identify protest participants and issue administrative fines. The fine for blocking a road - the charge most broadly applied - stood at 5,000 GEL, nearly twice the average monthly wage, rising to 15,000 GEL for repeat violations by November 2025.³¹ As of March 2026, blocking the road or sidewalk, as well as wearing a facemask at the demonstration is a criminal offense - punishable with up to 15 days imprisonment, up to 1 year for repeated action, up to 2 years for three or more repetitions.³²

According to the Public Defender's 2025 annual report, 8,200 violations were registered under Article 174¹ of the Administrative Offenses Code - the road-blocking provision - during the reporting year.³³ Fines were issued automatically through surveillance cameras with facial recognition. By March 2025, at least 2 million GEL in fines had been imposed on demonstrators.³⁴ Between 2024 April - 2026 April, 49 demonstrators are imprisoned and 65 are awaiting trial with criminal charges, according to Transparency International Georgia.³⁵

31. Transparency Georgia, 'De Facto Abolition of Freedom of Assembly – A Law Turned into a Repressive Mechanism' (4 November 2025), <https://shorturl.at/EOAZp> (25 May 2026)

32. Radiotavisupleba, 'Wearing a mask at a protest, blocking a road, and possessing pyrotechnics are punishable by imprisonment – the "Dream" party has passed the bill.' (16 October 2025), <https://www.radiotavisupleba.ge/a/33561705.html> (27 May 2026)

33. Public Defender of Georgia, 'Report of the Public Defender of Georgia, On the Situation of Protection of Human Rights and Freedoms in Georgia' (2025) <https://shorturl.at/7thPH> (27 May 2026)

34. BMG, 'The Amount Of Fines Imposed On Protest Participants Reaches GEL 2 MLN - GYLA' (19 March 2025), <https://bm.ge/en/news/the-amount-of-fines-imposed-on-protest-participants-reaches-gel-2-mln-gyla> (27 May 2026)

35. Transparency Georgia, 'Criminal Cases Against Protest Participants April 2024 – April 2026' (15 April 2026), <https://transparency.ge/en/blog/criminal-cases-against-protest-participants-april-2024-april-2026> (27 May 2026)

From December 2024 onward, the number of cameras operational along the protest route around Parliament increased. Procurement shows that between December 2024 - March 2025, the state purchased 251 advanced Dahua cameras at a combined value of \$1.2 million, deployed in Tbilisi.³⁶ Demonstrations in Tbilisi have historically concentrated on Rustaveli Avenue, near Parliament, and the cameras installed along that stretch are visible to anyone present.



Figure 1: A total of 46 cameras are concentrated at the Rustaveli protest site, in front of Parliament, covering an area less than half the size of a football pitch.

Source: AlgorithmWatch, CC BY 4.0.

Based on publicly available technical specifications of PTZ surveillance cameras installed along the protest route - including optical zoom range, facial recognition distance, and field of view - this report estimated the minimum number of cameras required to surveil the primary demonstration area near Parliament (approximately 100 by 50 metres). The methodology calculated coverage needed for two distinct functions: wide-angle documentation of crowd movement, and facial recognition-grade capture of individuals. The minimum functional requirement for both combined is 6 to 12 cameras.

The actual number installed in that area is 46 - between four and seven times the functional minimum. This excess is open to interpretation, but two readings are technically grounded.

36. OCCRP, 'Georgia's Surveillance Surge: Chinese Cameras Spark Protest Crackdown Fears' (28 March 2025) <https://www.occrp.org/en/news/georgias-surveillance-surge-chinese-cameras-spark-protest-crackdown-fears> (27 May 2026)

A PTZ camera tracks and zooms - it follows one person at a time. At 6 to 12 cameras, the system can identify whoever authorities choose to focus on. At 46, it can plausibly capture everyone present at the same moment. That is a different capability: not identifying a face, but reconstructing a crowd.

Second, 46 cameras on a 100-metre stretch are not hidden. Anyone standing there can see them. According to interviewed demonstrators, what produced behavioral change was not confirmed identification - it was the feeling that identification was unavoidable. At that density, the cameras don't even need to be working, they just need to be visible.



Figure 2: In case of high-turnout protests, when the demonstration scratches on Rustaveli Avenue, at least 129 cameras are concentrated. The actual amount of cameras is expected to be larger.

Source: AlgorithmWatch, CC BY 4.0.

From late November 2024 through January 2025, demonstrations drew tens of thousands of participants, documented in media photography in multiple independent outlets.³⁷ The protests persisted through police violence, mass detentions, documented beatings, and threatening phone calls demonstrators received.³⁸ From early 2025 onward, as the financial penalties accumulated and the legal framework tightened, the scale of demonstrations

37. CNN, 'Georgia is being rocked by growing protests. Here's what you need to know' (3 December 2024), <https://edition.cnn.com/2024/12/02/europe/georgia-tbilisi-eu-protests-intl-hnk/index.html> (27 May 2026)

38. Jamnews, 'Opponents of Georgia's "foreign agent" bill face threats and insults via phone calls' (9 May 2024), <https://jam-news.net/opponents-of-georgias-foreign-agents-bill-threatened/> (27 May 2026)

visibly decreased.³⁹ Photography from the same locations over the same period shows a reduction in the occupation of public space.⁴⁰ The in-depth interviews that follow explore the role surveillance and financial penalties played in that shift.

When protest becomes a traceable data event and surveillance becomes real

The practical impact of remote facial recognition begins when people understand that their presence in a crowd can be captured, stored, analysed and matched to identity databases. At that point, participation in protest stops being a temporary act and becomes a traceable and reconstructable data event.

Facial recognition works by reducing a face to a numerical imprint and matching it against a reference database - ID photographs, passport images, whatever the state holds.

In Georgia's case, ministry correspondence disclosed in 2025 confirms that the facial recognition system is integrated with the civil registry held by the Public Service Development Agency, which contains ID and passport photographs for every Georgian citizen.⁴¹

Giorgi Lubaretsi, a cybersecurity expert, describes the mechanics plainly. *"You collect pixels from a face and use those pixels to create a kind of imprint. Then you have a database where you can compare that imprint to existing data - for example, images from ID cards or passports."* The footage doesn't need to be acted on immediately. *"For analysis and verification, you need to store video. It can be stored for months or even years, depending on resources."* Once stored, it becomes retrospectively searchable: *"If the system detects that the same face appears in different places over several days, you should be able to find all instances where that person was detected across cameras."* The questions it can answer go beyond who was present: *"Who stayed longer at the protest, who arrived first, who came most often, who spent the most total time there."*

The attorney Nika Simonishvili describes how the procedural reality worked in practice. The Interior Ministry would request specific hours of footage from 112, screen it, run biometric identification, and file violation reports. *"They would ask for the first hour of a given protest and whoever appeared in that hour, they'd be fined. Because reviewing a longer period takes too much time and resources. In court documents, they say they identified the person using a 'special software'. What software, they don't say."*

For most demonstrators, this was abstract until they saw the footage itself.

39. Globalvoices, 'Georgia marks a year of protests' (7 December 2025), <https://globalvoices.org/2025/12/07/georgia-marks-a-year-of-protests/> (27 May 2026)

40. OC Media, 'In Photos | 365 days of consecutive protest in Georgia' (28 November 2025), <https://oc-media.org/in-photos-365-days-of-consecutive-protest-in-georgia/> (27 May 2026)

41. Mass Surveillance: Accountability of the Personal Data Protection Service, (2025), <https://drive.google.com/file/d/1JLS6kZJS6jyxfHhH0Wqpg2lL8MvUCex9/view> (25 May 2026)

One woman spent months reviewing protest recordings to compile timestamped evidence for lawyers. Going through a colleague's case file, she saw footage of him standing near the edge of the crowd. *"My friend was barely at the edge, but the zoom was so powerful that every expression, every smile, was clearly visible. It was unimaginable."* Another described what was presented in her own case: *"What was shocking to me was the quality of the video. There was even a moment where someone was messaging on their phone and reading something from a piece of paper - it was legible at that level of detail."* The screenshot circulated on social media. For people who hadn't been fined yet, it made the system harder to dismiss as rumor.

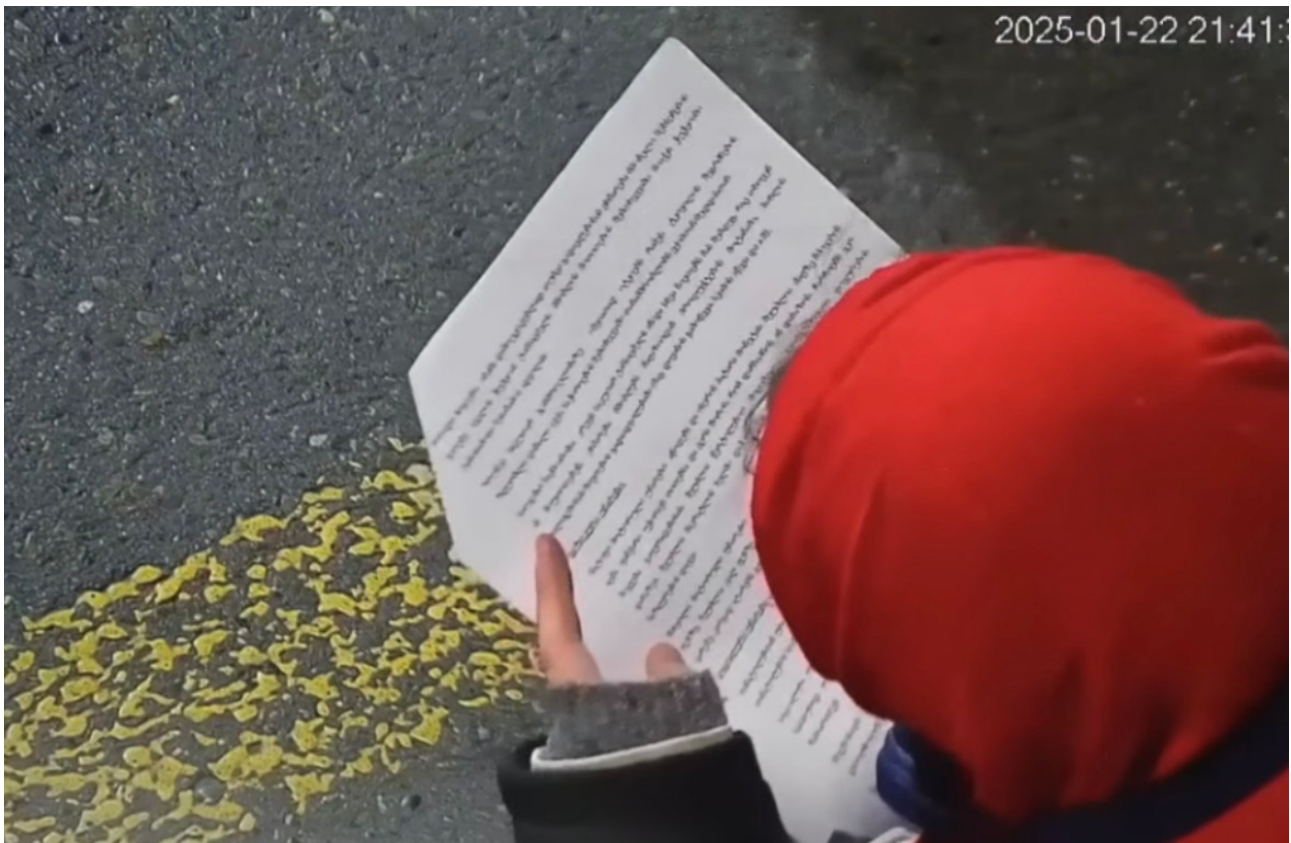


Figure 3: *The quality of cameras is not abstract. One footage shows what a demonstrator is reading. Chapter 4 explores official capacities documented by vendor companies.*

The chilling effect is not driven by confirmed technical specifications. It is produced by perceived total visibility, when people believe that not only their presence, but small details, gestures, expressions, can be captured and revisited. Giorgi Lubaretsi confirms that identification may begin before reaching the protest site:

"It is realistic that demonstrators can be identified already in the metro, where it is much easier to capture faces - for example, on metro escalators. You can do reverse analysis too - how a person is dressed, how they move, where they came from."

Lubaretsi notes that identification doesn't necessarily begin at the protest site: *"It is realistic that demonstrators can be identified already in the metro, where it is much easier to capture faces - for example, on metro escalators. You can do reverse analysis too - how a person is dressed, how they move, where they came from."*

What this produced, in practice, was a shift in how people understood their own exposure. One demonstrator put it directly: *"Until recently, their surveillance capacity was limited - maybe they could monitor around 2,000 people, mostly important actors, which was somewhat reassuring for ordinary people. But with these new systems, they have unlimited possibilities. It has become cheaper. They can track even insignificant individuals. That's what makes it dangerous, even if you're doing nothing too harmful for the state."*

This transition from targeted surveillance to perceived mass traceability is where the chilling effect takes hold. The chilling effect doesn't require the system to work perfectly - it requires people to believe it might.

Changes in behavior and how self-censorship takes hold

Once the footage became real and people understood what the cameras could see and what the system could do with it, behavior changed. The change did not happen dramatically and not all at once - it accumulated.

One demonstrator stopped walking through the Parliament area entirely - not just during protests, but during ordinary days. *"The cameras there are very dense and it gives me anxiety. I take a longer route to work."* Her communication changed too. *"I reduced my Facebook communication to almost zero. Everything is on Signal now."*

Face masks produced their own form of unease. One demonstrator describes what the protest site felt like once covering up became common: *"I became less confident. Once everyone started wearing facemasks, the protest site became an anxious location for me. When you do not see faces, expressions, when you cannot recognize people, even friends - this is very stressful."* The measure people adopted for protection made the space feel less safe, not more.

A teacher, who continued attending throughout, watches the same process in herself. *"This is like retreating in a war, but not the end of the fight. The sparks are still alive."* But she uses the word "retreat".

One demonstrator walked home from a protest wearing a mask and stopped mid-route. *"I realized there was no point - I live nearby, a police officer could follow me and identify me anyway."* Another avoided the road itself: *"People were standing on the blocked road, but I crossed through the underground passage instead, out of fear."*

None of this meant people abandoned what they believed. As one demonstrator describes

it: *"For me protest is two things - physical, standing on Rustaveli, and internal, which you carry everywhere. You can tell the shop assistant, talk to the taxi driver. That physical part - it did shake for me."*

Why people reduced or stopped attending

Among the demonstrators interviewed, the decision to stop attending or pull back significantly was rarely a single moment. It built the same way the behavioural changes did.

The attorney Nika Simonishvili describes what the penalties numbers looked like from inside the courtroom: *"From my count, approximately 3,500 complaints have been filed with the city court. And that's not 3,500 fines - one complaint can cover five separate violations. The real number is much higher."* The outcome in court was consistent: *"In every case where the Interior Ministry brought a violation to court, the person was found guilty. One hundred percent. The best outcome you could hope for was a verbal warning."*

For those fined, the weight was not only the amount. *"It was impossible for me to pay the fine alone. I had to take more responsibility, I couldn't allow myself to get fined again and ask other demonstrators to help me pay. I prefer to avoid going to protest at all or being very careful."* A winemaker describes the same calculation differently: *"I couldn't ask my family to pay that amount. And I felt uncomfortable asking others for help. I knew other people were in worse situations than me."* A third: *"I have three fines. Every notification, every call from an unknown number, every time I had to go pick up documents - it's constant stress."*

The enforcement was also designed to be unpredictable. Fines arrived weeks or months after the fact, sometimes surfacing at a border crossing. *"Every time I leave the country, I do it with fear. I constantly feel that at some point I'll find out I've been fined again."* Simonishvili notes that fines were written in one month and delivered in another, and that disinformation about what was actually penalized spread in parallel. *"People couldn't figure out what they were being fined for and what they weren't. That uncertainty also did its job."*

In March 2025, the courts froze the support funds where people had been pooling money to cover penalties. *"When the funds were frozen and there was no longer hope of help paying fines, far fewer people came out. You can't blame them. In the end, some even had to take loans."* One demonstrator describes what solidarity had looked like before that point: *"At first, you could feel unity when people donated money for protesters to pay fines. But we know the financial situation is tough in this country and at some point, donations would stop. Students, waitresses, bartenders - at some point they were left alone. They did not manage to raise any money at all."*

For some, the breaking point was not the fines. *"That crossed a line I hadn't expected,"* one demonstrator says of the shift to administrative arrests. For a public servant with three small children, it was the criminalization of sidewalk protest. *"I felt it was a choice, but*

the right one, to preserve myself for my family and my country. There simply was no other way. Georgian Dream has followers who are unleashed - people who find purpose and financial reward in the physical destruction of anyone who thinks differently."

He does not describe it as defeat: *"These practices brought the protest to a minimum, but didn't defeat it. With cameras and arrests, they try to make the protest disappear - not in reality, but visually."*

Those who continued to protest, and on what terms

Not everyone pulled back in the same way, some kept coming throughout.

One respondent,, who accumulated four fines and kept attending, says: *"I'm genuinely confused about why people stopped because of the fines. You could cover your face, you could stand on the sidewalk - there were options. The quality of my life of course decreases day by day, but I do not see the way back."*

Another respondent, who also kept attending but less frequently, describes a similar practical adaptation. She found ways around the cameras, adjusted how she moved, changed what she wore. *"That recognition thing made me more careful. But it's not the reason I go less."* The reason she goes less has to do with other things - exhaustion, the changing shape of the protest, the frozen funds, the harder calculation of what showing up can accomplish at this stage.

The teacher never stopped framing each physical retreat as tactical. When road-blocking was penalized, she moved to the sidewalk. When sidewalk presence was penalized, she moved further back. Each step was a response to a specific legal change, not a retreat from the principle. *"The system tries to slow protest, split it, shift attention, spread the feeling that nothing will change anyway. Society splits more easily than a peach. But it hasn't managed to put out the fire. The sparks are still alive."*

What connects these people, and separates them from those who stopped, is partly about material conditions. One respondent raised her fine money in thirty minutes through her network. Another had comrades who collected hers. When that collective infrastructure was intact, the financial weight of enforcement (the mechanism that made surveillance operationally effective) could be partly absorbed. When protest support funds were frozen, even those who had stayed started going less. The chilling effect and the solidarity structure were directly connected all along.

4. The Infrastructure Behind Chilling Effect: How Russian Facial Recognition was Built and Deployed

The surveillance infrastructure that made protest identification possible was assembled over thirteen years, through five procurement cycles, from a single Russian vendor - and its implications extend well beyond the protests. The chapters that follow document what it can do and what it means for Georgian citizens' biometric data to sit inside Russian-manufactured architecture.

4.1 A decade in the making facial recognition surveillance layers

Georgia's facial recognition infrastructure was not built for the 2024 protests. It was built, upgraded, scaled across 13 years of public procurement.

დანართი №1 2013 წლის "4" - "09" - "2013" "სელ?"
შპს-ის მფლობელი

№	საქონლის დასახელება	საქონლის ძირითადი მახასიათებლები (ტექნიკური პარამეტრები)	რ
1	პაპილიონური საიდენტიფიკაციო სისტემა Papillon Polyface	ტექნიკური მახასიათებლები დანართი 2-ს შესაბამისად. პაპილიონური საიდენტიფიკაციო სისტემის შემადგენლობა და შესასრულებელი სამუშაოები: ერთი ერთეული სერვერის ლიფტინგით რომელიც ითვალისწინებს ცენტრალური პროცესორის 12 გამოთვლით ბირთვს, ასევე მონაცემთა ბაზას 500 000 პაპილიონური ბარათის ტევადობით და დღეში 500 ბარათის გამტარუნარიანობას; 20 მუშა სადგურის ლიფტინგით (მათგან 4 ერთეული ლიფტინგის ერთდროულად გამოყენების შესაძლებლობით); თითოეული სადგურის მონაცემთა ბაზას 20 000 პაპილიონური ბარათის მოცულობითი ტევადობით და დღეში 20 ბარათის გამტარუნარიანობით; - მწარმოებლის სპეციალისტი გამართავს პაპილიონური საიდენტიფიკაციო სისტემას ზემოაღნიშნული ცენტრალურ სერვერზე და მუშა სადგურებზე; - გამართავს ფაილების იმპორტის დამხმარე პროგრამას და გაუწევს დახმარებას პერსონალს არსებული ბაზის იმპორტირებაში; - ჩატარებს სპეციალისტების მოსამზადებელ 2 დღიან ტრენინგს კურსს. დამონტაჟდება გამზოვირედეტა დამკვეთის - შემსყიდველის მიერ წარმოდგენილ კომპიუტერულ პროგრამულ უზრუნველყოფის მინიმალური სისტემები მოთხოვნები: პროცესორი - Intel Core i3 2,6 Ghz; ოპერატიული - 2GB RAM; მყარი დისკი 320GB ROM; ვიდეოკარტა 128 MB Video. თითოეულ წარმოდგენილ კომპიუტერზე დაყენებული იქნება ლიფტინგებული პროგრამული უზრუნველყოფა.	

დამკვეთის მხრიდან:

შპს საფინანსო-სამეურნეო დეპარტამენტის
დირექტორის მთავარი

ოთარ დანელია

Figure 4: The Ministry of Internal Affairs signed its first contract with Polyface in 2013 - the earliest documented step in building Georgia's facial recognition infrastructure.

In April 2013, the Ministry of Internal Affairs acquired its first biometric face identification system, Polyface, under simplified state tender SPA130017726.⁴² The supplier was Papillon AO, headquartered in Miass, in Russia's Chelyabinsk Oblast.⁴³ The contract, shown in the picture, worth 125,000 GEL, specified a system capable of holding 500,000 fingerprint records, performing 2D face recognition, and cross-referencing faces directly against the criminal database - with linked personal records retrieved automatically when a match was found.⁴⁴ Inspection of the delivered system was assigned to the Forensic-Criminalistic and Computer-Technical Expertise Department. A two-day training course for ministry operators was included in the contract, indicating first-time deployment and immediate operational use.

Four upgrades followed. A May 2017 upgrade, worth 96,970 GEL, introduced Deep Learning CNN-based (Convolutional Neural Network) face recognition, the neural network approach used in large-scale surveillance systems worldwide.⁴⁵ It also added 3D facial composite tools and anthropological measurement integration.

CAPABILITIES	POLYFACE 2	POLYFACE 3
Face database capacity	Up to 5 million	Not limited
Automatic cropping and scaling	Yes	Yes
Automatic encoding		Yes
Automatic face detection		Yes
Group photo processing		Yes
Video file and video stream processing		Yes
Search using neural networks		Yes
Grouping of faces into black and white lists with automatic updates		Yes
Web interface (thin client)		Yes
Rest API		Yes

Table 2: *Polyface 3, supplied to Georgia's Ministry of Internal Affairs from 2018, marked a significant upgrade in mass surveillance capability over earlier versions.*

42. Agreement on state procurement N934 (4 September 2013), <https://tenders.procurement.gov.ge/public/library/files.php?mode=contract&file=71996> (25 May 2026)

43. Papillon Systems, <https://www.papillon.ru/>

44. Agreement on state procurement N934 (4 September 2013), <https://tenders.procurement.gov.ge/public/library/files.php?mode=contract&file=71996> (25 May 2026)

45. Agreement on state procurement N295 (24 April 2017), <https://tenders.procurement.gov.ge/public/library/contract.php?go=213938> (27 May 2026)

A 2018 upgrade, worth 91,750 GEL, added real-time face recognition from live surveillance camera streams and from archived video footage, with automatic matching against watchlists.⁴⁶ Licensing was extended to thirty simultaneous operators. Two features of this contract are worth noting. It was supplied directly by Papillon AO rather than through a Georgian intermediary, as in 2013. And training was delivered by Papillon specialists traveling from Russia. From 2018 onward, the ministry was operating a system specifically designed to process live camera feeds and identify faces in real time, and being trained on it by the manufacturer's own staff.

A 2020 upgrade for extending the service was procured for 146,856 GEL and a 2022 contract upgrade was valid through 2024.⁴⁷

The most recent contract was signed on October 10, 2024.⁴⁸ Protests began on Rustaveli Avenue on November 28. Delivery was specified for January 2025, by which point the systematic retrospective identification and fining of demonstrators had begun. The ministry was by then operating Polyface version 3.7.0. The 2024 contract is perpetual and has no expiry date.

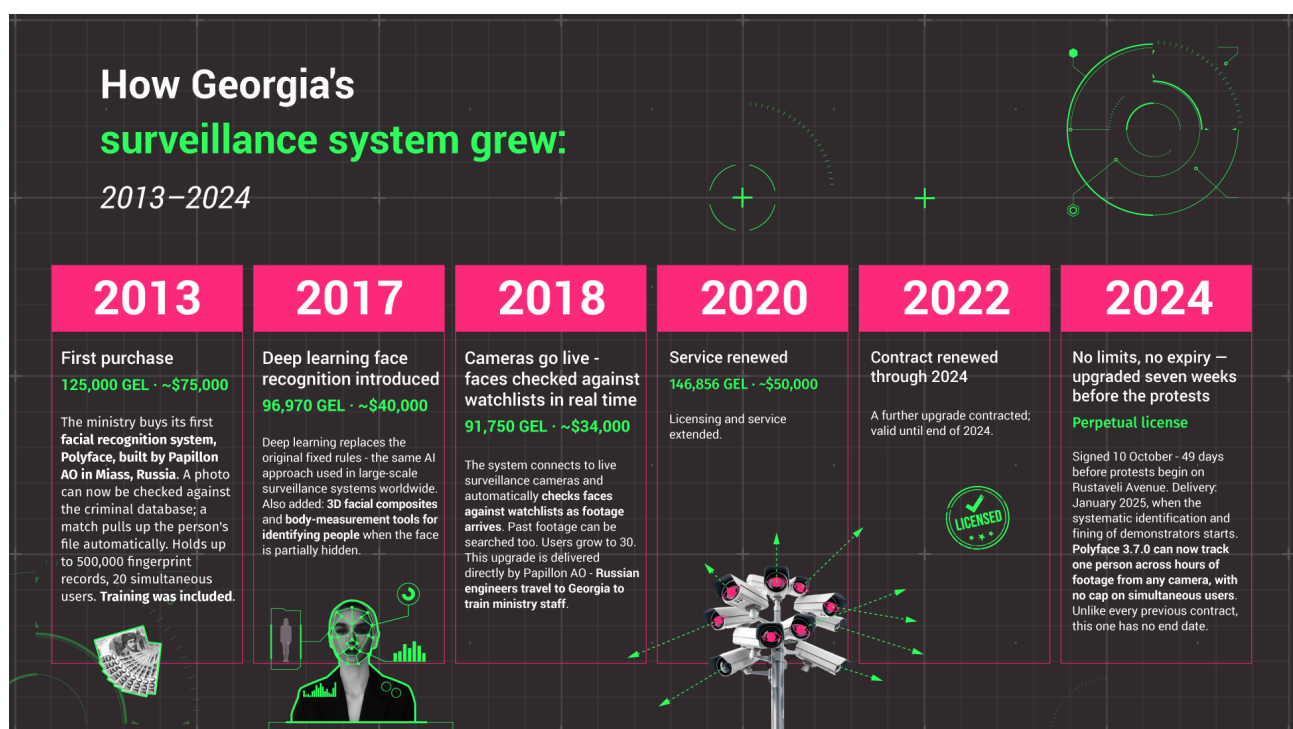


Figure 5: The timeline overviews contracts between the Papillon and Georgia's Internal Affairs Ministry

Source: AlgorithmWatch, CC BY 4.0.

46. Acceptance and Handover Act (2 October 2018), <https://tenders.procurement.gov.ge/public/library/files.php?mode=app&file=3034146&code=1539263877> (27 May 2026)

47. Minutes No. 2 of the Tender Commission Meeting of the Ministry of Internal Affairs of Georgia (14 July 2020), <https://tenders.procurement.gov.ge/public/library/files.php?mode=app&file=3905530&code=1594753524> (27 May 2026)

48. State Procurement Contract No. 1 (10 October 2024), <https://tenders.procurement.gov.ge/public/library/files.php?mode=contract&file=581514> (27 May 2026)

Analysis

The analysis builds on Polyface system features defined in contracts described above, as well as information available on Polyface demo at the Papillon's website.⁴⁹

According to the 2024 contract, the system can now track a single individual across long stretches of archived footage, taking one face and finding every moment that person appears across hours of video, across different cameras, angles, and days.⁵⁰ In practice, once a person is identified at one protest, the system can find them in every other protest recorded on camera.

The thirty-operator cap from 2018 is gone. Under the old contract, only thirty people (police officers) could use the system at the same time. The new contract specifies unlimited web interface users for photo-based identification, meaning any number of police officers can run searches in parallel. The 8,200 road-blocking violations registered under Article 174¹ during the Public Defender's 2025 reporting period would not have been technically achievable under the previous license.⁵¹

According to the 2024 contract, the system can also pull in footage from outside sources.⁵² Cameras on the street no longer need to be part of the same integrated system - video can be fed into Polyface software from anywhere: the 112 network, patrol police body and vehicle cameras, privately owned cameras connected to the state network. The 251 additional cameras purchased after December 2024, largely from Dahua, could be searched together with all the footage already stored.⁵³

The facial recognition market is not small. Ministries in comparable democracies have procured from Clearview AI, Amazon Rekognition, and Microsoft in the United States, NEC in Japan, IDEMIA in France, and Cognitec in Germany.⁵⁴ Across eleven years and at least five documented procurement cycles, the Georgian Ministry of Internal Affairs has not bought from any of them. It has bought, and kept buying, from Papillon AO.

For comparison: Moldova uses Cellebrite (Israeli) and LACE for facial recognition, supplied

49. Papillon Systems, 'POLYFACE Face Recognition System' <https://papillonsystems.com/products/programs/polyface/> (27 May 2026)

50. State Procurement Contract No. 1 (10 October 2024), <https://tenders.procurement.gov.ge/public/library/files.php?mode=contract&file=581514> (27 May 2026)

51. Public Defender of Georgia, 'Report of the Public Defender of Georgia, On the Situation of Protection of Human Rights and Freedoms in Georgia' (2025) <https://shorturl.at/7thPH> (27 May 2026)

52. State Procurement Contract No. 1 (10 October 2024), <https://tenders.procurement.gov.ge/public/library/files.php?mode=contract&file=581514> (27 May 2026)

53. OCCRP, 'Georgia's Surveillance Surge: Chinese Cameras Spark Protest Crackdown Fears' (28 March 2025) <https://www.occrp.org/en/news/georgias-surveillance-surge-chinese-cameras-spark-protest-crackdown-fears> (27 May 2026)

54. E. Jakubowska, A. Petrovski and D. Krivokapić, Beyond the face: Biometrics and society (2023), https://sharefoundation.info/wp-content/uploads/Beyond-the-Face_Biometrics-and-Society.pdf (27 May 2026)

through US government funding;⁵⁵ the Baltic states use EU-aligned vendors including Infotech, iProov, and SK ID Solutions;⁵⁶ Albania has contracted the UAE's Presight AI for its smart-city deployment;⁵⁷ Ukraine uses Clearview AI, supplied free of charge during the war;⁵⁸ and Serbia uses Chinese vendors including Huawei and Dahua.⁵⁹ None of these countries has procured its primary state facial recognition infrastructure from a Russian-headquartered vendor.

Papillon's systems are used primarily by Russian law enforcement and, as the company itself has advertised, by the Federal Security Service (FSB).⁶⁰ They are deployed in Russia, Tajikistan, Turkmenistan, Georgia, Kazakhstan, India, Turkey, and Belarus, and in the de facto Republic of Abkhazia, Georgian territory under Russian occupation.⁶¹ Russian law obliges domestic technology companies to cooperate with state intelligence services.⁶² A Georgian biometric system built, upgraded, serviced by a Russian company, and trained on by that company's personnel from 2018 onward, sits inside that legal obligation.

When Georgian whistleblowers first raised the question of whether citizens' biometric data was exposed to Russian access, the Ministry of Internal Affairs dismissed the concern as "an attempt to mislead the public and to deliberately discredit Georgian investigative and expert institutions."⁶³

The sections that follow examine what this system is technically capable of (4.2), how its capabilities align with the laws passed between December 2024 and March 2026 (4.4), and what it means for Georgian biometric data to sit inside Russian-manufactured architecture (4.5).

55. UNDP, 'Moldovan Police strengthens its capacities in cybercrime investigations; (9 February, 2026), <https://www.undp.org/moldova/press-releases/moldovan-police-strengthens-its-capacities-cybercrime-investigations> (27 May 2026)

56. Biometric Update, 'X Infotech wins Estonia deal for remote face, fingerprint biometric capture, verification' (17 November 2025), <https://www.biometricupdate.com/202511/x-infotech-wins-estonia-deal-for-remote-face-fingerprint-biometric-capture-verification> (27 May 2026)

57. Intellinews, 'Albania shifts to high-tech policing with expanded use of security cameras and surveillance drones' (21 September 2025), <https://shorturl.at/PH2Pt> (27 May 2026)

58. CNBC, 'Ukraine has started using Clearview AI's facial recognition during war' (13 March 2022), <https://shorturl.at/zFQsx> (27 May 2026)

59. Rferl, 'How Serbia Became Blanketed In Chinese-Made Surveillance Cameras' (30 July 2023), <https://www.rferl.org/a/serbia-surveillance-cameras-china/32526515.html> (27 May 2026)

60. BuzzFeednews, 'FBI Software For Analyzing Fingerprints Contains Russian-Made Code, Whistleblowers Say' (26 December 2017), <https://shorturl.at/rcJCA> (27 May 2026)

61. BuzzFeednews, 'FBI Software For Analyzing Fingerprints Contains Russian-Made Code, Whistleblowers Say' (26 December 2017), <https://shorturl.at/rcJCA> (27 May 2026)

62. 'SORM'<https://en.wikipedia.org/wiki/SORM> (29 May 2026)

63. Ministry of Internal Affairs, official Facebook page, (13 February 2026)

4.2 How facial recognition works in practice: cameras, software, and identification

Remote facial recognition is not one system. Cameras capture images, software converts faces into searchable records, state databases turn those records into names. Each layer is procured and maintained separately, and each is documented in public procurement. This section describes what sits in each layer and what the combination produces in practice.

The cameras

The Ministry of Internal Affairs and the State Security Service do not publish the number of cameras they operate. After protests began in December 2024, the state purchased 251 more, largely from Dahua.⁶⁴ Between 2019 and 2024, state spending on surveillance technologies increased thirteenfold, reaching approximately 5 million GEL, according to Civic Idea.⁶⁵

The hardware comes primarily from two Chinese companies: Hikvision and Dahua. Both are sanctioned by the United States.⁶⁶ Both operate under Chinese intelligence legislation that obliges them to cooperate with state authorities. A 2023 BBC experiment found that a professional hacker needed less than a minute to exploit Hikvision systems.⁶⁷

The specific models deployed on Rustaveli Avenue are not listed publicly. Based on what [Dahua](#) and [Hikvision](#) typically sell to state clients, the cameras used in urban surveillance are likely to include:

- High-resolution imaging, typically 4K (8 MP), able to capture faces and fine detail that can be enlarged afterwards
- Pan-tilt-zoom control with full horizontal rotation and vertical tilt
- Optical zoom of 25× to 40×, allowing close framing of individuals at distance
- Infrared illumination for low-light monitoring up to 200 metres or more
- Automated motion and face tracking

Mounted on elevated infrastructure, cameras with these specifications can observe crowd movement across roughly 500 metres and capture facial images usable for recognition

64. OCCRP, 'Georgia's Surveillance Surge: Chinese Cameras Spark Protest Crackdown Fears' (28 March 2025) <https://www.occrp.org/en/news/georgias-surveillance-surge-chinese-cameras-spark-protest-crackdown-fears> (27 May 2026)

65. A. Akhmedova, New challenge: Chinese surveillance cameras in Georgia, (Tbilisi 2025), <https://civicidea.ge/%E1%83%90%E1%83%AE%E1%83%90%E1%83%9A%E1%83%98-%E1%83%92%E1%83%90%E1%83%9B%E1%83%9D%E1%83%AC%E1%83%95%E1%83%94%E1%83%95%E1%83%90-%E1%83%A9%E1%83%98%E1%83%9C%E1%83%A3%E1%83%A0%E1%83%98-%E1%83%A1/> (25 May 2026)

66. U.S. Department of Commerce, Bureau of Industry and Security, "Addition of Certain Entities to the Entity List," 84 Fed. Reg. 54002 (October 9, 2019), <https://www.federalregister.gov/documents/2019/10/09/2019-22210/addition-of-certain-entities-to-the-entity-list>. (29 May 2026)

67. BBC, 'The tech flaw that lets hackers control surveillance cameras' (26 June 2023), <https://www.bbc.com/news/technology-65975446> (27 May 2026)

software from distances of 100 to 200 metres. For reference: end to end, the Rustaveli daily protest corridor measures 93 meters and up to 700 meters in case of large protests.

Recorded footage can also be digitally enlarged afterwards, so faces that were not deliberately framed at the time can still be extracted later.

What this looked like to the people on the ground was described in the previous chapter. One demonstrator said the footage shown in her case was clear enough to read text on a phone screen and on a piece of paper. Another said that even at the edge of the crowd, *“every expression, every smile, was clearly visible.”*

The software: Polyface

Polyface is the identification layer. It is an automated biometric face identification system developed by [Papillon AO](#). The version in use by the Georgian Ministry of Internal Affairs is 3.7.0, delivered in early 2025.⁶⁸ The system is built around a Deep Learning CNN recognition algorithm developed by 3DiVi.⁶⁹

According to Papillon’s published specifications and the features added across the Georgian procurement contracts (2013 contract⁷⁰, 2017 contract⁷¹, 2018 contract⁷², 2020 contract⁷³, 2024 contract⁷⁴), Polyface can:

- Verify whether a specific person matches a specific identity (1:1 verification)
- Search an unknown face against an entire database and return ranked candidate matches (1:N identification)
- Process live video from surveillance cameras and extract faces in real time
- Search stored archived video for the appearance of a specific face
- Recognize faces at angles and tilts, under partial coverage including masks
- Work with low-quality images, down to 30 pixels between the pupils
- Maintain watchlists of monitored individuals, exportable to mobile devices for field checks

68. State Procurement Contract No. 1 (10 October 2024), <https://tenders.procurement.gov.ge/public/library/files.php?mode=contract&file=581514> (27 May 2026)

69. Papillon Systems, ‘POLYFACE Face Recognition System’ <https://papillonsystems.com/products/programs/polyface/> (27 May 2026)

70. Agreement on state procurement N934 (4 September 2013), <https://tenders.procurement.gov.ge/public/library/files.php?mode=contract&file=71996> (25 May 2026)

71. Agreement on state procurement N295 (24 April 2017), <https://tenders.procurement.gov.ge/public/library/contract.php?go=213938> (27 May 2026)

72. Acceptance and Handover Act (2 October 2018), <https://tenders.procurement.gov.ge/public/library/files.php?mode=app&file=3034146&code=1539263877> (27 May 2026)

73. Minutes No. 2 of the Tender Commission Meeting of the Ministry of Internal Affairs of Georgia (14 July 2020), <https://tenders.procurement.gov.ge/public/library/files.php?mode=app&file=3905530&code=1594753524> (27 May 2026)

74. State Procurement Contract No. 1 (10 October 2024), <https://tenders.procurement.gov.ge/public/library/files.php?mode=contract&file=581514> (27 May 2026)

- Hold an unlimited number of biometric templates
- Connect to other Papillon products, including the company's fingerprint system and its 3D facial composite software

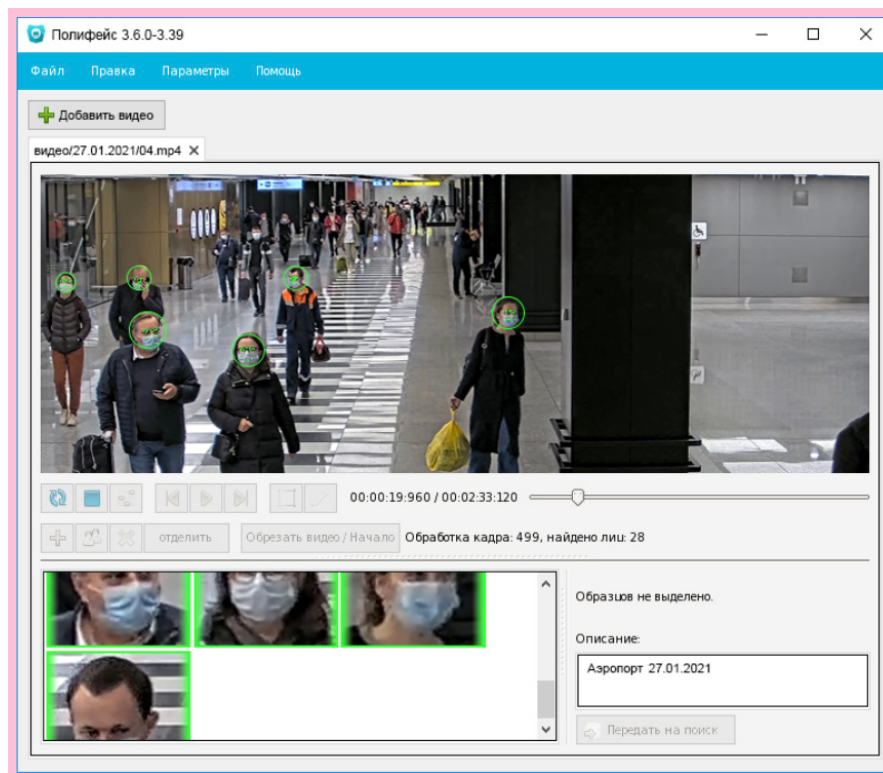
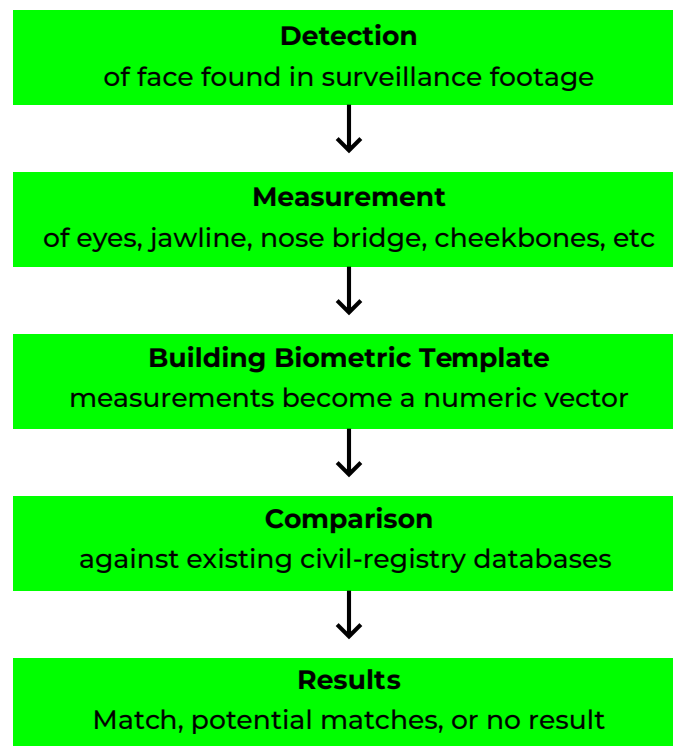


Figure 6: *Polyface demo showcasing its real-time identification features*

The step that turns surveillance footage into personal data happens inside Polyface. The system detects a face in a frame of video, measures the geometric relationships between reference points on the face - distance between the eyes, jawline shape, nose bridge, cheekbone structure - and converts those measurements into a numerical vector: the biometric template. The template is compared against templates already stored in the system, and Polyface returns either a match, a ranked list of candidates, or no result. The template is what is stored, searched, and matched. Under data protection law, it is personal data.



How the cameras and the software connect

The 2018 upgrade delivered by Papillon to the Ministry of Internal Affairs added real-time face recognition from live camera streams, along with face recognition from archived video files.⁷⁵ The 2024 upgrade added programmatic integration with external video archives, meaning footage can be loaded into Polyface from sources that are not themselves part of the Polyface system.⁷⁶

This is the technical bridge. Any camera connected to the 112 video management network - whether installed by the Ministry of Internal Affairs, by the patrol police, or by a private owner linked to the state network - can produce footage that Polyface can read and search, either live or afterwards.

The same works for still photos. Polyface can search any facial image against its stored templates, no matter where the image comes from. A photo from a Facebook profile, a tagged picture, a press photograph, or a screenshot from a video posted online can be loaded into the system and matched against protest footage, or added to a watchlist. What can be confirmed from procurement documents is that the capability exists, has been in place since 2018, and that cameras and software were operational. What cannot be confirmed from procurement documents alone is that any specific camera on Rustaveli Avenue feeds directly into Polyface. Polyface is, however, specifically designed for this kind

75. Acceptance and Handover Act (2 October 2018), <https://tenders.procurement.gov.ge/public/library/files.php?mode=app&file=3034146&code=1539263877> (27 May 2026)

76. State Procurement Contract No. 1 (10 October 2024), <https://tenders.procurement.gov.ge/public/library/files.php?mode=contract&file=581514> (27 May 2026)

of integration. Papillon's own product page and demo describes it plainly: the system "lets you populate your database with facial images recognized in streaming videos captured with surveillance cameras or downloaded video files."^{77,78}

What the cameras are doing on Rustaveli

Footage taken from cameras that we have accessed shows them behaving in two distinct ways. In some recordings, a camera fixes on a well-known activist or journalist and tracks them. In others, a camera moves between faces standing next to each other, pausing on each for a few seconds before moving on.



Figure 7: *In the first footage, the camera seems to be run by a human operator, for observing more active demonstrators who create the protest atmosphere. In the second footage, the camera seems to automatically stop at random faces for a few seconds - once look up, turn around, or just make their faces visible to collect pixels, the camera captures it and then moves to the other random demonstrator. This indicates that installed cameras at the Rustaveli protest corridor may have different functions - some capture general crowd movements, some track automatically, some manually.*

These are not the same behaviour, and they correspond to different modes of use that Polyface supports:

- **Automated capture:** Polyface's Video Recognition Tool detects faces in a video stream automatically and holds each face in frame long enough to extract a reliable biometric template before moving to the next. The few-second pause is the time the system needs to capture enough frames.
- **Operator-directed search:** A human operator steers a PTZ camera onto a specific person, runs a database search in real time, and moves to the next face. The 2018 contract licensed thirty simultaneous operators.⁷⁹ The 2024 contract⁸⁰ removed that

77. Papillon Systems, 'POLYFACE Face Recognition System' <https://papillonsystems.com/products/programs/polyface/> (27 May 2026)

78. POLYFACE Face Recognition System, YouTube (Uploaded 16 May 2022) <https://www.youtube.com/watch?v=5zr1Ptd1e4o> (27 May 2026)

79. Acceptance and Handover Act (2 October 2018), <https://tenders.procurement.gov.ge/public/library/files.php?mode=app&file=3034146&code=1539263877> (27 May 2026)

80. State Procurement Contract No. 1 (10 October 2024), <https://tenders.procurement.gov.ge/public/library/files.php?mode=contract&file=581514> (27 May 2026)

cap and an unlimited number of operators can run it. Several footages taken from the cameras acquired for this report shows that the camera tracks and zooms in to the person that initiates road blocking, or chants for creating atmosphere, which is likely to indicate that those specific cameras are run by human operators manually.

- **Watchlist alerting:** A list of individuals of interest - activists, organizers, previously fined persons, people flagged through prior intelligence - is pre-loaded into the system. When the camera feed detects a matching face, Polyface alerts the operator. This capability has been supported since the 2013 procurement.⁸¹

All three modes are documented Polyface capabilities.⁸² All are consistent with the observed camera behaviour. There is no technical reason they cannot run in parallel, on different cameras or at different times.

What turns an image into a name

Polyface can produce a match. It cannot, on its own, produce a name. For identification to be actionable, the facial template extracted from surveillance footage has to be compared against a reference database that links a face to an identity.

The Public Service Development Agency, under the Ministry of Justice, holds that database.⁸³ It contains the national ID and passport registry, facial images and fingerprints of the entire Georgian population, and the population registry with address and family links. Any Georgian citizen who has been issued an ID card or a passport has a facial image and a set of biometric identifiers stored in a state system that Polyface can compare against.

This is the step that converts an unknown face in a crowd into a named individual with an address, a phone number on record, a tax history, and a family structure.

The enforcement pattern observed from December 2024 onward - some fines issued within days, others months later, some delivered only at a border crossing - fits both real-time identification and retrospective analysis of archived footage. The infrastructure supports both. Court documents, as the interviewed attorney in the previous chapter noted, do not specify which. They identify the tool only as “special software.”

4.3 How law formalizes surveillance

The facial recognition infrastructure described in the previous sections was operational well before the 2024 protests. The technology did not change between December 2024 and

81. Agreement on state procurement N934 (4 September 2013), <https://tenders.procurement.gov.ge/public/library/files.php?mode=contract&file=71996> (25 May 2026)

82. Papillon Systems, ‘POLYFACE Face Recognition System’ <https://papillonsystems.com/products/programs/polyface/> (27 May 2026)

83. SDA, Guarantees for lawful processing and protection of personal data, <https://sda.gov.ge/en/guarantees-for-lawful-processing-and-protection-of-personal-data/> (27 May 2026)

March 2026. The legal framework did. Each amendment in that period released a capability that had been technically available for years.

In February 2025, amendments to the Administrative Offenses Code gave authorities formal powers to photograph suspected violators, collect fingerprints, record voices, and take identification measures.⁸⁴ Identification and fining of protesters had begun in December 2024. The February amendments provided retrospective legal cover for a practice already months underway.

The operational instrument is Minister of Internal Affairs Order No. 73, “On the approval of the rule for conducting identification measures, including verification through a special electronic program.” Order 73 authorizes officers to photograph a person and cross-check the image against ministry databases through the electronic program.⁸⁵ The ministry’s own 2021 Intelligence-Led Policing strategy, signed by the Minister of Internal Affairs on 11 July 2021, identifies that program by name and it is Polyface.⁸⁶

Order 73 was issued under Article 20 of the Police Law, which permits identification measures only in the circumstances described in Article 19.⁸⁷ Article 19 requires an officer, in the interest of public safety, to first attempt to identify a person directly, by stopping them and requesting their identification documents. In the protest cases reviewed by Rights Georgia, this step did not happen.⁸⁸ Officers went directly to biometric processing. The less intrusive measure the law prescribes was skipped.

The procedural mechanism that converts a Polyface match into an enforcement case is Article 174¹ of the Administrative Offenses Code, the road-blocking provision.⁸⁹ The Public Defender’s 2025 annual report records 8,200 violations registered under this article during the reporting period, most of them built on footage-based identification.⁹⁰ As the interviewed attorney in chapter two observed, the Interior Ministry wins every case it brings to court. *“The best outcome you could hope for was a verbal warning.”*

The transfer of footage between the 112 emergency service and the police departments that run the identifications takes place without judicial oversight. Case files reviewed by

84. Socialjustice.org.ge, ‘Social Justice Center will Dispute the Legality of Using Facial Recognition Technology to Fine Citizens’ (19 March 2025), <https://shorturl.at/hY7oU> (27 May 2026)

85. Mass Surveillance: Accountability of the Personal Data Protection Service, (2025), <https://drive.google.com/file/d/1JLS6kZJS6jyxfHhH0Wqpg2IL8MvUCex9/view> (25 May 2026)

86. Order of the Ministry of Internal Affairs of Georgia, On the Approval of the Strategy for the Development of Intelligence-Led Policing (ILP) (2021–2025), (11 July 2021), <https://info.police.ge/uploads/63f38bcd3981f.pdf> (25 May 2026)

87. Police Law of Georgia (2013) <https://matsne.gov.ge/en/document/view/2047533?publication=41> (27 May 2026)

88. Mass Surveillance: Accountability of the Personal Data Protection Service, (2025), <https://drive.google.com/file/d/1JLS6kZJS6jyxfHhH0Wqpg2IL8MvUCex9/view> (25 May 2026)

89. LAW OF GEORGIA GENERAL ADMINISTRATIVE CODE OF GEORGIA (1999), <https://matsne.gov.ge/en/document/view/16270?publication=45> (27 May 2026)

90. Public Defender of Georgia, ‘Report of the Public Defender of Georgia, On the Situation of Protection of Human Rights and Freedoms in Georgia’ (2025) <https://shorturl.at/7thPH> (27 May 2026)

Rights Georgia show that the Patrol Police or the Tbilisi Police Department send 112 a simple written letter, citing no legal basis and accompanied by no court order.⁹¹ 112 then transfers the video. For stored computer data in a criminal investigation, the Criminal Procedure Code requires a judge's ruling. The Administrative Offenses Code has no such provision.

Biometric data on thousands of protesters moves between state agencies on the strength of internal correspondence.

Once the identification is made, the data stays. Under Interior Ministry Order No. 271 of 2006, administrative violations under Article 174¹ are held in active records for eight years, archived for a further twenty years, and retained in depersonalized form after that, so twenty-eight years at minimum.⁹² Under Article 39 of the same code, a person is considered to have no administrative penalty on their record one year after paying the fine. The legal consequence ends after a year, but the data persists for a generation.

Georgia's Personal Data Protection Law, in force since March 2024, requires a Data Protection Impact Assessment before any deployment involving new technologies, biometric processing, or systematic monitoring of public gatherings.⁹³ The Personal Data Protection Service uses precisely this scenario, "smart surveillance in public gathering places, using AI for monitoring," as the illustrative example in its own DPIA guidance. There is no public record that such an assessment was conducted for the cameras along Rustaveli.

By March 2026, the repressive regulatory framework had escalated further.⁹⁴ Road and sidewalk blocking became criminal offenses. Demonstrations now require pre-registration and state approval. Pre-registration makes facial identification partly redundant: the state already has organizers' names on a form before the protest happens.

4.4 Procured from Moscow: The Strategic Risk of Georgia's Surveillance Vendor

The Georgian Ministry of Internal Affairs has been procuring from Papillon AO since 2013.⁹⁵ Across eleven years, the ministry went through five procurement cycles. The 2013 deployment was supplied through a Georgian intermediary, Ltd My Mobile+, which has won

91. Mass Surveillance: Accountability of the Personal Data Protection Service, (2025), <https://drive.google.com/file/d/1JLS6kZJS6jyxfHhH0Wqpg2IL8MvJCex9/view> (25 May 2026)

92. Mass Surveillance: Accountability of the Personal Data Protection Service, (2025), <https://drive.google.com/file/d/1JLS6kZJS6jyxfHhH0Wqpg2IL8MvJCex9/view> (25 May 2026)

93. Law of Georgia on Personal Data Protection (2011), <https://matsne.gov.ge/en/document/view/1561437?publication=23> (27 May 2026)

94. Transparency Georgia, 'De Facto Abolition of Freedom of Assembly – A Law Turned into a Repressive Mechanism' (4 November 2025), <https://shorturl.at/EOAZp> (25 May 2026)

95. Agreement on state procurement N934 (4 September 2013), <https://tenders.procurement.gov.ge/public/library/files.php?mode=contract&file=71996> (25 May 2026)

tenders worth more than 38 million GEL in total from the state.⁹⁶ From 2018 onward, the supplier has been Papillon AO directly, with training delivered by specialists traveling from Russia. On 10 October 2024, the ministry signed a perpetual licence, with no expiry date.

A system was upgraded five times over eleven years, serviced by personnel from the manufacturer, with training delivered directly to ministry staff.⁹⁷ It has survived changes of Ministers in the Internal Affairs Ministry and changes of Prime Ministers. Despite the 2008 war, the de facto annexation of twenty percent of Georgian territory, the sanctioning of Russian state-linked technology across Europe and the United States, and the post-2022 shift of much of the democratic world away from Russian suppliers, the partnership has not been reconsidered.

Eto Buziashvili, a researcher at the Atlantic Council's Digital Forensic Research Lab, frames the problem in strategic terms:

"Papillon Systems represents a core part of Russian security infrastructure. Integrating this kind of Russian-developed biometric technologies into national infrastructure represents a substantial risk to Georgia's national security and is also an instrument of hybrid warfare against the country. In the context of hybrid warfare, deploying adversarial AI surveillance is a mechanism for long-term dominance over another country's citizens in the information domain."

A breach of a password database is recoverable, but a breach of a biometric database is not.

"When a civilian technology starts to process non-fungible data, for example, biometrics, in a black-box type environment, it transitions from being just a technology to being a point of potential security vulnerability. Unlike a password, a face or a fingerprint can't be changed. If that data is compromised through a vendor-side backdoor, then the vulnerability is permanent."

The ministry does not publicly audit Polyface's source code, and the code is not available for audit for public experts. The system has been bought from a company based in Russia, where the law requires technology firms to cooperate with state security services. What runs inside the system, and what it sends back, cannot be checked from Georgia.

Giorgi Lubaretsi, a cybersecurity expert, describes what independent verification would require.

"For a security or algorithmic audit, you need full access to the system. You check the software, you see where the servers are located, where the data is stored, and you may need continuous access. That is the industry standard."

He is direct about whether this has been possible in Georgia.

96. Tendermonitor, Mai Mobail + Tenders, <https://tendermonitor.ge/en/organization/31301> (27 May 2026)

97. Acceptance and Handover Act (2 October 2018), <https://tenders.procurement.gov.ge/public/library/files.php?mode=app&file=3034146&code=1539263877> (27 May 2026)

“Access to their systems is a big no from the Ministry of Internal Affairs. We saw it with the CEC machines during the elections - the audit was superficial, and when there were requests to actually study what the systems were doing, no real audit happened. No independent expert was allowed to verify how the machines work. Nothing was published.”

The ministry has publicly defended Polyface on the grounds that data is held on physical servers disconnected from the internet.⁹⁸ Lubaretsi notes that this claim, on its own, does not establish what the ministry says it establishes.

“If the device is not connected to the internet, the data cannot reach Papillon. But this needs proper protection. It is not as simple as ‘I didn’t connect it to the internet, so that’s it.’ There are specific protocols that have to be followed.”

Buziashvili places this technical uncertainty within the legal framework that makes it consequential.

“Any software that is produced under the jurisdiction of an adversarial state, where such state can legally compel company to cooperate - for instance, the FSB’s authority over Russian tech firms - operates as a persistent and high-access sensor to that adversarial power, turning another country’s security apparatus into a satellite of their own. When a nation-state is dependent on Russian state-linked AI, it allows Russia to export a surveillance model that matches its own authoritarian internal controls and erodes the sovereignty of the host nation.”

The Kaspersky Lab precedent is directly on point.⁹⁹ Kaspersky produces antivirus software, a lower-sensitivity product than biometric identification. The United States banned Kaspersky from federal networks in 2017. Germany issued a formal warning against its use in March 2022. Several other European governments have followed. In each case, the reasoning was the same: a Russian-jurisdiction company cannot guarantee the independence of its systems from Russian state access. The product did not have to be shown to be compromised, the jurisdiction was sufficient. Papillon sits in the same legal position, with a product that processes a more sensitive class of data and is marketed explicitly to law enforcement.

Buziashvili identifies two distinct risks:

“Russian AI surveillance systems’ ‘backdoor’ provides opportunity for data to be taken from Georgian infrastructure, while integrity attacks could involve software being programmed to ‘ignore’ particular individuals - for example, to ignore a foreign intelligence officer of a hostile country, while creating a detailed map of the power structure within the host country, from high level officials down to grassroots activists, and selectively target political dissent.”

“When an adversary gets access to facial recognition archives, it makes them able to use the facial recognition database for intelligence profiling. Biometric capture had a tragic example

98. Ministry of Internal Affairs, official Facebook page, (13 February 2026)

99. ‘Kaspersky and the Russian government’ https://en.wikipedia.org/wiki/Kaspersky_and_the_Russian_government (29 May 2026)

during the Taliban's takeover in Afghanistan, when they inherited US-built biometric systems to identify and target US's local allies."

The Afghan example matters because the system was not built for bad purposes.¹⁰⁰ The US military collected biometric data - iris scans, fingerprints, facial images - to verify identities at checkpoints, screen recruits, and disrupt insurgent networks. The core database sat on secure Department of Defense servers, but handheld devices known as HIIDE held local copies of profiles, including of Afghans working with coalition forces. During the Taliban's August 2021 offensive, these devices were seized from Afghan government forces, along with US-built Afghan identity and payroll databases containing biometric records on an estimated 2.5 million people. Human Rights Watch subsequently documented cases of Taliban forces using HIIDE devices at checkpoints and during home raids to identify former security personnel. A system built to protect one group of people became a tool to hunt them. The technology stays the same; who controls it changes.

"We also have a historic example of the use of imported technology as a tool of state influence and it happened during Russia's invasion of Georgia in 2008 when Georgian internet traffic was re-routed through Russia's servers and it was used as a main tactic to isolate the Georgian government and control the narrative."

In 2008, the concern was how internet traffic was routed. In 2025, it is how faces are identified. The technology is different. The logic is the same: whoever controls the system controls what passes through it.

"In a worst-case scenario, biometric data collected now serves as a library of targeting and blackmail for future potential conflicts or in various other situations. For Georgia, the risk is that this information could facilitate digital or physical purges, or high-precision blackmail. Even if no abuse can be shown today, the fact that there is access to this data enables a hostile state the ability to unmask, track and neutralize any political opposition with a keystroke."

The decision to procure Polyface from Papillon, upgrade it five times, accept training from Russian personnel on Georgian territory, and sign a perpetual licence in October 2024 is a decision about the architecture of Georgian state power. As of May 2026, critical components of that architecture remain under the jurisdiction of the state that occupies Georgian territory - Russia.

100. HRW, 'New Evidence that Biometric Data Systems Imperil Afghans, Taliban Now Control Systems with Sensitive Personal Information' (2 September 2025), <https://www.hrw.org/news/2022/03/30/new-evidence-biometric-data-systems-imperil-afghans> (27 May 2026)

5. Emerging Surveillance Practices: A First Look on Elections, the Church, and Mental Health Issues

The protests on Rustaveli Avenue were the most visible application of the surveillance infrastructure described in the preceding chapters, but they were not the only one. The same state that tracked demonstrators through facial recognition has compiled dossiers on bishops, converted welfare rolls into electoral leverage, and passed a psychiatric registry law initiated not by clinicians but by the Ministry of Internal Affairs. This chapter examines three of those settings - elections, the Orthodox Church, and mental health - where personal data functions as a tool of political control in domains of Georgian life that extend well beyond protest.

5.1 Personal Data for Social Control: Electoral Practices

Elections are one of the clearest settings in which personal data becomes a tool of political control in Georgia. The issue is not that political parties use voter information; this is common across democracies. The issue is that personal data is assembled from across state institutions and party networks in ways that sort citizens into categories: loyal, disloyal, persuadable, and vulnerable. Once people are sorted, the information is used to reward or pressure them. This section traces that pattern - the production of political files on individuals, the use of social programmes as leverage, and the monitoring of voters on election day.

From voter lists to political files

Electoral subjects in Georgia have lawful access to the unified voter registry, which covers roughly 3.5 million people. Access is formally regulated: registered electoral subjects and observer organisations can obtain the list under a written agreement with the election administration, restricting its use to legal purposes and to the framework of Georgian data protection law.

In practice, as an election observer and investigator interviewed for this report explained, the safeguards are undermined by simple scale: *“this unified voter list, the data of three and a half million people, ends up in the hands of very many people, because there can be several electoral subjects, then their staff, and so on.”* Once every voter is identifiable at scale, richer profiling becomes possible.

The more serious problem, according to the same observer, is not the registry itself but what is built around it. *“The biggest problem we face in the pre-election period,”* they said, *“is the various political and party activities aimed at identifying supporters,”* carried out mainly by ruling-party coordinators and local municipalities. The profiling runs at household level and draws on a wide range of indicators. The observer described the tasks routinely assigned to coordinators: identifying *“who has a family member in prison, determining the level of vulnerability household by household, who has had a driving licence revoked in their area of operation, whose child is of conscription age or currently performing compulsory military service, who is abroad, information about income,”* along with religious identity in at least one case they had encountered. Data flows into this system from multiple state sources: the Ministry of Internal Affairs (records of detention, fines, and licence revocations), the Ministry of Foreign Affairs (persons registered with consulates abroad), the Penitentiary and Justice ministries (persons in detention), the Ministry of Health (including psychiatric placement), and the Social Service Agency’s unified register, which, the observer estimated, holds the records of *“around 700,000 people who receive social assistance.”*¹⁰¹ They were explicit that the underlying figure, the profile, is political: *“these data are then used to identify whether a person is likely to be considered a supporter or an opponent of the ruling party.”*

The scale of the operation is significant. Asked how many people were involved, the observer estimated *“somewhere around 15,000 people - coordinators and those party types who work on elections.”* They also confirmed that the entire electorate of each precinct is divided up among these operatives in advance, to the point that, on election day, *“the party knows how many of its supporters have shown up, who has not shown up, and so on. This control is quite refined.”*

The “Gogashvili files” show what this kind of profiling looks like when documented.¹⁰² The materials, handed to Transparency International Georgia and ISFED by the former deputy head of the State Security Service, Iosef Gogashvili, describe a scheme in which state institutions were used to collect personal information on budget-sector employees and other citizens, and to convert that information into electoral pressure. According to Radio Free Europe/Radio Liberty’s summary of the NGO analysis, the documents include political dossiers on school directors, education resource-centre staff, and other public-sector employees, in which political orientation, relatives’ political activity, neutrality, and “electoral resource” were treated as decisive variables.¹⁰³ One director was described in the competence column as energetic, talented, hard-working; in the next column the same person was marked as having the “wrong political orientation”; the party’s assessment was “negative”; the State Security Service concluded: “oppositionally minded, not recommended to appoint.” The operative category is not professional performance but political reliability.

101. ‘Why is “Georgian Dream” Reviewing Socially Vulnerable Families Whom it “Uses for Political Control”?’ (Batumelebi, 13 May 2026), <https://batumelebi.netgazeti.ge/news/615902> (4 June 2026)

102. ‘How to Collect Electoral Votes – the Ruling Team’s Recipe from the “Gogashvili Files”’ (Radio Free Europe/Radio Liberty – Radio Tavisupleba, 22 July 2022), <https://www.radiotavisupleba.ge/a/31955411.html> (4 June 2026)

103. *ibid*

Between autumn 2020 and August 2021, the Ministry of Education did not reappoint at least 112 public-school directors after their terms expired. Of the 95 directors assessed in the leaked materials, resource centres rated 29 negatively, the ruling party rated 80 negatively, and the State Security Service rated 89 negatively - an overlap that points to a shared evaluation process rather than independent state judgment.

The Gogashvili files also show how requests to adjust individual citizens' legal situations in exchange for votes flowed through state channels. Between October 2018 and January 2019, lists of around 900 people with suspended or revoked driving licences and around 1,700 probationers were reportedly sent from the email address securgd@gmail.com to senior officials, including the then Deputy Minister of Justice Giorgi Pataridze and the head of the Ministry of Internal Affairs General Inspection, Alexander Khojevanishvili. The notes attached to individual names are explicit: one person's licence should be restored because "he helps us in Mukhiani"; another, because he "helps us in Gldani village." The same pattern applied to requests to cancel conditional sentences, reduce criminal charges, defer military service, or improve prison conditions - for example, transferring a detainee closer to home so that his street's residents would support the party. Data later obtained from the National Probation Agency confirms a sharp spike in decisions to cancel conditional sentences in November and December 2018, during the second round of the presidential election: the permanent commission that normally met once a month met thirteen times in those two months.¹⁰⁴

What matters analytically is not the favour itself. It is that each transaction depends on accurate, individualised information - who is charged with what, who has what kind of family, who can mobilise how many voters on which street.

Welfare and employment as leverage

The second layer is social policy. In March 2022, the government launched a public works programme that employed socially vulnerable citizens on a monthly salary of 300 GEL while they continued to receive assistance. The Employment Agency's 2022 parliamentary report stated that 71,319 citizens applied and 29,323 were employed in the first year; by 2025 the figure had risen to roughly 40,000. Reporting by Batumelebi documented how the programme worked on the ground.¹⁰⁵ In the village of Zvare, a settlement of 57 registered households, twelve socially vulnerable people were hired as cleaners. In Barataui, five people were assigned to clean a single village administrative building. In Tsoniarisi, two were assigned to "guard" a Soviet-era tank standing in the village centre.

104. *ibid*

105. "I Am a Georgian Dream Coordinator" – the Scheme to Employ 30,000 Socially Vulnerable People Ahead of Elections' (Batumelebi 11 May 2023), <https://batumelebi.netgazeti.ge/news/477949/> (4 June 2026)



Figure 8: *Soviet-era tank in Tsoniarisi, guarded by two persons from a public works programme*

Several interviewees struggled to explain their daily tasks. One employed beneficiary, Nana Gatenadze, said on record: “I am in Georgian Dream, I work as a coordinator.”¹⁰⁶ Another, Teona Shavadze, employed in a kindergarten, described having been a Georgian Dream coordinator in every election. Employees were typically assigned work by the local mayor’s representative rather than by any conventional employer. The observer interviewed for this report described the same dynamic from the coordinator’s side: in parallel with political pressure and welfare-style benefits, *“coordinators also distribute money directly to families. There were several cases in which it was written down exactly which family should receive how much.”*

The political function of the programme became harder to deny when it ended - and harder still when the Prime Minister explained why. In December 2025, after the 2024 parliamentary elections, the government announced that the 2026 budget would not include funding for the scheme. Asked in 2026 why employment figures had fallen, Prime Minister Kobakhidze attributed the decline directly to the programme’s cancellation, describing it as “fictitious” employment: around 30,000 people, he said, had been counted as employed while continuing to receive social assistance. He called the cancellation “an absolutely correct step.” The characterisation is striking. For four years and roughly 377 million GEL in budget expenditure, the government ran a programme its own Prime Minister would later describe as fictitious - one that grew steadily through each electoral year and was terminated the month elections closed. Salome Shubladze of the Social Justice Center told Batumelebi that the programme had been designed to match the electoral cycle and that employees

106. *ibid*

had reported being asked directly for political support;¹⁰⁷ once the elections closed, they were abandoned. The budget trajectory is consistent: approximately 48 million GEL in 2022, 107 million in 2023, 109 million in 2024, and 112 million in 2025 - rising through the electoral period and terminated immediately after.

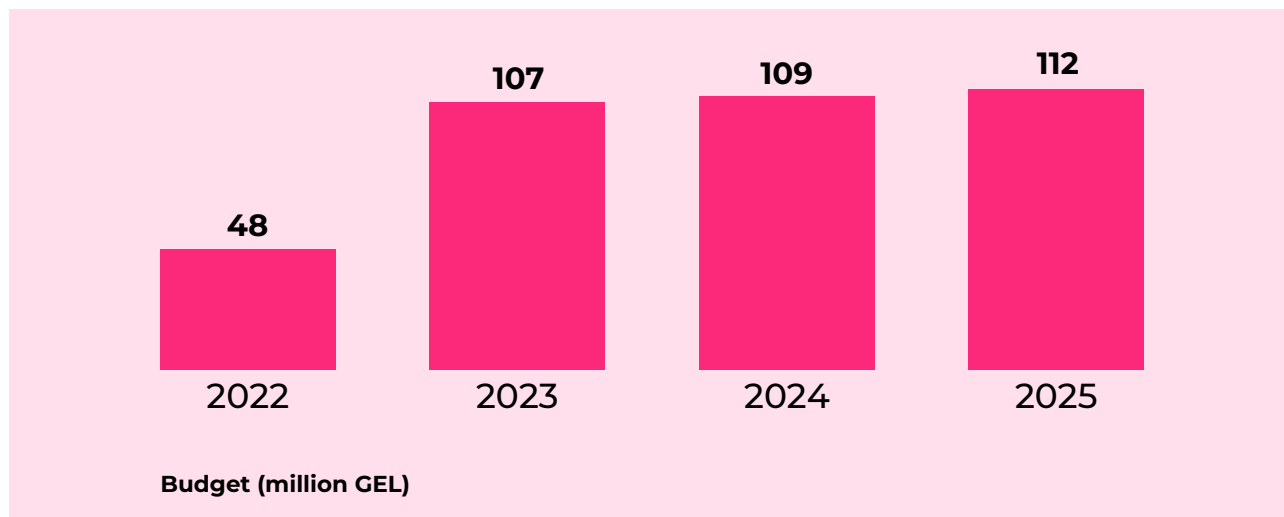


Figure 9: *Budget spent on a public works programme*

What makes this relevant to using personal data for social control is the information environment around the programme. Benefit eligibility, household status are administrative data. Once they are mediated by local officials with partisan loyalties, that data becomes part of an electoral control architecture. The recipient does not have to be threatened - when people feel their income depends on the ruling party's goodwill, their support follows without anyone having to ask.

Captains and election-day monitoring

An investigation by TV Pirveli, published after the October 2024 parliamentary elections, documented the election-day side of the same architecture.¹⁰⁸ According to internal Georgian Dream text and voice messages obtained by the journalists, the ruling party operated call centres near polling stations on election day. Around 6,000 people were registered on a purpose-built platform as "captains." Each captain managed a group of agitators assigned to a specific polling station. One such call centre was reportedly located in the director's office of Tbilisi's 30th public school, where an official polling station was also open.

The operational loop was simple. Agitators called citizens from pre-prepared lists and asked them to come and vote. Captains supervised the agitators. Call-centre operators entered into a database the names of citizens who had come to vote and who, according to the

107. 'Why Did "Georgian Dream" Cancel the 300-Lari Employment for the Socially Vulnerable – "After the Elections, They Abandoned Them"' (Batumelebi 2 December 2025), <https://batumelebi.netgazeti.ge/slideshow/597330/> (4 June 2026)

108. 'Exclusive: Who Are the Captains of the Captains? – New Evidence' (TV Pirveli, 9 November 2024), <https://tvpirveli.ge/ka/siaxleebi/politika/85398-eqskluzivi-vin-arian-kapitnebis-kapitnebi-akhali-mtkitsebulebebi> (4 June 2026)

investigation, had marked number 41 - the ruling party's ballot number; this data was visible in real time to the party's central office. A prominent lawyer, Alexander Kobaidze, confirmed to the journalists that he had served as a captain; his role, he said, was to maintain "maximum communication" with supporters on his list. A follow-up report described a second tier. In the Kvemo Kartli region, captains were coordinated by a public official, Daur Ismailov. Above him, Nino Kharaishvili, head of Marneuli municipality's social service, is described in the materials as the "captain of captains," reporting in turn to Amiran Giorgadze, chair of the Marneuli municipal assembly. One responsible person, Asid Samarov, an employee of a village school, said he had been given fuel coupons in exchange for bringing voters to the polling station. The journalists also obtained recordings in which captains were pressured by superiors to produce voter lists and were threatened with consequences if they had not met their targets. Payments to call-centre workers, including minors according to the investigation, were reportedly made in cash, outside the banking system.

For the observer interviewed for this report, what TV Pirveli documented was an unusually vivid case of a long-standing practice. Asked about the captains system, they noted: *"there was nothing particularly extraordinary there, if you ask me. Dividing the party resource in such a way that data could be collected in real time has always been their weapon, their card, so to speak."* They also pointed to the party's access to an additional stream of information during the day itself: the signed precinct lists recording which voters have turned up. That information is formally available only to the election administration, but, the observer said, *"for Georgian Dream this is also an important lever: it knows who has come and who has not, and whom it needs to work on."*

What was new in 2024, in the observer's account, was not the tracking itself but its scale and its second use. Beyond mobilising supporters, the ruling party worked to demobilise opponents. *"The ruling party ensured,"* they said, *"that some portion of opposition-party supporters, as many as might have given the opposition an advantage, were left at home."* The methods described included confiscating ID documents from people whose loyalty could not be assumed, "renting" IDs in exchange for money where there was no confidence the person would vote for the ruling party, turning voters away from polling stations, and intimidation by groups *"including representatives of the criminal underworld."* The observer called the election day itself *"very aggressive, effectively not peaceful at the precincts, with mobilised groups that had existed at every previous election, but on a scale that had not been seen before."* For any of this to work selectively, household-level lists distinguishing likely supporters from likely opponents had to exist in advance. That is what the profiling was for.

Taken together, these practices erode the social meaning of ballot secrecy. Formal secrecy in the polling booth may remain intact, but secrecy is also a social and psychological condition: it depends on voters believing that their choice cannot be inferred or punished. Once parties hold household-level voter lists, cross-reference multiple state databases, run call centres to mobilise specifically identified voters, receive real-time information on who has voted, and reward or penalise public employees based on political files, the belief

that one's vote is unobservable begins to weaken. This matters most for citizens whose lives are already legible to administrative and party networks - public-sector employees, beneficiaries of social programmes, probationers, residents of small villages where the local coordinator knows every household, and those with relatives in detention, abroad, or on the social assistance register. Personal data, in this system, is what makes the framework possible.

5.2 Personal Data for Social Control: Faith and the Orthodox Church

In September 2021, a leak of more than 3,000 documents from inside the Georgian State Security Service (SSG) revealed that the state had been running surveillance inside the Georgian Orthodox Church since at least 2014.¹⁰⁹ The Church-related documents were part of a wider release totalling some 60,000 files from the SSG's archives.¹¹⁰ The material was sorted into folders by category - "Adulterers," "non-traditional sexual orientation," "Russian influences," former ruling-party ties.¹¹¹ Some folders held video kompromat.¹¹² This chapter follows three questions about that surveillance. What did it contain? Who disclosed it? How have the dossiers it produced been used?

The Georgian Orthodox Church as the Target of State Surveillance

In March 2026, an estimated 1.5 million people queued at Sameba Cathedral in Tbilisi to pay their respects to Patriarch Ilia II.¹¹³ The figure represents close to 40 per cent of Georgia's population of approximately 3.7 million.¹¹⁴ It is one of the clearest available measures of the institution the SSG had chosen to surveil.

The Church has held first place in Georgian trust polling for more than a decade. The 2014 IRI poll recorded 94 per cent trust - the highest figure for any institution in the country.¹¹⁵ The rate has fallen since but the rank has not changed: in 2018, Transparency International Georgia / CRRC found 76 per cent;¹¹⁶ in 2020, the Carnegie Endowment found that close to 80 per cent of Georgians considered the Church the foundation of their national identity.¹¹⁷

109. 'Leaked "Kompromat" Against the Clergy Rocks Georgia' (OC Media, 14 September 2021), <https://oc-media.org/leaked-kompromat-against-the-clergy-rocks-georgia/> (4 June 2026)

110. 'Gogashvili Describes the Scheme of How So-Called "Dossiers" Are Created in the SSS' (Netgazeti, 15 September 2022), <https://netgazeti.ge/life/630109/> (4 June 2026)

111. 'Leaked "Kompromat" Against the Clergy Rocks Georgia' (OC Media, 14 September 2021)

112. 'Georgia Flooded with Leaked Surveillance Recordings of Clergy' (Eurasianet, 17 September 2021), <https://eurasianet.org/georgia-flooded-with-leaked-surveillance-recordings-of-clergy> (4 June 2026)

113. 'Georgia Honours Its Spiritual Father' (Hungarian Conservative, 26 March 2026), https://www.hungarianconservative.com/articles/culture_society/georgia-spiritual-father-patriarch-ilia-ii-death/ (4 June 2026)

114. 'Georgia's Population 3.704 Million - Geostat' (Civil Georgia, 25 April 2025), <https://civil.ge/archives/677760> (4 June 2026)

115. 'Political Ratings and Public Attitudes in IRI-Commissioned Poll' (Civil Georgia, 25 March 2015), <https://civil.ge/archives/124492> (4 June 2026)

116. 'TI-Commissioned Public Opinion Survey' (Civil Georgia, 11 May 2018), <https://civil.ge/archives/241208> (4 June 2026)

117. 'The Future of Georgia 2020 Survey: Trust in Institutions' (Caucasus Barometer, 2020), <https://www.caucasusbarometer.org/en/dw2020ge/FOUNDIDNTT/> (4 June 2026)

Throughout his nearly five-decade patriarchate, Ilia II himself polled as the most trusted public individual in the country.¹¹⁸

The surveillance reached across the Church's hierarchy. Members of the Holy Synod, bishops, priests, nuns, and Patriarchate staff appear in the dossiers. Telephone communications were transcribed. Notes were kept on the targets' political views and on what was observed of their private and professional lives.

The files were sorted into thematic categories. "Adulterers" listed clergy alleged to be conducting affairs, with names, identification numbers, addresses, and photographs. "Ties with natsebi" tracked associations with former ruling-party affiliates. Other categories included "non-traditional sexual orientation," "crime and drug abuse," and "Russian influences." Some files referred to video material held for use as kompromat. The cache also contained recordings from foreign diplomatic missions - the EU and Israeli embassies and the Council of Europe - with diplomats monitored through their aides.

The disclosure landed in a country with a long history of state surveillance. The previous government, under the United National Movement, had relied on the same methods. When Georgian Dream came to power in 2012, it presented itself as breaking with the practice. In 2013 it publicly destroyed 100 CDs said to contain personal recordings inherited from the previous administration. In 2017 the same government passed legislation granting an SSS-affiliated agency access to communications intercepts subject to court approval.¹¹⁹ The 2021 disclosure should be read against this background of formal regulation and informal extension.

The Disclosure as Insider Action

Who disclosed the files? The evidence points to an insider, not to the state.

The expert interviewed for this study described clerical-state surveillance as an informal feature of the relationship between Church and state. On this account, clergy treated surveillance as a tolerated cost of doing business with the state, so long as the material stayed inside the system. The shock of September 2021 was the public release, not the surveillance itself.

Iremashvili and Shaishmelashvili, two former senior police officials, co-host the podcast *The System from the Inside*.¹²⁰ From inside the apparatus, Iremashvili described the SSG's practice of compiling dossiers on politically active individuals, including those affiliated with the ruling party. According to Iremashvili, the purpose was to provide future leverage:

118. 'Georgia Honours Its Spiritual Father' (Hungarian Conservative, 26 March 2026), https://www.hungarianconservative.com/articles/culture_society/georgia-spiritual-father-patriarch-ilia-ii-death/ (4 June 2026)

119. 'Georgia Flooded with Leaked Surveillance Recordings of Clergy' (Eurasianet, 17 September 2021).

120. 'The Rotten "System from the Inside"' (Mismine, podcast, 9 May 2026), <https://www.youtube.com/watch?v=0NTS6UG1XMk> (4 June 2026)

material to be deployed if the subject moved against the party or required pressure to act in particular ways. Surveillance of the Church had intensified during Ilia II's later years, he said, in preparation for the patriarchal succession.

Iremashvili argued that the scale of the disclosure pointed away from a state source. Tens of thousands of files were released in total. A state interested in discrediting the Church would have selected the most damaging recordings for a targeted release. The mass release shifted the public discussion onto the scale of state surveillance itself.

Two former SSG figures have been publicly named in connection with the disclosed material.

The first is Akaki Nemsadze, an intelligence officer in the SSG's special department. Shaishmelashvili names Nemsadze as the most likely source of the leak - a participant who, in his account, could no longer tolerate what he was being asked to do.¹²¹ The forensic record is consistent with this. Nemsadze's name appears within the disclosed material itself: one dossier - a surveillance report on a conversation between Bishop Rusudan Gotsiridze of the Evangelical-Baptist Church and journalist Tornike Mandaria - is filed under his name.¹²² He was a documented participant in the surveillance operation. A letter attributed to him accompanied the release. In it he described the SSG as a "cancer" and a destructive threat to the state, acknowledged his own years of service within it, and called on the public to rise up and dismantle the system.¹²³ According to Mtavari Arkhi, Nemsadze died by suicide on 8 July 2021, approximately two months before the files were released; Mtavari speculated that he may have arranged for the material to be released posthumously.¹²⁴ The website hosting the files used the pseudonym "Hakim Pasha." The same pseudonym had been used in March 2014, when an anonymous account released video material concerning the late former Prime Minister Zurab Zhvania and the Deputy Governor of Kvemo Kartli, Raul Yusupov. No public determination of the cause of his death has been made. In October 2021, weeks after the files appeared, two former senior Interior Ministry officials and friends of Nemsadze - Akaki Koberidze and Giorgi Butikashvili - were detained. Their lawyers and families said the evidence was planted: a weapon on Koberidze, drugs on Butikashvili. Formula reported the arrests in connection with the leaked files and Nemsadze's presumed role in their release.¹²⁵

The second is Soso (Ioseb) Gogashvili, a founding figure of the SSG and its First Deputy Director from 2014 until approximately 2017, under SSG chief Vakhtang Gomelauri. He became a public critic of the Georgian Dream government from 2020. He was arrested on the night of 15 July 2022 and charged with exceeding official powers, the unlawful

121. 'Leaked "Kompromat" Against the Clergy Rocks Georgia' (OC Media, 14 September 2021)

122. 'Georgia Flooded with Leaked Surveillance Recordings of Clergy' (Eurasianet, 17 September 2021)

123. 'Georgia Flooded with Leaked Surveillance Recordings of Clergy' (Eurasianet, 17 September 2021)

124. 'Leaked "Kompromat" Against the Clergy Rocks Georgia' (OC Media, 14 September 2021)

125. 'The SSS Files and the Arrest of 2 MIA Employees' (Formula News, 29 October 2021), https://formulanews.ge/all_videos/სუსის-ფაილები-და-შსს-ს-2-თანამშრომლის-დაკავება/59131 (4 June 2026)

obtaining, storage, and dissemination of personal data using his position, and the illegal acquisition and possession of firearms and ammunition. He denied the charges and described the prosecution as politically motivated. Pre-trial detention was imposed on 18 July. On 21 July, the Georgian NGOs Transparency International and ISFED released documents which they said Gogashvili had provided to them - documentation of the ruling party offering benefits to citizens in exchange for their votes during the 2021 parliamentary elections, including the return of confiscated driving licences, the removal of probation, the cancellation of fines, and the early release of convicts. In April 2023 Gogashvili was convicted on all charges and sentenced to five years in prison.¹²⁶

Gogashvili's role in the September 2021 Church disclosure is not established. The disclosed files contain a single reference to him - a communication between SSG officers describing him as the person who "took away the videos that we cannot find" - implicating him in the handling of clerical surveillance material, though not conclusively. His documented whistleblowing concerned the conduct of the 2021 elections, not Church surveillance. His arrest nonetheless appears to have closed the matter for the Church. On the expert's account, the institution treated the leak as a glitch that the state had fixed by arresting Gogashvili: with someone in custody, the episode could be regarded as resolved.

The Use of Surveillance Material in Church Politics: The Mamaladze Case

On 10 February 2017, Archpriest Giorgi Mamaladze was detained at Tbilisi International Airport. He was head of the Patriarchate's treasury and a close associate of Patriarch Ilia II. Prosecutors claimed cyanide was found in his luggage and that he had planned to poison a senior cleric. Hidden-camera footage released by prosecutors shows him asking about obtaining the substance. The trial was classified top secret and held behind closed doors. On 5 September 2017, he was sentenced to nine years. He was released in 2024.¹²⁷

Mamaladze denied the prosecution's account. He stated the cyanide had been procured at the request of the official later named as the intended victim,¹²⁸ and that his arrest served to remove him from a position where he had begun to examine internal corruption at the Patriarchate.¹²⁹ The Public Defender and the Human Rights Centre criticised the closed proceedings and the denial of defence access to airport surveillance footage relevant to the arrest.¹³⁰

Former senior security officials, speaking on the podcast *The System from the Inside*, have

126. 'Former Georgian Security Chief Sentenced to Five Years' (OC Media, 4 April 2023), <https://oc-media.org/former-georgian-security-chief-sentenced-to-five-years/> (4 June 2026)

127. 'Details from the Archive on the Cyanide Case that Led to Giorgi Mamaladze's Arrest' (On.ge, 15 February 2024), <https://go.on.ge/9gw> (4 June 2026)

128. 'Georgia: Verdict Arrives in Church Poisoning Plot' (Eurasianet, 5 September 2017), <https://eurasianet.org/georgia-verdict-arrives-in-church-poisoning-plot> (4 June 2026)

129. 'Patriarch Murder Plot a "Coverup of Church Corruption"' (OC Media, 16 February 2017), <https://oc-media.org/patriarch-murder-plot-a-coverup-of-church-corruption/> (4 June 2026)

130. 'Georgian Archpriest Found Guilty in "Church Poison Plot"' (OC Media, 5 September 2017), <https://oc-media.org/georgian-archpriest-found-guilty-in-church-poison-plot/> (4 June 2026)

raised anomalies in how the case was assembled and presented. On their analysis, its principal effect was factional: the hidden-camera footage, selectively disclosed, weakened the position of Dimitri Shiolashvili, Ilia II's nephew and widely regarded favoured successor, within the Church hierarchy. He withdrew from active involvement in Church affairs.¹³¹

In May 2026, Shio Mujiri was elected Patriarch.¹³² In the period before the May 2026 election, Archbishop Zenon Iarajuli - a voting member of the Holy Synod - publicly stated that Shio's candidacy was favoured both by the Georgian government and by representatives of the Moscow Patriarchate. He also claimed that government representatives had "summoned bishops one by one" in an effort to secure support for him.¹³³ If accurate, this describes a second register of influence: not the slow removal of a rival faction's figure through the courts, as in the Mamaladze case, but direct pressure applied to individual electors at the moment of decision.

The available evidence does not resolve what actually happened in the Mamaladze case. What it shows is that hidden-camera footage of a senior cleric, assembled and selectively disclosed by state prosecutors, shaped the internal balance of the country's most trusted institution over nearly a decade.

State surveillance in Georgia reaches institutions whose public trust would, in principle, place them beyond routine state pressure. The 2021 disclosure made public an operation that had been running for at least seven years on the senior leadership of the country's most trusted institution. The disclosure changed little. Shio Mujiri was elected Patriarch in 2026, the candidate identified by Zenon as the one supported by the government. The SSG continues to operate. The figure most clearly identifiable as the source of the disclosure - Akaki Nemsadze - died under disputed circumstances two months before the files were released. The 2017 Mamaladze case shows what use of surveillance material looks like in practice, even where the direct documentary connection between dossier system and prosecution cannot be established. The 2026 succession shows that the effects of such use persist over long time horizons. The system is not occasional - it is operational.

5.3 Personal Data for Social Control: Mental Health Records

Mental health records constitute a distinct layer within Georgia's emerging data architecture. Unlike surveillance footage or voter lists, a psychiatric diagnosis carries social consequences independent of any state action: stigma, employment risk, disrupted family

131. 'The Rotten "System from the Inside"' (Mismine, podcast, 9 May 2026), <https://www.youtube.com/watch?v=0NTS6UG1XMk> (4 June 2026)

132. 'Metropolitan Shio (Mujiri) Becomes New Patriarch of Georgian Orthodox Church' (Civil Georgia, 11 May 2026), <https://civil.ge/archives/733754> (4 June 2026)

133. 'Senior Georgian Bishop Calls Leading Patriarchal Candidate Mujiri "Dangerous" and Preferred by Russia' (OC Media, 8 May 2026), <https://oc-media.org/senior-georgian-bishop-calls-leading-patriarchal-candidate-mujiri-dangerous-and-preferred-by-russia/> (4 June 2026)

relationships. When the state builds a registry around that data, the effect on behaviour begins before the registry is ever used. This section traces an amendment to Georgia's Mental Health Law initiated not by the health ministry but by the Ministry of Internal Affairs, its alignment with parallel Russian legislation, and the chilling effect already produced on people seeking care.

How the amendment was passed

In June 2024, the Ministry of Internal Affairs initiated amendments to Georgia's Law on Psychiatric Assistance. The stated justification was public safety. The practical effect was to mandate that the Ministry of Health create a unified state registry of individuals with mental health diagnoses. The originating institution matters. As Elene Koridze, a psychologist and mental health specialist, observes:

"The MIA has no connection whatsoever and has nothing to do with the mental health law – it doesn't understand the context, doesn't understand the subject – and still addresses parliament with an initiative, obliges the Ministry of Health to create such a registry. And completely quietly."

The framing – safety of citizens – carries an implicit premise that people with mental health conditions represent a threat. Koridze is direct about what that premise does:

"The idea that people with mental health problems are dangerous is wrong from the start. There is absolutely no connection between having mental health problems and committing crimes. This is the fuelling of stigma and an additional barrier for people who genuinely need to see a specialist."

The legislative process was designed to minimise scrutiny. The first reading took place in March 2025. There followed a gap of several months with no public consultation. The third and final reading passed on 9 December 2025. No psychiatrist, clinician, or person with direct professional experience was consulted at any point in the process. Koridze is unequivocal on this exclusion:

"Not one psychiatrist, mental health specialist, or person with experience was involved in this process. This is a huge violation. It contradicts modern guidelines and human rights."

What the registry creates – and what it signals

The amendment establishes a centralised state registry of individuals who have received psychiatric diagnoses or sought mental health treatment. The terminology used throughout is also telling. Terms such as "alcoholism" and "toxicomania" appear in the text – terms retired from clinical use decades ago. Koridze identifies their origin precisely:

"These terms are absolutely copied from Russian manuals and laws. The same law was being initiated in Russia in parallel. The title itself, even in Georgian, is an absolute analogy of the Russian one."

The Public Defender's Office, in a formal assessment addressed to the Prime Minister on 22 April 2026, concluded that no equivalent centralised registry – one that automatically registers persons on the basis of mental-health or addiction data and imposes a separate legal regime on them – exists in any Council of Europe or European Union member state.¹³⁴ The one near-parallel, Koridze notes, is Russia, where comparable legislation granting the Interior Ministry access to the medical records of people with mental illness and addiction was approved by the government in April 2024, signed by President Putin in July of that year, and came into force on 1 March 2025.

Zura Sikharulidze, an addiction medicine specialist and clinical director **writing** publicly in the days after the law's passage, frames the registry in terms its defenders cannot: "The registry does not protect society – it protects the system from people."

Georgia has ratified the United Nations Convention on the Rights of Persons with Disabilities. The convention prohibits discrimination on the basis of disability, requires that persons with disabilities enjoy legal capacity on an equal basis with others, and mandates the elimination of stigmatising practices in law and policy. Koridze assessed the amendment's compatibility with that framework in stark terms:

"Georgia is a signatory and has ratified the UN Convention on the rights of persons with disabilities, and this amendment absolutely contradicts it. This law is so incompatible with the convention that if someone were to file a lawsuit, the Georgian government could appear before an international court."

A chilling effect before implementation

The registry's most consequential effect has arrived before it has been operationalised. As with facial recognition surveillance and protest participation, the mechanism does not require deployment to change behaviour – awareness of its existence is sufficient. Koridze relays the response she is already encountering:

"Already, more than one person is asking the question: should I go to a psychiatrist? Won't I end up in this database by chance?"

This dynamic – deterrence before enforcement – is structurally identical to the self-censorship documented among protest participants in chapter three. In that context, people modified their routes, reduced communication on visible platforms, and withdrew from public space not because they had been penalised, but because they believed they might be. Here, people avoid clinical contact not because they have been entered into a registry, but because they believe they might be. Koridze connects the two explicitly:

"Censorship is preceded by self-censorship."

134. Public Defender (Ombudsman) of Georgia, 'Assessment of the Law on Amendments to the Law of Georgia on Weapons and Accompanying Legislative Changes' (22 April 2026), <https://ombudsman.ge/res/docs/2026042212574862349.pdf> (4 June 2026)

The law creates conditions under which people will manage and conceal symptoms rather than seek professional help – a public health cost with no offsetting benefit. Koridze also identifies a structural consequence for the profession itself:

“This risks creating underground psychiatry.”

When individuals with genuine clinical needs avoid the registered system, care does not disappear. It moves outside the oversight frameworks that protect patients from harm.

Psychiatric detention and the political context

The mental health registry does not stand alone. A separate amendment passed in the same legislative period modifies criminal procedure for individuals with mental health conditions. Under the new provisions, a person accused of a criminal offence who is found to have a mental health condition loses the right to appear before a court until a psychiatric institution has assessed and certified their fitness to stand trial. Koridze describes the mechanism:

“If a person commits a crime and a mental health problem is found in them, neither they nor their lawyer will have the right to present themselves in court. They will first be placed in a psychiatric institution, treated, and only if the institution decides they are well will they then appear before the court.”

The implications for Georgia’s current political context are not, in Koridze’s assessment, incidental:

“This is how Georgia’s political situation is developing – that instead of a court, they will send you to a psychiatric institution.”

Maia Tsiramua, a psychologist and clinical supervisor interviewed separately by Batumelebi, places the law within a longer Georgian history of state psychiatric abuse.¹³⁵ Recalling how the Soviet regime turned psychiatric treatment against the dissident Nazi Shanauri, she warns: “that’s where everything is heading.”

The psychiatrist Nino Okribelashvili draws the same conclusion from comparative experience: history, she writes, has repeatedly shown that “such registries easily become tools of political, subjective, or bureaucratic persecution.”

Coinciding with these legal changes, a new university psychiatric clinic opened in Tbilisi with one hundred dedicated psychiatric beds. Koridze does not treat this as coincidental:

“It is not a coincidence, in my opinion, that a new university psychiatric clinic opened with 100 psychiatric beds. All of this together creates a picture in which these instruments will be used very selectively, with political motives, with great probability – and then spread to the whole population.”

135. ‘What is the Mental Health Registry that “Georgian Dream” is Creating – Interview with a Psychologist’ (Batumelebi, 18 December 2025), <https://batumelebi.netgazeti.ge/news/599431/> (4 June 2026)

This sequence – legal framework, institutional capacity, selective initial use, eventual wider application – follows the pattern described throughout this report. The infrastructure is assembled before it is deployed at scale. Its chilling effect precedes its operational use. On that point, Koridze is precise:

“Mental health has always been and will always be an effective instrument for manipulation, control, and the sowing of fear. The effect of this law is real now, before it has come into force.”

The psychologist Elene Japaridze [names](#) without circumlocution what the other voices describe: “The mental health registry is a modern form of social control.”

What these accounts share is a single diagnosis. A registry initiated by a security ministry, designed without clinical input, mirroring legislation [parallel to Russia’s](#), and incompatible with European data-protection and human-rights frameworks is, in the view of the professionals quoted here and in the wider public response that has met the law’s passage, more likely to function as a mechanism of social control than as a public-health measure. Whether or not it comes to be used in that way, its early effects on people seeking care are already visible, in the avoidance, mistrust, and self-censorship that the prospect of inclusion has begun to produce.

6. Conclusion

This report has documented how personal data is used as an instrument of political control in Georgia across four domains: protest, elections, the Orthodox Church, and mental health. In each case, the relevant infrastructure was assembled by separate state institutions over time and predates the uses examined here. The Ministry of Internal Affairs and the Public Service Development Agency hold the visual records and biometric data that make remote identification possible. The unified voter registry, the Social Service Agency's records, and data drawn from multiple ministries make household-level political profiling possible. The State Security Service's dossiers, disclosed in 2021, document surveillance of the Church running since at least 2014. The 2024 amendment to the Mental Health Law mandates a centralised psychiatric registry. No single dataset constitutes the threat; the recurring finding across these chapters is that the data becomes consequential when it can be matched to a specific individual and combined across sources.

A second finding is consistent across the domains examined: the effect on behaviour does not require full deployment of the infrastructure. The interviews show the scale of the chilling effect of remote face recognition systems on demonstrators and its impact on freedom of expression. The same dynamic appears in the mental health context, where practitioners report that people are already avoiding psychiatric care out of fear of being entered into a registry that is not yet operational. In both cases, awareness of the system's existence, rather than its confirmed use, is what changes how people act.

Finally, the report documents specific external dependencies and legislative parallels. Georgia's facial recognition software was procured from Papillon, a Moscow-based company whose products are used by Russian law enforcement; the cameras feeding the system are manufactured primarily by Hikvision and Dahua, Chinese firms sanctioned by the United States. The mental health registry uses terminology drawn from Russian manuals and was initiated in parallel with comparable Russian legislation that came into force in March 2025. The Public Defender's Office found no equivalent centralised psychiatric registry in any Council of Europe or European Union member state. These are the documented conditions under which this infrastructure now operates, and they are the basis for the concerns this report has set out.

