The use of AI by the state to discourage the exercise of the freedom of assembly in Russia

Input for the report on the right to privacy in the digital age

SUBMITTED BY OVD-INFO

May 2021

About us

OVD-Info is a non-governmental human rights media project that provides legal assistance to those who face persecution for exercising their freedom of assembly.

In 2019, our lawyers handled 1,430 administrative and 30 criminal cases in the courts and assisted 2,212 detainees in police stations. In 2020, our lawyers participated in 502 court hearings, assisted 681 detainees in police stations, and filed 494 complaints with the European Court of Human Rights.

In our report, we will focus primarily on our area of expertise — freedom of assembly.

We are looking forward to the adoption by the Human Rights Committee of an updated General Comment on the right to privacy, hoping it would also explore the impact of emerging technologies on the right to privacy and the interlinkages of the right to privacy with other human rights, such as the right to assembly.

E-mail: data@ovdinfo.org

Relevant factors driving the development and use of AI in Russia (1.1)

Several factors propel the use of AI in Russia.

Firstly, in Russia, the state plays a central role in many spheres of life. On a federal level, there is a state policy promoting AI (the National strategy for the development of artificial intelligence till 2030, national policy for Russian digital economy, federal project 'Artificial intelligence'). Its goal is 'to raise the wealth and standard of living of its citizens, ensuring national security and public safety, achieving the competitiveness of Russian economy, including worldwide leadership in AI'.

On a regional level, the authorities in wealthier regions, such as Moscow, invest in technological solutions. There the use of face recognition software was being tested since 2016. Its vast public transport infrastructure is undergoing a rapid technological transformation.

Sometimes, different levels of government are finding common ground in the field. In the summer of 2019, wide-scale protests against the decisions barring independent candidates from competing in the Moscow city parliament elections erupted in Moscow. Thousands of people were arrested and prosecuted. In autumn of 2019, the Minister of Internal Affairs announced that all Moscow cameras would be equipped with face recognition software. The city bought the hardware for the system; the contract was initially valued at 1.2 billion RUB (about 19 million USD). In 2020 Moscow announced a further contract for 1.9 billion RUB (about 30 million USD).

Moscow IT department's annual budget is larger than 1 billion USD (90 billion RUB in 2020). In the absence of effective means of public participation, the funds are distributed at the executive's discretion. The lack of legal regulation and independent judicial oversight allow such developments to go unchecked without regard to human rights and the interests of the citizens.

This development is propelled by Russia's tech giants, tech market and high internet penetration, providing conditions to accelerate AI development. Citizens do reap some benefits; for example, face identification for contactless payment in the metro may be convenient for some. Tech giants use AI technologies for sophisticated user profiling to better market their services or sell ads. However, an indirect beneficiary is the government, as legally, it is entitled to access all such data collected and stored.

Uses of AI for the promotion of the right to privacy (1.2)

AI can help secure personal data, especially sensitive, from being improperly disclosed or published. Firstly, it could help hide such information as home address, place of work and medical conditions from documents that should be made public (for example, court judgements). Secondly, when such data is published to intimidate

political opponents (doxxing), companies can use AI tools to prevent it from recirculating.

Automated decision-making tools can help citizens defend their right to privacy in courts by offering free or cheap legal advice and help write legal documents. We are currently developing such tools.

Challenges posed by the AI for the exercise of human rights (1.3, 1.5)

The Russian society is already faced with challenges that the use of AI presents in the enjoyment of the right to privacy and assembly and fair trial.

The AI is, in certain circumstances, good at face recognition but is terrible at understanding context. In April and May 2021, the police used face recognition to track down dozens of peaceful protesters that came out on 21 April 2021. We know about at least 69 such cases. Among those identified at the protest were journalists working to cover the events, observers and passers-by. They were, in many cases, detained by the police for hours after being identified by the cameras. In the case of journalists and observers, this creates an illegal interference with their freedom of expression.

In other cases, facial recognition may be wrong. We have recorded numerous instances in which a wrong person was identified by the software and subsequently prosecuted for protesting peacefully. However, as the algorithms are complex and their results practically incomprehensible to humans, it makes it hard to rebuke its conclusions. This leads to their conclusions being practically unchallengeable in the courts.

Still another problem is that for standard machine learning models, the only way to remove an individual's data altogether is to retrain the whole model from scratch on the remaining data, which is often not computationally practical. In such circumstances, there can be no effective remedy.

Another challenge is that we can not know which data can be used to train AI or will be sensitive in the future (voice, walk, blinking patterns, etc.). The police now record such features of detained protesters as eye colour, height, weight, tattoos. The courts alluded to such features as necessary for identification. The head of the Russian Biometric society mentioned such features as enabling better automated identification when describing a system under development. Thus we are apprehensive that even people giving away such data voluntarily to the police are not fully aware of its implications.

The use of AI allowed Russian state authorities to identify and prosecute assembly participants without stressing the law enforcement machinery. It allows the police to track the movements of the identified person and choose the moment to press charges

and detain them which is convenient for them. The state has already been using face recognition systems to track the movements of political activists.

After detaining an activist at a protest, the police have started using facial recognition software to identify the detained at other protest rallies and prosecute them for it, as well.

Some telecommunication companies use automated filters to censor text messages mentioning assemblies, opposition politician Alexei Navalny or independent candidates in municipal elections.

Discriminatory impacts of the use of AI on specific groups in their exercise of the right to assembly (1.4)

The state is collecting sensitive biometric data from protesters detained for the peaceful exercise of the right to protest. It is also using AI technologies to track down and punish them for exercising assembly rights. The government is targeting its political opponents in a discriminatory way.

Non-citizens are more vulnerable to such technologies since they are in a vulnerable position, and they undergo compulsory biometric data collection. At the same time, there is a concern that AI models trained on certain subsets of the population might not be well-equipped for dealing with ethnic minorities.

Russian agency tasked with youth issues (Rosmolodezh) monitors social networks to protect teenagers from harmful information using machine learning algorithms and automated decision-making. Given the importance of social networks in the youth's life, this is undeniably an interference with the right to privacy. Moreover, the state is spearheading a particular policy, which bans communicating to minors that non-heterosexual ("non-traditional") relationships are normal (article 6.21 of the Code on Administrative Offences) or involving them in 'unauthorised' assemblies (Article 20.2, part 1.1 of the CAO). Other vague bans include 'justifying illegal behaviour'. The agency is using such monitoring to demand the removal of such information. It may communicate its findings to law enforcement and social workers, whose involvement carries a stigma and causes problems at school. Overall, such interference often results in violations of the rights to privacy, freedom of assembly, freedom from discrimination. It also interferes with their right to education.

Current legislative and regulatory frameworks (2.1)

1) The law "On (law-enforcement) intelligence-gathering activities" (144-FZ) allows "observation" and "identification", which may theoretically include AI. However, people subject to intelligence-gathering activities have little control and even knowledge about such procedures. They receive no warning, and the

options for challenging it are limited. The 144-FZ set forth a list of cases in which intelligence-gathering activities are allowed:

- An open criminal case.
- Information received by the law-enforcement conducting criminal intelligence gathering on:
    - elements indicative of a crime if such information is insufficient for the decision on opening a criminal case;
    - events or actions threatening Russia's security;
    - persons evading law enforcement;
    - missing persons, unidentified bodies.

The Constitutional Court found that intelligence-gathering activities are not allowed for violations other than criminal ones (Ruling N 86-O/1998 (14.07.1998) and Ruling N 327-O (09.06.2005)). However, contrary to this, in practice, police often exercise them for administrative violations.

2) Federal law "On personal data" prohibits any collection or use of personal data that characterise physical or biological features of a person without his or her written consent. Exceptions to this consent rule are listed in Article 11, section 2. They include the processing of personal data for court justice or intelligence-gathering activities. None of these exceptions allows the processing of personal data for administrative violation cases. Nevertheless, the latter practice is massive.

AI-related human rights gaps (2.2)

Consequently, detailed regulation for the facial recognition procedure is absent, leading to the following abuses. Facial identification is conducted on a mass scale without considering specific circumstances of a case and the seriousness of an offence (in violation of the right to privacy as interpreted by the ECtHR, Gaughran v. The United Kingdom, § 88). Such intelligence-gathering activities fall outside of judicial control, and such evidence is practically unchallengeable. There is no procedure to challenge such measures or initiate a review of the legality of storage of such sensitive information. The accuracy of algorithms and their limitations are unknown but presumed. The police are using such algorithms to identify specific people found to be unsupportive of the regime and seek other instances of their participation in 'illegal' rallies on the photo and video records stored by the authorities. This enables the police to file charges any time after the fact, causing law enforcement to become unpredictable.

The framework establishing the limits on who can access such databases, the maximum storage period, prohibited uses, logging of access, a periodical review is also absent.

Social networks use machine learning algorithms to ban content but do not consider public interests and the significance of such information. Human Rights Center 'Memorial', a leading Russian human rights NGO, had their Instagram account blocked because of mass reports. Appeals were long unsuccessful. Novaya Gazeta, a leading independent investigative newspaper, had their YouTube channel blocked moments before the long-awaited online marathon (stream) in support of political prisoners organised together with OVD-Info was scheduled to take place. YouTube later admitted there had been no grounds to block it.

Prohibiting certain AI use cases (2.3)

AI should be banned from being used on political activists. Law enforcement should not use it to identify and prosecute participants of peaceful assemblies, except for specific exceptional cases, such as identifying persons using violence on other protesters. The state would, however, likely abuse any broad exceptions from the ban.

No information for machine learning should be collected under duress (such as 'voluntary' fingerprinting of those detained at police stations). Such data shall only be provided voluntarily after an informed and revocable consent.

The authorities should collect the data for a specific case and purpose; its use for other purposes should be banned.

Algorithms that cannot 'unlearn' shall not be used.