EUROPEAN LAW BLOG
NEWS AND COMMENTS ON EU LAW

ELB Blogpost 39/2023, 19 September 2023
Tags: Facial recognition, *Glukhin v Russia*
Topics: Data protection and digital governance

Glukhin and the EU regulation of facial recognition: Lessons to be learned?

By Isadora Neroni Rezende

On July 4th 2023, the European Court of Human Rights (ECtHR) handed in its first judgement on the use of facial recognition (FR) in law enforcement. The Court ruled that Russia breached Articles 8 and 10 of the Convention by using the technology to find and arrest a peaceful demonstrator. The decision reignites the European debate on FR. For the European Parliament and several NGOs, the use of FR in public is incompatible with EU values and should be banned (Reclaim your Face, 2023; AlgorithmWatch, 2023; European Parliament, 2023). However, the reasoning of the ECtHR does not necessarily follow this assumption. The Court does not embrace a proactive stance in the case, leaving many questions open on the legitimate use (if any) of the technology. This "laid-back" approach may be justified by the exclusion of Russia from the Council of Europe. The ECtHR is aware that the decision will not be executed and might have decided to avoid any confrontation on the matter with other Contracting Parties. Still, this might also have been a chance for the Court to take some liberty and provide general guidance.

Nonetheless, *Glukhin* is an interesting read to understand current issues in the regulation of FR, and what might be missing in the upcoming EU legislation. This analysis highlights its implications for the legislative process of the Artificial Intelligence Act (AIA).

Introduction

Undoubtedly, the case *Glukhin v. Russia* intervenes in a moment of heated political debate around FR. Thus, one cannot avoid seeing its implications for future EU legislation on the topic. Coming from a human rights court, the judgement could have set clear legal limits

to the technology in public. This was not the case. Rather, the judgment shows that decisions around FR will remain essentially *political*.

This stresses how topical the positions of EU institutions are in the current legislative process. Foremost, the Court's self-restrained approach may worry the European Parliament, which holds the 'ban solution' as the only compatible with European liberal democracies. This position may not hold up in the trilogues, possibly forcing the Parliament to revise its views. The negotiating mandate was voted by a left-to-centre coalition (Volpicelli 2023), but political winds may shift after next year's elections (Camut 2023). Conversely, the decision implicitly favours the Commission and the Council's approach, which wish to regulate the technology rather than banning it. The framework proposed is, however, still lacking from a human rights perspective. *Gluckin* could have set specific standards for laws applying to FR, providing guidance for upcoming EU negotiations. As we will see, nonetheless, the Court's reasoning remained under-theorised, leaving *carte blanche* to EU institutions to pursue their agenda.

But before delving into these questions, more background is needed. The case originated from the arrest of Mr Nikolay Sergeyevich Glukhin. The applicant had held a peaceful solo demonstration while holding a life-size cardboard of the Russian dissident Kostantin Kotov in the Moscow metro. The police found photos and a video of the event on social media and arrested him a few days later. Mr Glukhin was convicted of an administrative offence for failing to notify competent authorities of his demonstration. The social media screenshots and video-recordings were used as evidence against him. According to the applicant, the police had used FR technology both to identify and later locate him in the Moscow metro. He complained before the ECtHR that his arrest and the use of FR violated Articles 8 and 10 of the Convention.

While the applicant could not prove that the police had used the technology, the Court was convinced that this was plausible (paras 70-72). The processing of his biometric data thus raised an interference in his right to private life. FR had been used both *ex post,* to identify the applicant, and *live*, to locate and arrest him in the metro. Even if the interference had a legal basis, this did not meet "quality of the law" requirements (para 82). It is a long-standing position of the Court that legal bases grounding an interference on human rights should be foreseeable and accessible. This means that individuals should be able to access it easily and predict the consequences of its violation. Specifically, the law in question was widely formulated. It admitted the use of FR "in connection with the administration of justice", that is in *any* kind of proceedings. It did not indicate the people likely to be monitored, nor the situations and purposes which could legitimate the use of the technology. No prior authorisation was foreseen, and there were no procedures for examining, using and storing the data obtained, nor providing supervisory control mechanisms and remedies (para 83). In the case at stake, FR had been employed for the

legitimate aim of preventing crime (para 84). However, its use in the proceedings had been disproportionate. Mr Glukhin had conducted a peaceful protest, which did not pose any danger to the public or transport safety (para 88). His prosecution had only led to a conviction for a minor offence. Ultimately, there had been no pressing social need to have recourse to the technology, and its use was considered unnecessary in a democratic society (para 90). Consequently, the Court found a violation of Articles 8 and 10 of the Convention.

A self-restraining approach to surveillance

The decision was depicted as a victory for privacy activists (Article19, 2023). And yet, there are reasons to be cautious about this optimism. Actually, the decision is coherent with the self-restrained approach of the ECtHR in surveillance matters. Indeed, the tendency is not new. A Grand Chamber decision like *Big Brother Watch* was equally welcomed with enthusiasm by some (Privacy International, 2021; Big Brother Watch, 2021). For others, it opened up the way to the normalisation of mass surveillance (Milanovic 2021; Sajfert 2021; Ni Loideain 2021).

The same happened with *Glukhin v. Russia.* As for bulk interception of communications, the Court did not find an abstract incompatibility between FR and the European human rights system, for example, on proportionality grounds. Maybe aware of the political implications of this decision, it downsized the scope of its analysis. The Court bypassed indeed the question of the acceptability of certain FR uses under the Convention. The only issue to be considered was "whether the processing of the applicant's personal data was justified under Article 8 § 2 of the Convention in the present case" (para 85). Certainly, this is coherent with the institutional nature of the Court, which only rules on concrete cases (with the exception of Article 1 Prot. 16 ECHR). However, a more proactive approach is not unknown in the ECtHR's jurisprudence, even in surveillance matters.

Even if we focus only on the requirements for legitimate FR uses, some gaps can be found in *Gluckin*. For instance, the case involved both *ex post* and *live* FR. The two practices entail indeed very different interferences with the right to private life. While *ex post* FR can be assimilated to classic investigatory measures targeting individuals, *live* FR is directed at anyone in the cameras' range. However, the Court does not distinguish how personal limitations should apply in these cases. We shall come back to this issue below, but, overall, the ECtHR's approach comes across as superficial. Seemingly, it made little effort to discern different uses of the technology and frame them in its jurisprudence. Certainly, it found a violation of the right to private life. Still, it may have availed the deployment of FR in Europe, without restraining its "fair" applications clearly.

Facial Recognition in the EU: Where are we at?

As said, FR is one of hottest topics in the legislative process leading to the adoption of the AIA. Indeed, the approaches of the European Commission, the Council and the Parliament diverge significantly.

The European Commission's proposal classifies remote biometric systems (both 'live' and 'post') as high-risk. It bans the use of live FR in public places for law enforcement purposes, unless certain (broad) conditions apply (Article 5(1)(d)). Such systems can be used, when strictly necessary, to:

- search for crime victims;
- prevent threats to life and physical safety, or terrorist attacks;
- detect, identify, and locate suspects of serious offences (those legitimising the issuing of a European arrest warrant).

Proportionality requirements are foreseen (Article 5(2)), especially in relation to:

- the nature of the situation where to deploy the technology;
- the consequences of deploying it;
- the temporal, geographical, and personal limitations of the deployment.

Only judicial or administrative independent authorities can authorise the use of such systems, based on reasoned requests (Article 5(3)). Member States can adopt national rules on the request, issuance, exercise, and supervision of the authorisations. (Article 5(4)) No conditions are set instead for using 'post' remote biometric systems, besides those foreseen for high-risk systems (Title III).

The Council fine-attunes the Commission's approach, but without overturning it. It clarifies that *ex post* FR remains subject to data protection requirements (specifically, Article 10 LED) (Recital 24). It also extends the derogations of the ban on live FR in public places. Protecting critical infrastructure and countering offences punishable with at least five years of imprisonment are added as grounds for authorisation (Article 5(1)(d)(ii) and (iii)). However, this version prevents from using the technology to *detect* suspects, possibly limiting its preventive uses.

The Parliament aims instead to ban live FR altogether. Its position also introduces a ban on "AI systems that create or expand FR databases through the untargeted scraping of facial images from the internet or CCTV footage" (Article 5(1)(db), as well as on emotion recognition systems in law enforcement (Article 5(1)(dc)). The Parliament shows more attention on 'post' remote biometric identification too, introducing a ban on such systems, unless specific conditions apply. Their use is subject to a pre-judicial authorisation. It

should also be strictly necessary for the targeted search connected to serious criminal offenses as defined in Article 83(1) TFEU, which already took place (Article 5(1)(dd)).

These positions should be harmonised in the upcoming trilogue negotiations, but opinions on a partial or total ban on police use of FR in public seem hardly reconcilable. Even if the 'ban solution' does not prevail eventually, limiting the conditions for legitimate use of the technology will certainly be a dividing topic for EU legislators.

Lessons to be learnt from *Glukhin*?

How does *Glukhin* impact the positions of EU institutions on FR? In many aspects, the decision is more impactful for what it does not say, rather than for what it actually says.

Seemingly, indeed, the ruling implicitly suggests that a complete ban on live FR cannot be deduced from the principles of the European human rights system alone. Or, at least, the Court will not engage with such a question now. Importantly, the ECtHR's jurisprudence impacts the EU system. Article 6(3) of the Treaty of the European Union (TEU) establishes that fundamental rights guaranteed by the ECHR constitute general principles of EU law, thus having the *status* of primary law. Likewise, Article 52(3) of the Charter of Fundamental Rights of the EU (CFREU) provides that Charter rights corresponding to those of the ECHR must be interpreted as having the same meaning and scope as the rights enshrined in the Convention. Based on this, in *McB,* the CJEU stated that Article 7 CFREU has the same meaning and scope of Article 8 ECHR "as interpreted by the case law of the European Court of Human Rights" (*McB*, para 53; cf. *Volker and Schecke*, paras 51-52). Nonetheless, this does not hamper the EU from granting a higher level of protection (Article 52(3) CFREU). According to the Explanations to the Charter indeed, limitations upon fundamental rights established in the ECHR should not affect the "autonomy of Union law and of that of the Court of Justice of the European Union" (CJEU). This means that, although *Glukhin* may provide significant guidance to EU actors on FR, both the legislator and the CJEU would retain their autonomy to lay down higher standards of protection (e.g., by providing a ban).

This scenario is not to be taken for granted, given the current positions of the EU institutions and the CJEU. For instance, the Court seems now to embrace a more self-restrained approach to mass surveillance, as shown in *La Quadrature du Net*. Therefore, a decision on a total ban can be made at the political level only—which anticipates a good battle for the European Parliament. The Parliament also takes position on *ex post* FR, something that is neglected in *Glukhin.* Nonetheless, the rules proposed appear too generic to ensure a proportionate use of the technology. In the ruling, the ECtHR recalls its jurisprudence on surveillance matters, which requires the legal basis to specify the "categories of people who may be targeted" (*Huvig*, para 34). Yet, the current text does

clarify when the police can identify someone in a footage or which databases they can use. Therefore, the text should be amended to meet quality of the law requirements.

A lack of attention for the legitimate uses of *ex post* FR emerges also in Commission's and the Council's versions. The Council's version relegates the matter to data protection (i.e., Article 10 LED), but its requirements may be interpreted differently in Member States. Moreover, the Commission and Council's approach will pose additional problems, being open to live facial recognition. The Court avails the idea underpinning the Commission's and Council's positions, according to which FR can be used to prevent and prosecute crimes. However, the current legislative framework might not satisfy "quality of the law" standards (EDPB-EDPS 2021, p. 11) set in the ECtHR's case law. One example is the absence of clear "personal limitations" in the regime for real-time remote biometric identification (Article 5(2) of the Commission and Council texts). Both versions are ambiguous about *what* should be subjectively circumscribed. As far as live uses are concerned, it is unfeasible to limit the number of people caught by the camera in public. Thus, reasonably, this safeguard should only apply to the number of people inserted into the watchlists. However, the texts are silent on the conditions under which a person becomes liable to be identified in public by FR cameras.

This gap has worrisome implications. The Council and Commission's texts do not include any ban on social media scraping or emotion recognition (which instead are promoted by the Parliament). Apps such as Clearview AI have shown the dangers of enlarging FR databases (Neroni Rezende, 2020). Likewise, biometric classification systems can detect anyone displaying suspicious behaviour in public, going beyond the personal limitations of 'classic' identification tools (EDPS, 2021; Neroni Rezende, 2022). Multiple regulatory paths seem possible, and proportionality requirements will need to be adjusted accordingly if a ban is not adopted. Surely, if bans on social media scraping and emotion recognition are not adopted, EU institutions will have to ensure that such technologies cannot be combined with FR.

Lastly, the Council's and Commission's texts appear very weak on procedural safeguards. *Glukhin* reiterates that legal bases for surveillance should include rules to authorise the procedure, examine, use, and store the data obtained, as well as supervisory mechanisms and remedies (para 83). However, Article 5(3-4) is quite vague on this. This provision mandates Member States using live FR to foresee a prior authorisation by a judicial or independent authority, as well as rules for the request, issuance, exercise of, and supervision of such authorisations. It is unclear what aspects should be addressed under the rules relating to the "exercise of the authorisation". For example, do these extend to the examination, use, and storage of the data obtained? Can these be leveraged in other proceedings? Such vagueness may cause fragmentation across Member States. Therefore,

the Commission and the Council should negotiate a more detailed regime. Similar rules should also be extended to *ex post* FR.

Overall, reading *Glukhin* is worthwhile to spot gaps in the EU regulatory approach to FR. The Court leaves many questions open, which reinforces the need for clear and unambiguous choices by EU regulators. FR has sensitive implications for the endurance of democratic societies. Leaving things to interpreters' discretion may not be a good option. This is imperative if the EU means to move forward to a ban on FR altogether. However, the way seems still long in discerning the acceptable uses – if there are any – of remote biometric identification systems in the EU too.