The Regime's Digital Eyes: Real-Time Monitoring of Protest Participants

Tamar Ketsbaia[1]

The first part of the article's title is not an original idea of the author, just as the methods of implementing total control currently unfolding in Georgia are not practices "invented" by Georgian Dream.

A similar title was used in a piece published on 27 March 2025 about developments in Belarus - "Lukashenko's Digital Eyes",[2] which vividly illustrated the system that has been built there over the years. This "monster" was once created under the pretext of ensuring citizens' safety, but today is used for complete and boundless control over them.

In Belarus, tens of thousands of cameras are connected to a special system, which in turn is integrated with the Ministry of Internal Affairs' databases. This allows for the real-time and highly accurate identification of target individuals. Such a system makes it easier to monitor people engaged in activism not only in Belarus but also in Russia. These individuals are included in "blacklists," and when they appear in public spaces, they can be easily recognized by smart cameras (which are everywhere).

Since the launch of Russia's full-scale war in Ukraine, a widespread practice in Russia has been the use of facial recognition systems for the preventive detention of potential demonstrators on "high-risk days" (dates of national importance or other occasions when protests are expected).

Specifically, while using the metro (where payment methods involve facial recognition), passengers are photographed by special cameras. The algorithm checks the person against databases and cross-references "blacklists." If there is a match, the system triggers an alert and the procedure of preventive detention begins. Within seconds, police arrive, detain the person, subject them to maximum pressure, apply psychological intimidation, threaten, and force them to sign written pledges not to participate in demonstrations.[3]

[1] Research Institute Gnomon Wise. Email: t.ketsaia@ug.edu.ge
[2] "Lukashenka's digital eyes." Belsat, 27.03.2025 https://en.belsat.eu/85836830/lukashenkas-digital-eyes
[3] "Facial recognition is helping Putin curb dissent with the aid of U.S. tech," Reuters, 28.03.2023 https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions

On 4 July 2023, the European Court of Human Rights also addressed the use of facial recognition technologies against protesters in Russia (Glukhin v. Russia). The Court found such practices to constitute not only a violation of the right to respect for private life but also to have a chilling effect on the freedom of assembly and demonstration.[4]

In this case, the applicant, Glukhin, argued that within the framework of administrative proceedings, Russian law enforcement agencies unlawfully processed his special category personal data - both biometric information and data concerning political opinions. This, he argued, violated his right to privacy. In particular, based on photo and video material of his solo demonstration published on Telegram, he was identified through facial recognition, and his place of residence was determined. Later, using the same technology, he was located in real time for the purpose of detention, which ultimately ended with his administrative arrest.

The European Court emphasized that the use of facial recognition systems against peaceful demonstrators (unless intended to investigate serious crimes or prevent the immediate commission of a crime) is unacceptable and incompatible with the ideals and values of a rule-of-law-based democratic society. In this specific case, the Court considered the use of facial recognition disproportionate, as there was no risk to public safety and the measure targeted a peaceful protest. Therefore, the Court did not see any urgent need for such restrictive technologies and held that their use was not necessary in a democratic society.

Amidst the Russian and Belarusian experiences, it is important to analyze Georgian practices of processing protesters' special category personal data and to examine the attitudes of the Ministry of Internal Affairs and the courts toward such measures.

This article therefore aims to highlight these issues, drawing on trends observed in courtroom proceedings related to administrative cases concerning the artificial blocking of transport routes.

Delegating public order protection to “digital eyes”

According to a method approved by the Ministry of Internal Affairs, if a traditionally recurring protest in front of Parliament does not escalate into a particularly tense situation, the patrol inspectors mobilized

[4] Tamar Ketsbaia - Georgian Analogue of the Russian Practice of Demonstrators’ “Post-factum Detention”, Research Institute Gnomon Wise, 30.01.2025 https://gnomonwise.org/ge/publications/analytics/242

on the perimeter manage the participants' movement onto the roadway. They do not obstruct them, do not issue any warnings, and after the road is blocked, they leave the area. Usually, only a few patrol crews remain on the perimeter, blocking the road from Metro “Liberty Square” to “Tbilisi Marriott” and restricting traffic during the protest. The same approach is applied in other locations where the road is blocked.

Later, when protesters are summoned to court on charges of road blockage, the Ministry of Internal Affairs’ representatives do not comment on the passivity of the patrol officers on site (whose primary function is to ensure public order) and, moreover, often ignore the fact that the police themselves encouraged the blockage. They only emphasize that individuals are personally obligated to obey the law.

In parallel with the inaction of patrol officers on site, the so-called “digital eyes” work with special intensity, their number periodically increasing.[5] Smart cameras see and remember everyone. The cameras’ quality is notable, providing high resolution, which makes it easier to identify individuals, fine them, and post-factum “care” for public order.

Real-time surveillance of protesters - suspicion or a proven fact?

In hundreds of court cases, the main evidence used to establish the fact of road blockage and recognize individuals as administrative offenders has been footage from 112’s surveillance cameras. All other evidence is also based on video.

Initially, the recordings submitted by the Ministry of Internal Affairs in specific cases were only a few seconds long. For them, duration was irrelevant, and even for judges, the fact of a person standing in a specific place for just a few seconds was deemed sufficient to assign administrative liability.

But this was not the only reason why the courts were not provided with complete, uninterrupted footage. The secret lies in the fact that full recordings clearly reveal the illegal practice of monitoring protest participants in real time and exercising full control through 112’s surveillance cameras. The footage is not

[5] Nastasia Arabuli - When it comes to issuing a fine, they can see everything; but when it comes to proving a policeman’s crime, they can’t. See, where new “smart cameras” have been added, Radio Liberty, 21.03.2025 https://www.radiotavisupleba.ge/a/33355334.html

shot from a distance as a general view of the protest but rather shows that the camera approaches individual participants in real time and captures close-ups.

As revealed in recordings released by the Young Lawyers' Association, in some cases, extremely detailed information is collected about demonstration participants. For example, the camera operator focuses on documents held by a protester, which can be read due to the cameras' high resolution.

At first, courts were mostly presented only with cropped footage zoomed in on the individual. This created the impression that the zooming occurred later, during evidence review, and not in real time. However, courts could not be shown "unprocessed" (un-zoomed) footage, which gives a suspicion that such footage does not even exist.

Interestingly, this limitation only affected the Ministry of Internal Affairs and the courts in the initial stage. Once the secret was exposed, both institutions easily adapted to the new reality - treating real-time surveillance of individuals as normal and ignoring any criticism or complaints in this regard. They show no concern for the legality of the evidence, and any attempt to raise the issue is routinely dismissed as "outside the scope" of the case being examined. Notably, during proceedings no one attempts to deny that surveillance occurs in real time and that the cameras are mechanically operated.

"It looks like it [112 itself zooms in on specific individuals]," one of the representatives of the Ministry of Internal Affairs calmly tells the court, while another openly praises the quality and resolution of the footage, unashamed before those about to be declared offenders.

Neither representatives nor judges are disturbed by reminders that this practice of total surveillance mirrors Russian methods and will likely face the same fate at the European Court of Human Rights as in the Glukhin's case in 2023 - where a violation of the right to respect for private life was established. Notably, in that case, the plaintiff could not present direct proof that facial recognition technology had indeed been used against him in real time. Nevertheless, the Court did not impose the burden of proof on the plaintiff. Considering the Russian government's silence, the unreasonably short timeframe for identification, and the widespread practice in Russia, the Court accepted it as established that facial recognition technology had been used, constituting interference with the right to privacy.

Ambiguities in the Procedure of Identifying Individuals - Suspicion of Real-Time Surveillance

The scant evidence presented in court proceedings, the testimonies of those who prepared them, and the explanations of the Ministry of Internal Affairs representatives are so contradictory that, under conditions of a fair trial, it would be unthinkable to recognize someone as an offender on such a basis. Rather, these inconsistencies should themselves become the subject of a separate investigation into systemic violations, followed by appropriate legal responses.

To a simple question of who initiates the request for recordings from 112 and on what grounds, one can hear several conflicting answers. This becomes especially evident in cases where an individual is accused of blocking a roadway not at the standard location near the Parliament but elsewhere, where holding a protest is less expected. For example, in one case connected to the so-called “strike” on January 15, the more officials you asked about the video, the more confusing the answers became.

A Ministry of Internal Affairs representative, who strongly opposed summoning the patrol inspector who drew up the report as a witness, confidently claimed that the inspector himself requested the video after, on his day off (January 15), he had been watching TV (without clarifying which TV channel) and happened to see the offense. Later, in the same case, when the same patrol inspector was summoned as a witness in another proceeding about road blockage, he expressed surprise at hearing such a claim about himself. According to his testimony, January 15 was a normal working day for him, and he denied having watched TV at all.

Another representative of the Ministry in the same case, stated that the information about the alleged offense came from a police officer on site (while the other ministry representative had denied the presence of any police at the scene), and that this was why the video was requested from 112.

Meanwhile, the police inspector who drew up the report claimed that 112 had sent the recording to the duty station, which she then processed - identifying the offenders, marking them accordingly, and passing it along to the person responsible for the identification procedure.

Yet, when those same police officer was questioned by the court, she asserted that she had received the full video directly from 112, not from the inspector. According to her, the video contained no markers indicating specific offenders. Still, she was unable to explain the criteria by which she decided whom to identify.

Moreover, this official could not clarify the identification procedure itself. When asked what percentage match there was between the image entered into the system and the suggested identity from the Ministry's database, she replied that in this case it was an "absolute" match. When pressed further on whether the program explicitly displayed a 100% match (and in general whether it displayed percentages), the official, who signs off on multiple identification reports, gave a dubious response: "Well, we just assume that's the case".[6]

These and other seemingly minor facts emerging during proceedings together raise a reasonable suspicion that in reality we are dealing with a systemic problem. It is highly likely that the reports later drafted, often containing multiple errors, are in fact attempts to cover up real-time identification of protesters. It is clearly the Ministry of Internal Affairs' responsibility to dispel this suspicion, yet during proceedings it shows no sense of that duty, nor does the court impose such an obligation.

Notably, despite the sensitivity of processing protesters' personal data and the high public interest, the Personal Data Protection Service has yet to respond to the Young Lawyers' Association's appeal on this issue.[7]

How Does This System Relate to Developments in Belarus and Russia?

Processing demonstration participants' personal data under the pretext of "artificially blocking a road" is only the beginning in the hands of an authoritarian regime, as happened in Russia and Belarus.

In those countries, too, the authorities initially processed special categories of personal data of protesters under the pretext of violations of protest rules. These data were used selectively, primarily to punish certain participants as an example, intended to deter others from exercising their freedom of assembly and expression.

However, the main function of the "digital eyes" is to compile the most accurate possible list (a blacklist) of individuals critical of the regime. These individuals are then subjected to constant monitoring and

[6] It is interesting how this program actually works. An illustrative example is a video uploaded on Facebook by a citizen, which shows the identification procedure carried out on him by a patrol inspector for the purpose of testing the program. https://www.facebook.com/watch/?ref=saved&v=268204389255681

[7] Georgian Young Lawyers' Association - The Ministry of Internal Affairs is using facial recognition technologies for total control against peaceful demonstrators, 12.03.2025 https://gyla.ge/post/saxis-amomcnobi-kamerebi-saia

harassment, usually ending, in the traditional scenario, with imprisonment or forced emigration, closing the chapter of resistance.

A person added to the blacklist becomes a constant target of police attention through facial recognition systems. Authorities can then employ various instruments of pressure. Among them is the mechanism of preventive detention, which allows regimes to preemptively remove particularly active individuals from potential protest hotspots or to keep them in a state of constant discomfort. Such practices, responding to so-called “dangerous days”, can already be observed in Georgia. Summonses to court always increase in the run-up to large, planned demonstrations, as do instances of fine notices delivered to homes or calls from the police. Recently, there have also been noticeable cases of people being stopped at protests or metro exits, searched, and, if they resist, detained.

Unfortunately, in Georgia, relevant institutions initially turned a blind eye to the alarming practice of total control of people through “digital eyes”. They still have the power to eliminate its irreversible consequences but have yet to do so.

These officials spend no time or effort considering that they themselves have opened a Pandora box, unleashing effects they will no longer be able to control. Among those consequences is the fact that, in the future, they will not be able to shield themselves or their loved ones from the “sharp gaze of a Big Brother”.