GUIDEBOOK
ON THE APPLICATION OF BIOMETRIC SURVEILLANCE

SHARE Foundation

2023

Credits:

Editors:
Danilo Krivokapić & Andrej Petrovski

Authors:
Ana Martinović & Jelena Adamović

Art direction and Design:
Olivia Solis Villaverde

Publisher:
SHARE Foundation

2023

CONTENTS

WHY THIS GUIDEBOOK?

This guidebook attempts to serve as a starting point in mapping issues tied to the complex field of biometric surveillance. It aims to provide concrete recommendations for decision-makers on how to regulate and implement policies in the field of biometric surveillance in a way which complies with human rights and principles of the rule of law. The guidebook is therefore intended for all the stakeholders involved in the process of drafting, enacting and implementing laws and policies related to biometric surveillance. It could also be useful for civil society organizations and activists, who are seeking ways to get involved in the decision-making and oversight process.

In the guidebook, we primarily focused on the policy aspect of the phenomenon of 'remote biometric surveillance', being one of the most intrusive and prevailing negative trends worldwide. Remote biometric surveillance refers to any identification done "at a distance", using biometric data. Before going into specific recommendations, we will briefly explain the main terms and the process surrounding the use of biometric surveillance technology.

INSTEAD OF AN INTRODUCTION - A CASE STUDY ON INTRODUCING BIOMETRIC SURVEILLANCE IN SERBIA

In the text of the guidebook, we aimed to provide practical guidance which would presumably assist decision-makers in navigating through the complex process of regulating the use of biometric surveillance in their respective countries. Instead of an introduction, we wanted to tell you a story of how it all started - a short case study of a Serbian biometric surveillance legislative process. Our participation in that process gave us an invaluable experience and helped us map different issues and phases of policymaking and the interplay of different actors in a public arena. Drawing from the lessons learned during that time, we decided to create this guidebook.

How did it all start?

The first publicly-noted case of the biometric-enabled cameras being deployed in Belgrade was in June 2019. But the biggest rollout of the cameras across Belgrade came in 2020 and coincided with the COVID-19 pandemic and the subsequent national lockdown that was put in place.
Cameras were procured from the Chinese tech giant Huawei is the main supplier of surveillance for law enforcement in Serbia. This cooperation dates back to 2011 when the Serbian government and Huawei started talks on implementing a "Safe Society" project. The installation of 1000 surveillance cameras across 800 locations in Belgrade was announced in 2019 with a link to the "Safe City" project on Huawei's site. The page was quickly removed, but SHARE Foundation archived it in time.

DPIA process

The Data Protection Impact Assessment (DPIA), conducted by the Ministry of Interior in 2019 was sent to the Commissioner for Information of Public Importance and Personal Data Protection (Commissioner) for review of plans to install facial recognition cameras across Belgrade. According to the Commissioner, the DPIA did not meet the formal and material conditions which are prescribed by the national Law on Personal Data Protection. The Commissioner's opinion was that the unselective mass surveillance system being proposed by the Ministry of Interior could not be justified because it lacked a concrete purpose based on well-established facts. The biggest issue to date is that the government did not make a sufficient argument for the necessity for such a system, nor was it able to justify such an invasion of privacy.

Following the 2019 DPIA, the Ministry of Interior (MOI) submitted an improved version of their request to the Commissioner in March 2020. The reworked version of the DPIA still did not meet the Commissioner's requirements for the justification of such a project and was rife with arbitrary language. For instance, the DPIA showed plans for facial detection to be carried out on all persons walking through an area covered by the video-surveillance system, and for the police to use the system for profiling, even though it was unclear from the document what the profiling would specifically entail.

Two attempts at bringing law into the legal system

In September 2021, the MOI released a Draft Law on Internal Affairs which proposed provisions for the use of mass biometric surveillance technology in public spaces. SHARE Foundation submitted comments on the draft during the mandated public debate proceedings, pointing out that such a law would effectively legalize biometric mass surveillance. The comments called for several articles of the draft law that deal with biometric surveillance to be immediately removed, as well as an introduction of a moratorium on the use of biometric mass surveillance technologies and systems. The draft law was rescinded only a couple of days later amidst wide public scrutiny.

However, in late 2022, the MOI again released a re-revised Draft Law on Internal Affairs, along with a new Draft Law on Data Processing and Records in Internal Affairs, and a revised draft DPIA. Through the SHARE Foundation's analysis, it was determined that the risk of unselective and arbitrary surveillance and facial recognition practices were still not adequately addressed by the Serbian authorities. The new draft laws stipulated that the biometric data of residents would be extracted and retained for a period of 72 hours, which implies that the process is unselective and indiscriminate, allowing for potential gross violations of residents' rights to privacy.

Following public debates on the new draft laws, and thanks to a concerted effort from civil society organizations and help from the international community, including Members of the European Parliament, the draft laws were withdrawn from the procedure by the end of 2022. The government expressed a desire to further consult with experts in the field of data privacy and privacy issues in general before making any additional changes. This signalled a positive step in the fight against biometric mass surveillance, not only in Serbia but in Europe more broadly, as it showed clear dissatisfaction from the public and democratic representatives, especially on the transparency and accountability that was lacking in such a high-stakes endeavour.

WHAT IS BIOMETRIC DATA?

Our biometric features are our physical and physiological features (such as our face, eyes or voice). After being processed, they generate either biometric or biometrics-based data. The difference between biometric data and biometric-based data is primarily in their level of accuracy in establishing personal identification:

a. Biometric data are personally identifying data relating to someone's face, body, or other physical or physiological characteristics (face, gait, etc.), usually that have been processed into a machine-readable format (template) with some connection to a person's identity. Some jurisdictions, such as the EU, state that the data must be able to "allow or confirm" a person's unique identity to be biometric (for example, a template of a person's face) and are only sensitive when used for the "purpose" of unique identification;
b. Biometric-based data are data that may not initially seem to personally identify someone (e.g. hair colour, skin colour, emotion) and have been processed into a machine-readable format. However, with the increase in video capture power, many of these data are or will soon be able to uniquely identify a person. Even without this ability, their processing can still be equally intrusive or harmful. As such, we do not consider this to be a robust or scientific distinction. Instead, we advocate for biometrics-based data to be given the same (high) protections as biometric data. For these reasons, every reference to "biometric data" in the recommendations, will refer also to biometric-based data.

What is biometric surveillance?

Biometric mass surveillance refers to the untargeted collection, processing, or analysis of biometric data, usually in publicly accessible spaces. Being untargeted means that it does not only concern specific individuals of interest. Its non-selective approach means that it can span to gather the data of whole communities and even societies. In addition, it has a quality of being arbitrary, and more unselective than "targeted" surveillance such as phone

tapping, bugging, etc., which generally requires some form of authorisation like a warrant. In many European countries and many countries around the world, putting biometric surveillance to use is still largely an unregulated field.

Phases of the biometric surveillance process

The process of biometric surveillance commonly happens through several phases:

1. Monitoring biometric features (capturing of data);
2. Processing biometric features into biometric / biometric-based data - the process of extraction of biometric data;
3. Biometric identification - this is the process of predicting the identity of a person by comparing their biometric data against a specific database or multiple databases (e.g. national ID database, database of wanted persons) above a certain threshold of probability;
4. Potential use of biometric data obtained in the process - once identified, authorities might take a certain action based on the knowledge of the person's identity (e.g. allowing a person to cross the border based on the identification of a person's data in the biometric passport, arresting person based on the establishing of their identity through the use of biometric technology, etc.);
5. Storing biometric data - this phase could precede the phase of use of biometric data, depending on the purpose for which the surveillance is happening.

What is computer vision?

Biometric surveillance is possible through the use of artificial intelligence (AI). Artificial intelligence is the ability to perceive, analyze and understand information by machines, which can be applied to autonomously perform tasks in different fields, such as speech recognition, computer vision or natural language processing. Computer vision is an area of artificial

intelligence which allows machines to analyze and understand information acquired from various visual inputs, such as digital images or video materials.

Computer vision applications that can be used in a surveillance context are, for example: object recognition (car, person, suspicious device in the street for example), facial recognition, emotion recognition, behaviour tracking, etc. A significant amount of data must be used to train the system for it to be developed as a computer vision system. These data are used as an input value for learning, which helps the system interpret the information it receives and analyzes.

This whole process is not purely technical, but it has certain core (human) values built into its roots. Image datasets that are "fed" to the system for training may be based on social stereotypes and prejudices. This can have particularly adverse effects on ethnic minorities, people of colour, people on the move and essentially groups that don't fit into "normal"/"average" appearance or social status for various reasons.

Capabilities, risks and concerns related to the use of biometric surveillance and modern technologies

The highest risk of use of biometric surveillance nowadays comes from unregulated and/or unclear **mass biometric surveillance practices**. These practices allow for the use of a system which captures and processes multiple people's biometric features at once. Commonly, mass biometric surveillance is exercised in public spaces, which makes it possible that none of the people captured by surveillance technologies are aware of it happening. The use of mass biometric surveillance systems is by definition untargeted, and could therefore be excessive and intrusive, especially if performed without justification and procedural safeguards.

Risks and concerns related to the use of biometric surveillance technologies, as recognised by the European Data Protection Board in their 2022

Guidelines on the use of facial recognition technology in the area of law enforcement, include:

Chilling effect - The use of widespread and intrusive surveillance technology in public spaces makes citizens feel that they are subjected to constant surveillance, without even being sure if it is so. The feeling of significantly narrowed personal freedom, or even complete loss of privacy in public spaces, drastically changes behaviour and negatively affects the individual's personality, thereby ultimately affecting the character of society and corroding many democratic processes.

Threat to private life and data misuse - When used in public areas, including transportation nodal points or, technology that allows governments to track and analyze an individual's movements and uniquely identify them will reveal even the most private information about that person, including sexual preferences, religious beliefs, or health issues. This increases the very real possibility of unauthorized access to and exploitation of the data.

Threat to human rights and authority abuses - Due to the strong chilling effect caused by the mass processing of biometric data, a number of human rights and freedoms are directly threatened, such as freedom of thought, conscience and religion, freedom of expression, freedom of assembly and association (including attend a protest or other forms of organized gatherings). These threats are directly lined to the potential for abuse of this technology. Most serious abuses of authority may include tracking down movements and life patterns of activists, political opponents or whistleblowers. "Live" facial recognition, i.e. identification of people from surveillance footage processed in real-time, gets a lot of attention, but retrospective biometric identification of people from recorded video materials is not any less dangerous.

Threat to presumption of innocence - In scenarios where police officials use remote biometric identification, they are effectively treating every person as a possible suspect. In societies where the law is upheld, people are assumed to be righteous until and unless wrongdoing is established. Therefore, the mass and indiscriminate use of technologies such as facial

recognition also threatens the right to the presumption of innocence (Article 6 of the European Convention on Human Rights).

Possibility of misidentification - Although there are different manners to calculate the level of accuracy of facial recognition technology, as is pointed out by the EU Agency for Human Rights: "when applying the technology in places visited by millions of people – such as train stations or airports – a relatively small proportion of errors (e.g. 0.01 %) still means that hundreds of people are wrongly flagged." This can result in serious legal and practical consequences for citizens, including wrongful arrests or criminal convictions.

Threat to professional secrecy and journalism - Parties affected by mass surveillance include journalists, attorneys, and clergy who have a professional interest in maintaining the confidentiality of their connections (and frequently a corresponding legal obligation to do so). Therefore, there are risks of journalists' sources being revealed, or it might reveal that someone has consulted with a criminal defence lawyer or certain religious priesthood.

Threat to dignity - Citizens' unease with mass surveillance presence in public spaces may cause them to stay away from locations where it is used. This can lead to them avoiding certain social situations or cultural activities. Over time, people's ability to live a dignified life may be significantly impacted by the mass deployment of facial recognition technologies.

Vulnerable groups, discrimination and bias - Significant racial and gender bias effects are often incorporated into facial recognition systems. False-positive outcomes disproportionately impact women and people of colour, which leads to prejudice. Following a false-positive result, police actions like searches and arrests may further stigmatize already endangered communities or groups. Some vulnerable groups, such are children, cannot at all the protected in mass surveillance scenarios.

What is techno-solutionism?

Techno-solutionism is the term used to describe the intervention of technology into politics, culture and everyday life, with the belief that technology has the ability to solve political and social problems.[1] It is based on the "assumption that technology can correct for human error, pushing systems toward a standard of computational objectivity".[2]

However, the potential of automated systems to foster, perpetuate, and exacerbate social injustice is becoming more and more obvious. This is due to the lack of practical objectivity in machine predictions: as it must be humans who use faulty datasets that contain historical bias to make the systems do what they do.[3] When the system is deployed on such a flawed basis, all its outcomes can deepen the problems the system aims to solve or create a new set of non-predictable problems. So, more often than not, the solutions proposed by the technology sector tend to backfire, if not countered by legal regulation embedded with the proper ethical and human rights standards, procedural safeguards, and liability. This is also caused by the fact that the complexity of social problems is often neglected by techno-solutionists. Some social problems are simply ill-suited to be tackled by technology, as they are dependent on a whole range of social influences, human interactions or cultural or psychological factors.

Nowadays, many companies offer technological solutions that claim to solve certain political and societal problems. On the other hand, governments that procure such solutions are liable for their use and its effect on individuals and society. Neither companies nor governments should be devoid of responsibility for tech-solutions usage and should be able to account for the technologies they are implementing. With the introduction of the UN's Guiding Principles on Business and Human Rights, more and more legal systems are considering or implementing clear human rights obligations on companies.

1 E. Morozov, To Save Everything, Click Here: The Folly of Technological Solutionism, PublicAffairs, 2013

2 G. Byrum and R. Benjamin, Disrupting the Gospel of Tech Solutionism to Build Tech Justice, Stanford Social Innovation Review (SSIR), June 2022

3 Ibid.

HUMAN RIGHTS VS. BIOMETRIC SURVEILLANCE

General recommendations:

- **Biometric surveillance regulation and implementation must not infringe upon the enjoyment of basic human rights and fundamental freedoms, such as the right to privacy, right to data protection, freedom of expression, freedom of assembly, freedom of movement, prohibition of discrimination on any ground;**

- **To avoid the possibility of human rights violations, the legislation and policies put in place should be formulated in a clear and foreseeable manner. Moreover, governments must ensure that biometric data receives specific and sufficiently high levels of protection due to its inherent sensitivity. High levels of protection apply to all the phases of handling the biometric data - data collection, storage, use and removal of data from databases;**

- **Governments must draw clear red lines when it comes to collecting and using biometric data. Certain practices, such as mass biometric surveillance, should be explicitly prohibited.**

Biometric data have a twofold nature: they are part of our bodies and therefore fall into the sphere of protection of our privacy and private life, and they are also information. This makes them particularly sensitive and requires special attention on the side of the legislator, government, enforcement bodies, courts and operators of such data. Every phase of handling biometric data should be carried out with an elevated level of attention and with the particular consideration of potential human rights violations such handling might lead to.

This is not to say that the biometric data should not be gathered or used. It is important to note that every such gathering, processing and use has to occur in a way which is: a) regulated by the law, in a clear way, which does not allow

for free interpretations and b) in line with human rights standards, meaning that gathering, processing and use of biometric data does not infringe upon citizens' human rights. In case interpretations of biometric provisions are required, they must be given by the official authority, such as the legislator, the court or the independent data protection authority competent for oversight of the use of biometric surveillance technologies. Law must also be foreseeable, meaning that it is easy from reading it to predict its effects.

The use of biometric surveillance, as one of the biometric data gathering technologies, carries with it risks of multiple human rights violations. In any case, biometric surveillance by the state or private actors restricts the enjoyment of certain fundamental rights and freedoms. For these restrictions to not amount to human rights violations, certain conditions have to be fulfilled:

1. restrictions have to be prescribed by law;
2. restrictions need to pursue a legitimate aim, and
3. restrictions need to be necessary in a democratic society.

When analyzing whether the restriction violates one of the below-mentioned human rights, legislators, law enforcement authorities and judicial bodies should carry out proportionality analysis, i.e. analyze whether the means used to restrict the freedom of expression were proportionate to the goal which was intended and whether the same goal could be achieved by less intrusive means. The same set of criteria for restrictions applies to all the rights addressed below, for which reasons these will not be particularly analyzed under every human right in every case.

Having in mind the conditions for restrictions, it is abundantly clear that certain practices will, almost without any analysis, present a breach of human rights and governments should therefore abstain from allowing them. One such example is mass biometric surveillance, which will almost certainly never pass the test of proportionality - the highly intrusive and disproportionately large volume of mass surveillance will always be too excessive for whichever goal it has to fulfil, be it the safety of citizens, prevention of crime or disorder. It is without exception possible for all these goals to be achieved in less obtrusive ways. That is why mass biometric surveillance is the ultimate red line which governments should refrain from and explicitly prohibit when regulating the field of biometric surveillance.

Meaning and importance of public spaces

Recommendation: It is necessary for governments to ensure safe public spaces while enabling the enjoyment of the human rights of citizens temporarily inhabiting these spaces. The use of biometric surveillance in public spaces must be regulated in such a way as not to disproportionately restrict anyone's fundamental rights and freedoms.

Most violations stemming from the use of biometric surveillance occur in public spaces. Public spaces, particularly in urban environments, are places where we spend a great part of our days and where our parts of private and public lives occur. It is therefore important for governments to ensure the enjoyment of our human rights while in public spaces while keeping them safe. Violations happen exactly from the poor balancing of these two goals. It is important to note that, for purposes of protection of the freedom of expression, the Internet could be also considered a public space. Although it is a context-specific rule (as described in the ECtHR judgment of *Sanchez v. France* and numerous US judgments, such as the 2019 judgment of the United States Court of Appeals for the Second Circuit, concerning Donald Trump's behaviour on Twitter regarding his blocking of his political opponents), it should not be disregarded that major breaches and abuses of biometric data could also happen on the Internet.

Freedom of expression

Recommendation: Biometric data regulation could not be formulated or implemented in a way which violates the freedom of expression.

Freedom of expression is the freedom to hold opinions and to receive and impart information and ideas is essential to both personal expression of self and to the right of citizens and press to participate in democracy through means of public discourse.

Limitations of this freedom are only allowed if they meet the criteria of being prescribed by the law, pursuing a legitimate aim and being necessary

in a democratic society. Given that the nature of the freedom of expression is such that the expression of our opinion will often occur in a public space, during assembly with others, this right often overlaps with the freedom of assembly. The use of biometric surveillance in public spaces tends to have a repressive effect on freedom of expression in public spaces.

In the ECtHR judgment of 4 July 2023 in the case of *Glukhin v. Russia*, the ECtHR found a violation of Mr Glukhin's right to private life and his freedom of expression. Mr Glukhin travelled on the Moscow underground with a life-size cardboard figure of one famous Russian protestor, who had been facing a harsh prison sentence for peaceful protesting. The video of Mr Glukhin's protesting had been uploaded on social media. Russian police identified him during routine monitoring of the Internet. Mr Glukhin claimed that they had used facial-recognition technology for his identification, i.e. collected footage from closed-circuit television (CCTV) surveillance cameras installed in the stations of the Moscow underground through which he had transited on 23 August 2019, and, several days later, used live facial-recognition technology to locate and arrest him while he was travelling in the underground.

The ECtHR found a violation of Mr Glukhin's right to private life and freedom of speech, on the following grounds: a) the lack of detailed rules in the domestic law governing the scope and application of measures involving the use of facial-recognition technology as well as the absence of strong safeguards against the risk of abuse and arbitrariness and b) the measures taken against Mr Glukhin had been particularly intrusive in the face of what had been a peaceful protest, which had not presented any danger to the public or transport safety. Mr Glukhin was in fact only prosecuted for a minor offense.

Freedom of assembly

Recommendations:

- **Biometric data regulation could not be formulated or implemented in a way which poses a threat to the freedom of assembly of citizens;**
- **Governments should refrain from practices which allow authorities to use biometric surveillance technology on**

citizens peacefully gathering in public places, under the pretext of maintaining public safety;

- **Governments should regulate the possibility of using biometric surveillance in public spaces only in absolutely necessary cases: for example for the protection of citizens from expected outbursts of violence, under the clearly defined procedural criteria, which include prior approval of the judge or a similar decision-making authority.**

Freedom of assembly is defined as the right of everyone to assemble peacefully with others.

The assembly, under the meaning of this right, means any peaceful gathering of people both in private and public places. The scope of this right is not limited only to political peaceful demonstration and participation in a democratic process, but also to assemblies of a social character, cultural gatherings, religious and spiritual meetings. Restrictions to this right are possible, but similarly to the freedom of expression, have to be carefully weighed against the public interest. Only once the fair balance is struck between the public interest and individual freedom, we could say that the limitation of freedom of assembly was allowed.

Unrestricted mass biometric surveillance, with the possibility of unlimited biometric data processing, opens up endless opportunities for infringement of this right. Due to the various nature of possible gatherings, the use of biometric surveillance to limit the enjoyment of peaceful assembly could have long-lasting consequences of citizens failing to participate effectively in a democratic process. Possible infringements affect in particular members of political opposition, journalists and human rights activists. Moreover, the use or possibility of use of biometric surveillance could also prevent citizens from moving in public spaces and hence contribute to creating a distrustful, alienated and secluded society.

The example of the United Kingdom showed recently how biometric surveillance can be used to restrict freedom of assembly. The case of *R (Bridges) v Chief Constable of South Wales Police (2020)* was concerned, *inter alia*, with the use of facial recognition technology during protests that were held in London in 2018. Here, the UK Court of Appeal did not go into the matter of the right to freedom of assembly under Article 11 of the

ECHR, but it did find that the use of facial recognition technology by the police in this case was unlawful as it breached privacy rights, data protection laws, as well as equality legislation.

Right to privacy

Recommendation: A person's right to privacy must not be violated due to the use of biometric surveillance. The use of biometric surveillance has to be followed by strong procedural safeguards against arbitrariness.

The right to privacy, or the right to private life, is the right of everyone to maintain his identity, private life and personal sphere without intrusions, with the exception of allowed limitations cited above. Bearing in mind the particularly intrusive nature of the biometric surveillance techniques, this right means that the state must provide adequate safeguards when limiting the enjoyment of this right. As the ECtHR established in the already cited case of *Glukhin v. Russia*, in cases of using biometric surveillance, the state has to provide detailed rules in the domestic law governing the scope and application of measures involving the use of facial-recognition technology as well as the strong safeguards against the risk of abuse and arbitrariness.

Right to data protection

Recommendations:

- **Biometric surveillance systems should not deploy techniques which infringe upon the right to data protection of persons whose data is being obtained, stored, processed and disposed of;**
- **Governments should rigorously regulate biometric databases to only those that are strictly necessary: a) strictly limiting databases which are used for criminal investigations or prosecutions to include only convicted persons or suspects meeting a legal threshold of reasonable suspicion, with sufficient rules for removal in case of acquittals, etc. and b) ban of the use of facial images or other biometric data in other**

databases (such as passport, driving license databases, etc.) for any purpose other than administering these databases.

This right is derived from the right to privacy with the development of the EU General Data Protection Regulation (GDPR) and the Council of Europe Convention 108.[4] It has all the elements of the right to privacy, but it pertains only to personal data. In that respect, this right deals with the manner of obtaining personal data, storing them, processing them and disposing of them, in the context of the effect this might have on our private lives.

The above-mentioned case of *R (Bridges) v Chief Constable of South Wales Police* (2020) dealt with the police use of automatic live facial recognition technology on crowds. According to the decision, South Wales Police violated the rules for processing unique and sensitive data under data privacy legislation by using technology for real-time biometric surveillance on two concrete occasions that were the subject of the decision. The Court of Appeal held that South Wales Police piloting of facial recognition tools on these occasions had not satisfied the "in accordance with law" requirement and, as such, violated Article 8 of the ECHR.

Multiple ECtHR cases on data retention have developed meanings of certain terms in the context of data protection. At this point, it is worth noting that the ECtHR has dealt with the safety of biometric databases in the case of *Willems v. the Netherlands*, concerning the applicant's request to the local municipality to issue him a passport which is non-biometric, at the time when the biometric passport was a legal standard. The ECtHR in its decision relied heavily on two preliminary reference rulings on the matter, delivered by the Court of Justice of the European Union (CJEU). The ECtHR upheld the opinion of the CJEU that storing biometric data, such as fingerprints, not in a centralized database, but within the passport, which his owner always has on his person and uses only in situations of border crossing, does not infringe on a person's right the privacy in the context of data protection. The case could be used as an initial point in the analysis of what kind of database is to be considered adequate from the data protection standpoint and for which purposes the data could be used. This could be

4 Council of Europe Convention for the protection of individuals with regard to the processing of personal data

applied by analogy to banning the use of facial images or other biometric data in driving license databases for any purpose other than administering driving licenses.

Freedom of movement

Recommendations: The use of biometric surveillance should not infringe upon the person's freedom of movement

Freedom of movement is the freedom to move freely within the territory of one state and the freedom to leave any country, including his own. Such freedom is not absolute and is subject to the same restrictions as the other aforementioned rights. Where biometric surveillance and this freedom come into potential conflict is usually in the field of border crossing policies.

Facial recognition technologies are already deployed by some governments to control border crossings. These technologies are linked to pushback practices, i.e. the collective expulsion of persons, usually before they reach a particular country or territory, often in very dangerous ways. Some studies have shown that minoritised immigrant populations were found to be at higher risk of discrimination and criminalisation by national enforcement authorities in certain European countries.

In the EU, the latest version of the AI Act regulates that the high-risk AI systems include those systems in the areas of migration, asylum and border control management, under the conditions regulated in the AI Act. Once the AI Act enters into force, this would impose limitations on biometric surveillance border policing technologies. However, before the entry of the AI Act into force, it is important for the member states to introduce appropriate safeguards into their national legislation.

The high standards of the AI Act should be strictly observed by any decision-maker. The potential for violation of the freedom of movement with sophisticated AI surveillance technology was recognised in various discussions that were held during AI Act drafting and negotiations. For example, in May 2023, two committees of the European Parliament voted to endorse protections in the AI Act that would ban several uses of emotion recognition technologies (including law enforcement and migration),

biometric categorisation, remote biometric identification in publicly accessible spaces, and predictive policing systems. The negotiating position of the European Parliament from June 2023 followed the same concerns.

Discrimination

Recommendation: Biometric surveillance systems should not be deployed in a way which discriminatively targets certain groups. Biometric evidence should not be used as sole and decisive in the proceedings.

Border control practices, most notable examples coming from Greece as the Schengen entry point on a migrant route towards Western Europe, and targeting citizens in public spaces in the United States by using biometric surveillance have already shown a tendency of discriminatory targeting of minorities, racialised and disenfranchised groups. Results obtained from using biometric surveillance still do not have an absolute level of accuracy. There have already been court decisions in the United States based on the use of biometric surveillance, which the targeted persons tried to rebut as unreliable evidence since they claimed that the results obtained did not match their faces.

Countries are putting in place policies of biometric surveillance which will have obvious discriminatory results, such as the policies of using biometric surveillance in predominantly African-American neighbourhoods in the United States or around the borders of Europe. Powerful image recognition abilities of the biometric surveillance systems only deepen social disparities and accentuate the power gap in society - such software serves states and powerful non-state actors (big companies) and inevitably targets the most socially vulnerable categories of citizens.

To avoid this kind of targeting, the legislators need to put in place laws which would not give the sole and decisive power to evidence gathered by using biometric surveillance, but take it into account as one of the pieces of evidence during any kind of proceedings (criminal proceedings, asylum proceedings, etc.).

Countering mass surveillance

The ECtHR in its case law related to secret surveillance, interception of communication and data retention (see cases *Centrum för Rätvissa v. Sweden*, *Big Brother Watch and Others v. The United Kingdom*, *Ekimdziev and Others v. Bulgaria*) developed a clear set of criteria on human rights safeguards which national laws have to contain to effectively counter possible human rights violations arising from surveillance. These safeguards could be applied by analogy to the field of biometric surveillance:

1. The law must be accessible to the public.
2. There should be a clear legal grounds for the use of biometric surveillance and regulating which persons could be placed under biometric surveillance.
3. Duration of biometric surveillancemust be regulated.
4. There should be authorisation procedures, meaning the rules on: a) which authority can authorize the use of biometric surveillance and b) the manner in which that authority reviews biometric surveillance requests and authorizes them. We strongly advocate for this authority to be the court, since that allows for a subsequent appeal process.
5. There should be clear procedures prescribed for storing, accessing, examining, using, communicating and destroying data obtained through biometric surveillance.
6. People who are about to be put under biometric surveillance should be informed of the biometric surveillance warrant.
7. Remedies must be accessible and effective to be able to provide an appropriate redress in case of breaches of rights incurred due to biometric surveillance. One of the remedies should be a claim for damages. However, it is important for remedies to include also the possibility of the court ordering the destruction of the surveillance material.
8. Oversight arrangements by supervisory authorities must be set.

LAW MAKING

National processes of creating laws and policies have a different way of being carried out, both on paper and in practice. The legislative/policy-making process depends on the field that is about to be regulated, its complexity, the number of interested parties in the process (stakeholders) and the general political climate at the time when the process is unfolding. Technical and ethical complexity of biometric surveillance and regulation of biometric data, and the potential existence of directly applicable supranational law such as GDPR, Law Enforcement Directive (LED), AI Act once it enters into force or the European Convention on Human Rights and the Council of Europe Convention 108+, only bring additional layers to the legislative processes. This chapter thus aims to provide a simplified mapping of the most common issues when it comes to regulating biometric surveillance on a national level and some recommendations on how to avoid them.

Background and the context of use

Recommendation: Any new legislation or policy involving handling biometric data or introduction of the use of biometric surveillance technologies should be preceded by a detailed explanation of the government to the stakeholders and the public on the background and reasons for such measures. The explanation should come in a thorough, but easily understandable form, so as to open a public dialogue around the proposed measures.

The intrusiveness and highly abstract nature of biometric surveillance technologies require that every legislative attempt is preceded by a detailed but understandable explanation of the following points:

1. Purpose of the new piece of legislation or policy - any intention to gather, process or use biometric data or to deploy biometric surveillance technologies should be preceded by a clear explanation as to what is their purpose and why such measures are necessary to be introduced. The government should, in the act of full transparency, aim to publish the risk assessment study, in a way which is available to other stakeholders, citizens and civil society.

In addition, the government should make itself open to comments and clarifications on reasons for the introduction of these measures in every phase before the law/policy enters into force;

2. Ways of deploying biometric surveillance technologies or using biometric data - the government should provide a clear explanation to the public about how it aims to regulate this field.

These explanations and information are best to come (also) in an understandable form for a layperson so that it can foster public debate and allow citizens and civil society to provide comments on new laws or policies.

There should also be clear mechanisms determined in advance that would enable the government to include the results of the public debate in the legislative proposal. Enough time should be devoted to public debate so that it fully accomplishes its aims, instead of formally "thinking the box" so that the government could use it as the legitimization of the legislation.

Necessity and proportionality analysis as the balancing mechanisms

Recommendation: In order to ensure that the biometric surveillance policy restricts human rights least possibly, during the legislative process, decision-makers need to carry out a detailed analysis of the necessity and proportionality of proposed measures and introduce only those that are minimally invasive for the citizens.

Mitigating risks of human rights violations is possible through a careful analysis of whether the proposed manner of use of biometric surveillance is necessary and proportional to the goal with which it is being introduced. Necessity and proportionality as the standards are already explained in the context of human rights in the chapter above. In terms of new legislation, they work as a balancing mechanism to the state's intrusion on citizens' human rights.

When it comes to biometric surveillance, necessity and proportionality usually refer to the following type of analysis:

1. Necessity - Bearing in mind the particular sensitivity of biometric data on one side and advanced biometric surveillance technologies which are highly intrusive on the other, necessity analysis means that the stakeholders must carefully analyze whether the introduction of biometric surveillance at all and if so, in which form, is a necessary measure. In this analysis, stakeholders will measure conflicting interests - on one side, regard for citizens' human rights, on the other side, some form of public interest, be it protecting the health and safety of a larger group of citizens, or public security (both in context of securing large public spaces and in the context of allowing biometric surveillance to third private parties for purposes of securing public spaces, e.g. use of surveillance on sporting events, etc.). A necessary measure is one which cannot be imposed in this shape and form, i.e. which cannot be replaced by some other measure.
2. Proportionality - Proportionality analysis goes hand in hand with necessity, as the logical next step. It weighs the restrictive quality of the measure against the goal which is intended to be achieved with it, all with the purpose of minimally invading the human rights of the citizens. Following the example of the necessity of increasing police surveillance on the streets in cases of elevated street crime, this further means that stakeholders would have to measure how the goal of improving the safety of citizens and minimizing street crime could be achieved in the least intrusive way for the enjoyment of citizens' human rights in public spaces. It is safe to assume that such a goal could be achieved with an array of measures. For these reasons, decision-makers need to analyze whether the milder measures within that umbrella could lead to the fulfilment of the same goal. If so, the conclusion is that there is no need for a more intrusive measure. In cases where the rate of street crime is elevated, but still within the confines of what can be controlled and contained, there is possibly low to no need for the introduction of biometric surveillance as a measure, since the same goal could probably be achieved by an increased number of patrolling police officers on city streets or different criminal investigation techniques.

The body proposing the legislation or the new policy, usually within the government, together with the policy drafting group and stakeholders is the

one responsible for carrying out this analysis. Such an analysis has to be later assessed by the national parliament, before voting on the law.

Justification for the introduction of biometric surveillance could also be embedded in the wording of the policy, in the form of the preamble, or some other drafting technique. Such an explanation gives the law a higher level of legitimacy and shows that the decision-makers and the parliament took into account possible risks of human rights violations.

Since biometric surveillance is a rather technical topic, this analysis is often outsourced to specialized independent bodies or specialized governmental bodies. Necessity and proportionality analysis are usually framed within different risk assessments, which will be analyzed below.

DPIA and other risk assessments

Recommendation: Before putting in place biometric surveillance legislation/policies, the governments must conduct a thorough data protection impact assessment (DPIA) and other types of risk assessments.

As mentioned above, carrying out a necessity and proportionality assessment in cases involving handling biometric data or potential use of biometric surveillance technologies, usually involves expert knowledge that the government bodies do not themselves have.

With one of the biggest obvious risks connected to handling biometric data and use of biometric surveillance being a violation of the right to privacy and right to data protection, carrying out data protection impact assessment (DPIA) is essential.

The GDPR requires a DPIA in the case of "systematic monitoring of publicly accessible areas on a large scale" (Article 35(3)(c)), and establishes an obligation to designate a data protection officer if the processing "by its nature entails regular and systematic monitoring of data subjects on a large scale". This is of key relevance to the question of biometric surveillance because this definition includes the use of biometric technologies, such as facial recognition when monitoring and tracking individuals in public

spaces. DPIAs are also required in the case of automated profiling (Article 35(3)(a)) and when processing special category data (Article 35(3)(b)).

According to the GDPR, DPIA should contain as a minimum: a) a description of the envisaged processing operations and the purposes of the processing, as well as the legitimate interest pursued by the controller; b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; c) an assessment of the risks to the rights and freedoms of data subjects; and d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR.

If DPIA reveals that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, then the controller has an additional obligation to consult the supervisory authority before processing. If the supervisory authority is of the opinion that the intended processing might violate GDPR, it will provide written advice to the controller and it may further use any of its investigation or corrective powers. This includes the power of the supervisory authority to impose a temporary or definitive limitation including a ban on processing.

However, DPIA is not the only type of analysis or assessment that deployers of biometric surveillance programs should prepare. As mentioned above, when biometric surveillance techniques are being introduced, privacy and data protection are only one of the risks. There are multiple other risks to be taken into account, which should be considered and thoroughly assessed, such are risks associated with human rights or technological security.

According to the latest version of the AI Act, the use of the real-time remote biometric identification system in publicly accessible spaces should be authorized only if the relevant law enforcement authority has completed a fundamental rights impact assessment. The purpose of that assessment is to help the deployer identify the specific risks to the rights of people or groups of individuals who may be impacted and to recommend actions to be done should those risks materialize. This assessment should consist of a) a description of the deployer's processes in which the AI system will be used in line with its intended purpose; b) a description of the period of time within which, and the frequency with which, each system is intended to

be used; c) the categories of persons and groups likely to be affected by its use in the specific context; d) the specific risks of harm likely to have an impact on these persons or groups; e) a description of the implementation of human oversight measures; f) the measures to be taken where those risks materialize, including the arrangements for internal governance and complaint mechanisms.

In addition, when it comes to high-risk AI systems, such as the ones involving any biometric data, the AI Act Imposes the obligation of providers of such systems to perform the conformity assessment. This assessment is actually the whole process of demonstrating whether the requirements relating to a high-risk AI system from the AI Act have been fulfilled in the concrete case.

In addition to the protection of personal data and human rights noted above, the matter of citizens' security and protection is also important. In that sense, conducting studies on the safety and security of citizens in public spaces, safeguarding health, prevention of terrorism, prevention of crime and criminal investigation may provide some significant insights into certain scenarios. These studies could in some cases serve to explain why there is the need for the introduction of biometric surveillance technologies into some limited public spaces, by providing an insight into the specific statistics, or concrete methods of intended use of biometric surveillance technologies under specific circumstances or could provide examples of comparative practices where these methods have proven to be successful, etc.

Stakeholders and their involvement in the law and policy-making process

Recommendations:

- **Stakeholders should work together to get a proper grasp of the complexities of the topic of biometric surveillance prior to resorting to regulation.**
- **In order to prevent stakeholders from becoming gatekeepers, laws and policies should be created in a transparent process and implemented in a transparent process.**

The complexity of the topic of biometric surveillance, as we see, means that when it comes to regulating it, there are many interested parties who want to be involved in the process. These parties, known as stakeholders, are the government, national and European data protection authorities (DPAs), including the bodies overlooking the implementation of the AI Act, national courts, prosecution and law enforcement authorities, private companies who are developing biometric surveillance systems or purchasing them for their use, the legal community, civil society organizations and international organizations, such as the EU or the Council of Europe. All of them might be to a certain extent involved in the legislation-making process. Broadly speaking, interested parties are also the general public that can comment on the legislation and international community.

Once the legislation has entered into force, some of these actors would be responsible for its implementation. However, in order to prevent these state stakeholders from becoming gatekeepers, it is necessary for the legislation to contain provisions that allow for transparency. This can be achieved through instituting a legislative process which is transparent and open to participation of interest parties and various reporting duties on behalf of the state actors once the legislation is in force. The reporting duty should also fall on companies that use or provide biometric surveillance systems. Moreover, companies users of the biometric surveillance systems and companies providers could be having similar 'gatekeeping' duties as those recently imposed under the Digital Markets Act (DMA).

Transparency of the process and what it entails

Recommendation: Public debate, disclosure and transparency are necessary when the state is introducing new policies allowing the state and companies to use biometric systems.

Interested general public, academics, and human rights defenders cannot rely on occasional articles and non-governmental organizations to explain the proposed measures and its impact. From the initial phase of a legislative effort until any legal act is implemented, transparency should be present

from the government side – in terms of the types of information available as well as the manner in which that information is communicated (formally and informally).

In the initial legislative phases, the decision makers would have to ensure that the interested public is well-informed of a) the decision-making process, the steps taken so far and ways of the public to participate in the legislative process (for example, by submitting comments to the draft legislation during the public debate phase, or participation at open public discussions); as well as b) the content of the proposed legislation and its impact on citizens.

The content of new laws and policies should be elaborated to the public clearly and understandably, with a particular focus on ways of using biometric surveillance technologies and their impact on the enjoyment of human rights. The decision-makers should be also open to the feedback they receive from the public and should address any concerns brought up by citizens or the professional community.

Given the high complexity of the topic, experts from various fields should be involved and heard in this public discussion. Any technical issues concerning the concrete technology that might be used for biometric surveillance should be discussed taking into account the inputs from technical experts. They are the ones that would be well suited to understand and further explain the technical capabilities and limitations of any technology that can be used for surveillance purposes. For them to be able to participate in the discussion, the government must be transparent about any equipment procurement plans.

On the other hand, there are matters relating to the social impact that any biometric technology in public spaces would have on citizens. On those topics, experts from the field of sociology or psychology should have their say. As noted above, when it comes to the effect that biometric surveillance can have on citizens' rights and freedoms, various legal concerns should be analyzed. The same goes for the effect that concrete biometric surveillance legislation can have on the enforcement of other laws, such as criminal or migration laws.

In case some legislative proposal is actually passed, transparency obligations from any applicable laws should be diligently applied, as a minimum.

Personal data protection laws, as well as the AI Act, already contain concrete rules and obligations regarding the information that must be made available. Because of the sensitivity and complexity that comes with new technologies such as facial recognition, there should also be an additional educational effort from the government side to make sure that new rules are understood and acknowledged.

Liability

Recommendations:

- **The state should be held liable for violations of personal rights due to illegal use of biometric surveillance systems;**
- **The state should be held liable for the choice of companies from which it is purchasing biometric surveillance systems;**
- **Private companies using or providing biometric surveillance services should have compliance procedures in order to conform to legal requirements and human rights standards;**
- **Private companies should be liable for violations of personal rights due to illegal use of biometric surveillance systems.**

Issues of liability for the application of biometric surveillance systems lie primarily on the state, which has to safeguard the rights of everyone under its jurisdictions. Hence, it is necessary to establish a system of the legal liability of the state for human rights abuses incurred through the use of biometric surveillance, in the form of pecuniary claims.

The state is furthermore liable for the choice of its biometric surveillance system providers. Such liability should be established through a process of regulated and transparent public procurement, which allows for judicial review. Interested parties must be able to contest potentially illegal procedures of procurement of biometric surveillance systems.

Liability of private companies could be instituted through the process of internal complaint mechanisms or court mechanisms. Furthermore, private companies should be held liable for the mistakes arising from the lack of compliance with the biometric surveillance standards.

Bans of certain uses - policy red lines

Recommendations:

- **The harms posed by biometric surveillance systems are not hypothetical, and it is therefore necessary for governments to put forward laws which will prohibit unacceptably risky uses. This should cover not just use by police, but by all state authorities, as well as private actors;**
- **Such legislation should treat "real-time" (aka live) and "retrospective" uses of systems equally seriously;**
- **Mass biometric surveillance in public spaces for which there is no adequate reason, which is not proportionate and necessary should be banned, regardless of the mode of such surveillance (live or retrospective)**
- **There should also be an explicit ban on non-transparent personal data processing practices. It is necessary for laws and policies to ensure transparency regarding automatic personal data processing and the data subjects must be informed about the logic and consequences of such processing.**

The latest version of the AI Act regulates the use of facial recognition technology via regulation of the "real-time" remote biometric identification system and post-remote biometric identification system. In principle, the former falls in the "ban" category from Article 5 of the AI Act, subject to very detailed and narrow exceptions regulated therein. As for the latter, it must be based authorisation from a judicial authority for the use of the system and must be performed in compliance with other AI Act requirements.

The rules from the AI Act, once enacted, should be interpreted narrowly, and should in themselves serve as a red line when it comes to any use of technology that has a potential for live biometric surveillance. When considering the regulation of retroactive surveillance, governments should take into account all the risks that come from the capabilities of such surveillance in real life. It would not be acceptable for decision-makers to try to downplay its intrusiveness based on the formal criteria that data processing in that scenario happens after a period of time.

The regulation should in any case follow the highest requirements already established in the area of personal data protection, but also human rights standards. For these rules to be effective, the requirement of transparency cannot be overemphasised.

Although insight from private companies and their expertise on the technological side of things is valuable, industry self-regulation has proven not to be an appropriate or robust approach to preventing the harms and rights violations stemming from the misuse of biometric data, particularly surveillance use cases. Therefore, even though the state can encourage self-regulation in some aspects of surveillance technology, it cannot be left to private entities to set the parameters by which biometric systems can be used, especially given their impact on democracy and fundamental rights.

IMPLEMENTATION

Implementation of biometric surveillance laws depends a lot on the clarity of the law itself. Law is clear not only when it contains clear substantive provisions regulating the field of biometric surveillance, but also the provisions essential for its implementation - who is carrying out the oversight, accountability measures, sanctions and mechanisms for preventing misuse.

State oversight

Recommendation: States should oversee the application of biometric laws and policies.

Oversight of application of biometric laws and policies by the states is a twofold process. Firstly, states should provide a strong and independent judicial mechanism for performing judicial review of the application of biometric surveillance. Secondly, states should have supervisory bodies within their governments, which would facilitate the process of compliance and inspection of private companies using or producing biometric surveillance systems. Compliance procedures should be a mandatory requirement of the biometric surveillance laws.

Independent authorities

Recommendation: The use of biometric surveillance requires establishing independent oversight authorities, whose competence would be to monitor the implementation of biometric surveillance laws, to point out abuses and to provide complaint mechanisms in cases of breaches of individual rights.

One way to mitigate risks of human rights abuses when it comes to the use of biometric surveillance is to establish independent oversight authorities. DPAs as required under the GDPR, could assume duties concerning oversight of biometric surveillance. However, there are already cases of national legislation envisaging the institution of even more specialized

bodies. Such is an example of the United Kingdom, where the Biometrics Commissioner, with the main task of reviewing the retention and use of DNA samples, and the Surveillance Camera Commissioner in England and Wales, overseeing compliance with the Surveillance Camera Code of Practice were instituted, after the judgment in the ECtHR case of *S. and Marper v. the United Kingdom*.

In addition, the AI Act regulates the competencies of several institutions or bodies that will have a role in AI Act implementation. The European AI Office, which is established within the European Commission, has the main role in the harmonious application of the AI Act across the EU, but also has the power to make investigations about AI Act violations and issue fines. To perform its task, the European AI Office will work together with the European Artificial Intelligence Board (AI Board). AI Board is composed of representatives from each EU member state and its main activity of the Board is to advise and assist the Commission and the member states in order to facilitate the consistent and effective application of the AI Act. There are also a number of bodies at the national member state level with specific competencies.

For efficient enforcement of any legal rules that regulate any of these AI systems, including those that are used for biometric surveillance, the competent bodies must be granted enough resources, when it comes to the expertise they need, the number of staff or the financial means to fulfil the task granted to them according to applicable legislation.

Civil oversight

Recommendation: It is necessary for governments to allow opportunities for civil society and the general public to gain insight into the application of biometric surveillance laws and policies.

Transparency of biometric surveillance legislative implementation and use of biometric surveillance could be achieved in multiple ways:

- By imposing a duty on the government or independent oversight authorities to gather statistics and data on the use of biometric surveillance and publish them in the form of reports;

- By imposing a duty on all state and private bodies deploying biometric surveillance technologies to publish regular reports on the use of biometric surveillance, including statistics and case studies;
- By allowing a simple data access procedure to civil society organizations and the general public through which they can obtain data on the specific use of biometric surveillance by the state or private companies;
- By providing judicial review procedures in case that the state/ private companies deny access to data;
- By imposing a duty on the state and private companies to inform the public, in the form of reports, on the state of databases storing biometric data.

Education and capacity building

Recommendation: Authorities applying the law, private companies using or producing biometric surveillance systems and the general public should be educated on the complexities of biometric surveillance continuously.

As we have seen, biometric surveillance is a complex system. To properly understand biometric surveillance laws, one needs to have technical knowledge, an understanding of human rights, an understanding of the division of competencies in the state and an understanding of oversight and compliance procedures. For these reasons, successful implementation will heavily rely on the education of all actors that the law refers to. Authorities and judges need to gain a good insight into the technical capabilities of the biometric surveillance systems, whereas private companies need to be aware of their ethical components and human rights concerns. Software engineers in charge of operating and maintaining biometric surveillance systems need to be aware of human rights concerns surrounding these systems. All the actors need to understand the interplay between the technical and ethical components.

In addition, the law is only accessible to everyone once the general public is properly introduced to it, i.e. they need not only to know where to find the

text of the law but what the provisions mean, how their rights are restricted and which mechanisms they can use to protect themselves. In this process, the role of human rights organizations is essential. Expert human rights organizations should provide their knowledge to society and also offer their expertise, if possible, to states in the process of creating and implementing legislation concerning the use of biometrics. In addition, civil society would benefit from their own capacity building in this topic, by getting proper training on biometric surveillance systems and legislation, in order to be more competent to participate in the legislative process and overlook the implementation.

Benefit assessment

Recommendation: Biometric surveillance laws should be periodically assessed, in order to establish whether their application is still justified.

As we have seen, biometric surveillance legislation should be preceded by the DPIA and other risk assessments. Based on these risk assessments, drafting groups will decide which measures of biometric surveillance are necessary and justified. However, once the law enters into force and its application begins, it might turn out that certain measures are excessive, ineffective or that the factual situation changed in the meantime. An example could be if the biometric surveillance measures were introduced due to parameters which were from the very start inadequate and disproportionate, which the application of the law only confirmed (introduction of biometric surveillance in public squares to improve the level of safety on streets, only to be proven once the law enters into force that such an intrusive technique is not leading to that goal). For these reasons, biometric surveillance laws should be periodically assessed, in order to analyze their benefits and drawbacks and see whether there is a possibility for amendments. Amendments should be made whenever the need for biometric surveillance is no longer justified.

Accountability and sanctions

Recommendation: Authorities and private companies deploying biometric surveillance systems should be liable for their misuse of technology and be sanctioned by monetary penalties.

As mentioned above, company Clearview AI has already been fined several times after litigation proceedings for not complying with the GDPR regulations in several EU countries. In Brazil, company ViaQuatro S.A was fined by the Brazilian consumer protection authority, for collecting facial recognition data at subway stations without the consent of users and prohibited from further use of such technology. Certain legislations, like the State of Virginia and Canada, even introduced possibilities of criminal sanctions for misuse of biometric systems.

National DPAs in the EU countries, while deciding on a particular case, also have the power to impose fines of up to 4% of a company's global turnover. The first of such measures was issued in Sweden, when a DPA fined one Swedish municipality with 200,000 SEK (approximately 20,000 euros) for unlawfully using facial recognition technology to monitor the attendance of students in school.

As we can see, penalties could be imposed either by the state courts as a result of criminal or administrative proceedings or by the DPAs. Penalties imposed by the court could be enforced in the enforcement proceedings in case the penalized subject fails to pay voluntarily. However, penalties issued by the DPAs are likely to be more effective, for several reasons: a) DPAs are dealing exclusively with issues of data breaches, so they understand the nature of the violation better than courts, which do not specialize in the issue of data protection; b) DPAs are, in general, authorized to issue higher penalties in administrative proceedings than courts in criminal/misdemeanour proceedings and c) penalties issued by DPAs carry a certain public condemnation with it so the penalized subjects usually comply with them voluntarily.

Security measures

Recommendation: States must implement policies which provide for security measures to ensure data integrity.

State authorities in charge of using biometric data, as well as companies handling biometric systems, have to put in place policies which would ensure the safety of data. Some jurisdictions already introduced guarantees for maintaining the safety and integrity of biometric data (such are the Commonwealth of Kentucky, and China). These standards should cover the following:

- State-of-the-art technical measures, with an aim of providing systemic technical solutions to ensure data integrity. Some of the examples of these measures are the following: protecting data with encryption, using antimalware products, implementation of firewalls/intrusion detection systems, multi-factor authentication for system access, keeping system access and activity logs, data anonymization or pseudonymization, regular backups of data, technical disabling to copy and export data from the system on external media (CDs, DVDs, USB flash drives, external hard drives), and others;
- Organizational measures, with an aim of ensuring that any data handling issues require a prompt and organized response by the state or private company, stemming from established protocols. Some examples of such measures are: incident response and disaster recovery procedures, regular risk assessments and risk management processes, specific privileges for different types of accounts (roles) based on organizational hierarchy, transparent division of roles among employees, onboarding and offboarding policy for employees having access to the system.

Point of failure

Recommendation: Policies should provide mechanisms aimed at remedying points of failure, i.e. deficiencies of biometric surveillance technology.

Biometric surveillance technology, as mentioned previously, still does not operate with the highest degree of accuracy and reliability. It is essential to prescribe mechanisms which would rectify or annul the consequence of technological wrongdoings or abuses.

Common points of failure spotted when it comes to biometric surveillance technology, include (but due to the ever-evolving nature of technology are not limited to):

- Unauthorized access to the system and data;
- Destruction, compromising, exfiltration and publication of data;
- Vulnerabilities in vendor-supplied equipment that can be exploited by various threat actors;
- Abuse of administrative privileges by employees with access to the system and data;
- Privilege escalation due to vulnerabilities or abuse of the system;
- Too many matches for one suspect due to system error;
- Malfunction of the system due to technical errors and/or improper maintenance.

Mechanisms which should be implemented to rectify these situations are various and should be carefully assessed to target specific problems. Some of them should go in the direction of the possibility of using other types of data, once biometric surveillance technology starts providing inaccurate results or shows a system error, or if there is a situation of abuse of technology. One of the examples would be the possibility of using alternative methods of identification. In addition, it is necessary to provide mechanisms for remedying false positive/false negative and otherwise inaccurate biometric identifications, such as the procedural guarantee in the criminal or civil proceedings of establishing facts based on multiple evidence, instead of relying only on biometric identification. Also, consistent application of the standard 'beyond reasonable doubt' is necessary when it comes to criminal proceedings in which biometric identification is used, which would minimize wrongful convictions. It is worth noting here that the role of DPAs would be essential in cases of unauthorized access or any sort of compromising or publication of data. Finally, as a last resort, policies should envisage the possibility of putting out of circulation biometric technology which has proven to operate with a high degree of error.