14

A Central-Eastern Europe Perspective on FRT Regulation

A Case Study of Lithuania

Eglė Kavoliūnaitė-Ragauskienė

14.1 INTRODUCTION

In Lithuania, rather than being determined by the intrinsic needs of society, legal regulation of face recognition technology (FRT) came merely as a part of the EU's general data protection framework. Prior to this, the rules governing facial image usage of private persons were regulated mainly by the Civil Code of the Republic of Lithuania,[1] which provides that if a photo (or a part thereof), portrait, or other image of a natural person is to be reproduced, sold, displayed, and printed, the person may be photographed only with their consent – but this is not required if these actions are related to the person's social activities, their official position, the requirement of law enforcement authorities or if the photograph is taken in a public place. However, a person's photo (or part of it) taken in these cases may not be displayed, reproduced, or sold if this would degrade the person's honour, dignity, or professional reputation.[2] In terms of the work of law enforcement institutions, as will be seen from the analysis presented in this chapter, the laws regulating the work of separate law enforcement institutions or laws regulating specific activities of law enforcement (as a general rule) provide that the law enforcement institutions may collect and process personal data, usually without specifying the regime applicable to the collection and processing of biometric data.

As in all of the EU member states, law enforcement institutions in Lithuania have to adhere to EU standards of FRT usage, especially those laid down in the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (the Law Enforcement

[1] Civil Code of the Republic of Lithuania (Identification code 1001010ISTAIII-1864).

[2] Art. 2.22 of the Civil Code of the Republic of Lithuania.

https://doi.org/10.1017/9781009321211.017 Published online by Cambridge University Press

Directive).[3] However, each country also has local national standards that transpose other requirements to the FRT framework and its practical use.

From the perspective of the effectiveness of legal regulation, it should be noted that a country might have a very definite and clear legal rule or a set of rules regulating a particular field of social relations; however, this regulation may rendered as declarative and not implemented in practice. In Lithuania there are some examples of such, and one of the most prominent involves the legal regulation of lobbying activities. At the time of consideration of the Law on Lobbying Activities in the Parliament of Lithuania, one of the Members of Parliament noted that the relations that were going to be regulated were little known in Lithuanian society, so the law was not expected to be accepted in practice. He also said during the parliamentary session that it looked as if the law was aiming to 'prepare cosmonaut suits and then see if there would be cosmonauts willing to try them on'.[4] Indeed, this law (adopted in 2000) was one of the worst examples of legislation in Lithuania, as lobbying activities were practised despite what was stated in it until 2018 – when the law was amended significantly, this time following broad discussions with stakeholders and society. This and similar examples imply that in order for legislation to be applied in practice, it needs to fit both the legal culture and legal system of a country as well as fall in line with the views of wider society.

Keeping this in mind and recognising that society has an important role in controlling the implementation of legal acts, especially where they relate to human rights, the proper implementation of FRT regulations also relies on society and related interest groups deeming them necessary, otherwise they may remain declarative and void. If public awareness and pressure to have a law implemented properly are high, the implementing institutions are forced to take action. Usually, strong players in the performance of social control are non-governmental organisations (NGOs), especially where regulations or their improper implementation pose a threat to human rights. Therefore, it is of major importance that society and NGOs accept and understand the need and the usage of FRT in law enforcement institutions.

This section analyses the regulation of FRT usage by Lithuanian law enforcement institutions, as well as the public discussion relating to FRT usage in the media, NGO involvement, and other types of social control. Finally, the chapter considers what changes may be brought to national regulation of FRT by the EU Artificial Intelligence Act.

[3] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. [2016] OJ L 119, pp. 89–131.

[4] Alvidas Lukošaitis, 'Lobizmas užsienio šalyse ir Lietuvoje: teisinio reguliavimo ir institucionalizacijos problemos' 2(62) *Politologija* 3–42, at 34.

https://doi.org/10.1017/9781009321211.017 Published online by Cambridge University Press

14.2 LEGAL FRAMEWORK FOR THE USE OF FRT IN LAW ENFORCEMENT IN LITHUANIA

In general, the basis for the use of biometric data (including facial recognition data) in Lithuania is the Law Enforcement Directive,[5] which was transposed into the Law of the Republic of Lithuania on the Legal Protection of Personal Data Processed for the Prevention, Investigation, Disclosure or Prosecution of Criminal Offences, Execution of Sanctions or National Security or Defence and other legal acts.[6] Biometric data are classified as a special category of personal data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; they include genetic data and data concerning health or a person's sex life or sexual orientation. Processing of these personal data categories is only allowed when strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only where it is authorised by the EU or Lithuanian law – for example, when it is needed to protect the vital interests of the data subject or another person; or when such processing relates to data that are manifestly made public by people themselves.[7]

In Lithuania the collection and use of facial images on the one side, and processing of personal data such as biometric data, on the other, are regulated in law enforcement institutions by different laws and other legal acts. For example, the Law on Police of the Republic of Lithuania provides that with a person's consent and/or in cases established by law, police officers are entitled to take photos and make audio or video recordings. Without a person's consent, a police officer can take pictures of unidentified persons, persons in a helpless condition, unidentified corpses, risk group persons, and temporarily detained persons; they can be measured and their external features described, audio or video recordings can be made, fingerprints can be taken, samples can be taken for genetic testing to perform typification or for comparative research and identification, and all these data can be processed.[8] The law also states that the police can process personal data necessary for the implementation of police tasks, including the personal code, without the consent of the data subject, and that when processing data, the police have the right to collect them using technical means.[9]

The Penal Code provides that the Probation Service may receive data, documents, and other information necessary for the execution of public service sentences (or to get acquainted with this information) from the state, municipalities,

[5] Directive (EU) 2016/680, pp. 89–131.

[6] Law of the Republic of Lithuania on the Legal Protection of Personal Data Processed for the Prevention, Investigation, Disclosure or Prosecution of Criminal Offenses, Execution of Sanctions or National Security or Defence (Identification code 1111010ISTA0XI-1336).

[7] Law of the Republic of Lithuania on the Legal Protection of Personal Data, Art. 8.

[8] Law on Police of the Republic of Lithuania (Identification code 1001010ISTAIII-2048), Art. 22(1).

[9] Law on Police of the Republic of Lithuania, Art. 9(1) and (2).

and other institutions, bodies, or organisations with state information resources. The Probation Service is also entitled to process the personal data of convicted persons.[10]

In criminal procedure there is a general requirement that the use of technical means and their results are also subject to the requirements of public information, personal data protection, the right to inviolability of private life, and the protection of personal honour and dignity established in other laws.[11] This means that all steps in criminal procedure involving the use of biometric data should be in line with the previously mentioned provisions of the Law of the Republic of Lithuania on the Legal Protection of Personal Data Processed for the Prevention, Investigation, Disclosure or Prosecution of Criminal Offenses, Execution of Sanctions or National Security or Defence. It is therefore quite natural that, for example, the Law on Prosecution of the Republic of Lithuania,[12] or the Law on Financial Crime Investigation Service,[13] do not mention handling of any type of personal data at all.

However, a number of laws regulating the activities of law enforcement institutions do not provide clear wording on the possibility of collecting and using facial images. For example, the Law on Intelligence of the Republic of Lithuania provides only that state intelligence institutions have a right to process personal data, without clarifying what kinds of data these might be, and the provision for the performance of particular activities after having received a court permit only mentions 'access to a person's home, other premises or vehicles, their inspection and recording',[14] without a clear reference to collection or use of facial images. Similarly, the Law on Criminal Intelligence does not provide clear grounds for collecting and using facial images; it does not speak about handling personal data at all. This law only mentions that criminal intelligence activities (meaning the activities of criminal intelligence officers in collecting, recording, evaluating, and using available information about criminal intelligence objects) must be carried out in accordance with the procedure established by the law, and that methods of collecting criminal intelligence information are agency activity, survey, inspection, control inspection; controlled transportation; imitation of a criminal act; ambush; tracking; covert operation; and tasks of law enforcement authorities. However, this law also mentions that human rights and freedoms cannot be violated during criminal intelligence activities. Individual limitations of these rights and freedoms are temporary and can only be applied in accordance with the procedure established by law, in order to protect the rights and freedoms of another person, property, or

[10] Penal Code of the Republic of Lithuania (Identification code 1021010ISTA00IX-994), Art. 43(1).

[11] Code of Criminal Procedure of the Republic of Lithuania (Identification code 1021010ISTA00IX-785), Art. 260(4).

[12] Law on the Prosecution of the Republic of Lithuania (Identification code 0941010ISTA000I-599).

[13] Law on Financial Crime Investigation Service of the Republic of Lithuania (Identification code 1021010ISTA00IX-816).

[14] Law on Intelligence of the Republic of Lithuania (Identification code 1001010ISTAIII-1861), Art. 9(2) and Art. 13(1).

https://doi.org/10.1017/9781009321211.017 Published online by Cambridge University Press

public and state security.[15] The Code of Administrative Offences also generally states that investigative activities may include photography, video recording, audio and video recording, footprints and casts, plans and diagrams, and other recording techniques.

Regarding the activities of the Special Investigation Service, the handling of personal data is indirectly mentioned in the law that regulates the institution's analytical intelligence activities. It is stated that analytical anti-corruption intelligence means analytical activity carried out by the Special Investigation Service, which includes the collection, processing, comparison of information on corruption and related phenomena with other public or classified information available to the Service, obtaining qualitatively new data that is the result of these information processing processes, and use by and provision to state or municipal institutions and officials authorised to make significant decisions in terms of reducing the prevalence of corruption. The possibility of using available biometric data is provided, as in order to achieve its operational goal and implement the tasks assigned to it, the Special Investigation Service has the right to receive relevant documents from all public institutions.[16] Additional rules are applied in respect of the collection and usage of facial images and the usage of biometric data in the process of issuing identity documents and migration.[17]

Thus, it can be stated that the legal rules on the collection and usage of facial images and generating/usage of biometric data in Lithuania are rather fragmented and vague. As may be seen, in most cases it is stated that law enforcement institutions may collect and process personal data needed for the fulfilment of their duties without specifying any additional restrictions or criteria. Based on the personal nature of biometric data and the rigorous collection and processing of facial images, in accordance with the laws provided here, it is possible that every person may be affected: not only those who are subject to the issuance of personal identity documents or involved in migration issues, or those in any way involved in criminal proceedings or other proceedings that relate to national security and state interests, but also any other persons who act or appear in public places.

The second important issue is that the legal acts implementing the provisions of laws stray even further from the requirements applied to data collection and

[15] Law on Criminal Intelligence of the Republic of Lithuania (Identification code 1121010ISTA0XI-2234), Art. 2(7) and 8) and Art. 5(1).

[16] Law on Special Investigation Service of the Republic of Lithuania (Identification code 1001010ISTAIII-1649), Art. 8(1) and (9).

[17] Law on Identity Card and Passport of the Republic of Lithuania (Identification code 2014-21281); Law on the Legal Status of Foreigners of the Republic of Lithuania (Identification code 1041010ISTA0IX-2206), Law on Service Passport of the Republic of Lithuania (Identification code 1001010ISTAIII-1527), Order of the Minister of the Interior of the Republic of Lithuania on the Approval of Rules on Issuing Driving Licences for Motor Vehicles (Identification code 1082310ISAK001V-328), Order of the Minister of the Interior of the Republic of Lithuania on the Approval of Requirements for Personal Document Photos (Identification code 1022310ISAK00000569), etc.

https://doi.org/10.1017/9781009321211.017 Published online by Cambridge University Press

processing. For example, based on the provision of the Law on Police (the police have the right to collect and process personal data necessary for the implementation of their tasks without the consent of the data subject), all municipalities in Lithuania have adopted separate rules on the use of video surveillance cameras and the data they record.[18] Video surveillance may be established with the aim 'to identify persons who may have committed administrative offences and criminal acts'. Consequently, this means that cameras can be established in any public place and may collect video data on all persons appearing there.

Still, a nonetheless important issue is the processing of the video surveillance data and other facial images. According to the aforementioned and related legal acts, facial images can be stored in a number of databases (which are usually interlinked): the Police Information System and other police department registers and information systems, the Criminal Intelligence Information System; databases of detention facilities (prisons, probation offices, etc.); court and other authorities' databases; databases of institutions issuing identity documents; databases of the Migration Department and the State Border Guard Service; databases of the state enterprise Regitra, which issues driving licences; databases of institutions issuing personal documents; and municipal databases.[19]

In this context it is important that according to the law, as well as to the Law Enforcement Directive and the General Data Protection Regulation (GDPR),[20] 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a person, which allow or confirm the unique identification of that person. The definition of biometric data in GDPR (as well as in the Law Enforcement Directive) has generally been restricted to mean a technically defined digital representation of bodily traits that has been processed for machine or algorithmic analysis. This is suggested by the wording that data have to be subject to 'specific technical processing'. Speaking more broadly, data processing systems do not need all of the data, but instead rely on extracting meaningful sub-parts from voice or image data, which can then be easily compared to existing 'templates' in a database. This implies that photographs and

[18] For example, see Order of Biržai District Municipal Council. On the approval of the description of the procedure for handling video surveillance cameras installed in the territory of the municipality of Biržai district and their fixed video data (Identification code 2022-05136); Order of Tauragė District Municipal Council. On the approval of the description of the procedure for the use of video surveillance cameras installed in public spaces of the Tauragė district municipality and their fixed data (Identification code 2022-07557), Order of Kaišiadorys District Municipal Council. Regarding the approval of the description of the procedure for the use of video surveillance cameras and their fixed data installed in the territory of the municipality of Kaišiadorys district (Identification code 2022-13200).

[19] For more information, see TELEFI Project, 'Towards the European level exchange of facial images' (7 February 2020), Legal analysis for TELEFI project, www.telefi-project.eu/sites/default/files/TELEFI_LegalAnalysis.pdf

[20] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016) OJ L 119.

https://doi.org/10.1017/9781009321211.017 Published online by Cambridge University Press

video images of faces are expressly excluded from the definition of biometric data both in GDPR and the Law Enforcement Directive.[21] Therefore, there is a difference between the regulatory rules applied in respect of data images (which may be regarded as personal data) and images processed with FRT technology (which then is regarded as biometric data).

To summarise, in Lithuania there is quite a significant gap between the regulatory rules that set requirements for FRT from a data protection perspective and rules regulating activities of separate law enforcement institutions and law enforcement activities. Although the standards of data protection in general seem to be sufficient, the specific laws on law enforcement institutions solely provide the possibility to collect and process personal data, including facial images, without making it known whether FRT will be used to process such images or not. Therefore, there is a possibility that the general data protection rules are only declarative and not enforced in practice. Thus, in order to understand whether the legal regulation of FRT usage in Lithuanian law enforcement is sufficient, a deeper analysis of the practical implementation of regulatory rules on the usage of FRT in Lithuania is needed.

14.3 FRT USAGE IN PRACTICE

According to the respondents to the Government Use of Facial Recognition Technologies: Legal Challenges and Solutions project,[22] the volume of FRT usage in law enforcement institutions is not clear. In the course of this project the team sought to interview representatives from the institutions that are responsible for (or directly participate in) the processing of personal data, including facial images and biometric data. However, only very few representatives were willing to participate, whereas others stated they had insufficient knowledge of or competence in these issues. Moreover, according to a couple of respondents from the private sector, who were trying to investigate the use of FRT in the context of human rights, the representatives of law enforcement institutions disclosed to them that they felt comfortable as they benefited from having considerable latitude for when and how to use FRT as a result of the vague legal background.

As an example of insufficient regulatory basis for handling biometric data, including facial data processed using FRT, the case of the Register of Habitoscopic Data of the Republic of Lithuania may be analysed. This is a component of the Internal Affairs Information System – a general system for storing detailed personal identification data in a single database, which stores data on convicted persons, persons who have served a sentence of arrest or fixed-term imprisonment in the Republic of

[21] Amba Kak, 'Regulating biometrics: Global approaches and urgent questions' (1 September 2020), AI Now Institute, https://ainowinstitute.org/publication/regulating-biometrics-global-approaches-and-open-questions, p. 20.

[22] Government use of facial recognition technologies: Legal challenges and solutions (Face-AI). Project funded by the Research Council of Lithuania, contract No. S-MIP-21–38.

https://doi.org/10.1017/9781009321211.017 Published online by Cambridge University Press

Lithuania, temporarily detained persons suspected of having committed a criminal act, wanted persons, identification marks of unidentified dead bodies or unknown helpless persons, and other categories. This data is used by pre-trial investigation institutions, border protection, customs, the prosecutor's office and other law enforcement institutions in order to ensure the prevention of criminal acts and the fight against crime. It processes personal data for the following purposes: (1) to investigate criminal acts and ensure their prevention, organise, and carry out the search for persons, as well as to identify both unidentified corpses and unknown helpless persons according to personal identification marks; and (2) to determine the identity of a person in order to ensure the control of the movement of foreigners who have been detained by the competent control authorities for illegally crossing the state border by sea, land, or air from a third country and who have not been returned to that country.[23] The Register of Habitoscopic Data contains data on the external characteristics of a person, obtained by photographing, measuring, and describing the person's appearance. According to this definition and the list of processed data presented in the same Order, the Register of Habitoscopic Data processes personal data that does not fall under the definition of biometric personal data, meaning no additional rules on the processing of biometric data should apply. The Order does not mention or otherwise provide grounds for processing of FRT-related biometric data. However, there was a public announcement in the media about the reorganisation and improvement of the Register of Habitoscopic Data through the 'Modernisation of Register of Habitoscopic Data using advanced technologies of face recognition and identification tag search' project.[24] The project description states:

> [I]n the course of project activities, the Personal Face Biometric Recognition subsystem of the Register of Habitoscopic Data was modernized; using advanced facial biometric recognition technologies, the accuracy, performance, and reliability of personal facial biometric recognition was improved. Facial biometric recognition functions of the Register of Habitoscopic Data were modernised using high- facial biometric recognition software (NeoFace Watch, manufactured by NEC Corporation), which enables software users to perform facial biometric recognition (1:1; 1:N) in indirect mode, using digital facial photographs, and face-to-face biometric recognition (N:N) in live mode using real-time IP video cameras. Purchased facial biometric recognition software also includes a specially designed

[23] Order of Minister of the Interior of the Republic of Lithuania: On the reorganisation of the departmental register of identification marks of persons who have served a sentence of arrest or fixed-term imprisonment into a Register of Habitoscopic data (Identification code 1132310ISAK001V-440), para. 4.

[24] 'As part of the project funded by the Internal Security Fund, the Habitoscopic Data Register was modernised to introduce advanced biometric recognition technologies for a person's face.' IRD, 'Įgyvendinant Vidaus saugumo fondo lėšomis finansuojamą projektą modernizuotas Habitoskopinių duomenų registras – įdiegtos pažangios asmens veido biometrinio atpažinimo technologijos' (5 April 2020), https://ird.lt/lt/naujienos/igyvendinant-vidaus-saugumo-fondo-lesomis-finansuojama-projekta-modernizuotas-habitoskopiniu-duomenu-registras-idiegtos-pazangios-asmens-veido-biometrinio-atpazinimo-technologijos.

https://doi.org/10.1017/9781009321211.017 Published online by Cambridge University Press

> software component for smart devices. The 'Face Recognition' application of a smart device provides an opportunity for mobile face recognition of a person, that is, taking a picture of a person with a phone and performing a search (recognition) of the face image of such a person based on the captured face image data in the database of the Register of Habitoscopic Data.[25]

The Police Department website provides information about a related project. It is stated that:

> [This aims to] create a uniform system for collecting personal identification marks and biometric data and submitting them to the Register of Habitoscopic Data of the Ministry of the Interior of the Republic of Lithuania. After the implementation of the project, sixteen specialised workstations for collecting personal identification marks and biometric data and submitting them to the Register of Habitoscopic Data were established in the main police commissariats and detention centres of the country's counties. It became possible to capture images of unidentified persons, take biometric data, as well as other data of an event related to a person, process them in police custody and detention facilities, register them, and transfer them to be recorded in the Register of Habitoscopic Data. After arresting a person suspected of having committed a crime, it is possible to promptly compare the person's biometric data with the data contained in the HDR – in this way, this data will be used to reveal criminal acts faster, determine the identity of the person, conduct investigations more efficiently, conduct forensic investigations faster, and, with better quality, ensure crime prevention, public order, and public safety.[26]

However, as mentioned earlier, there is no legal ground for processing biometric personal data in the Register of Habitoscopic Data, nor are there security measures to be applied in order to ensure the protection of biometric personal data based on the criteria established in the Law Enforcement Directive and the Law of the Republic of Lithuania on the Legal Protection of Personal Data Processed for the Prevention, Investigation, Disclosure or Prosecution of Criminal Offenses, Execution of Sanctions or National Security or Defence. Furthermore, there are no terms for storage of biometric data (data processed by facial recognition technologies that allows identification of a specific person) in the Register of Habitoscopic Data.

Moreover, the Order of the Minister of the Interior establishing the Register of Habitoscopic Data allows the linking of the Register of Habitoscopic Data with other state registers (Residents' Register, Addresses' Register, Register of Application

[25] IRD, 'Įgyvendinant Vidaus saugumo fondo lėšomis finansuojamą projektą modernizuotas Habitoskopinių duomenų registras – įdiegtos pažangios asmens veido biometrinio atpažinimo technologijos' (4 May 2020), https://ird.lt/lt/naujienos/igyvendinant-vidaus-saugumo-fondo-lesomis-finansuojama-projekta-modernizuotas-habitoskopiniu-duomenu-registras-idiegtos-pazangios-asmens-veido-biometrinio-atpazinimo-technologijos.

[26] Lietuvos policija, 'Sukurta vienoda asmens atpažinimo žymių ir biometrinių duomenų rinkimo Sistema' (13 August 2020), Lietuvos policija, https://policija.lrv.lt/lt/naujienos/sukurta-vienoda-asmens-atpazinimo-zymiu-ir-biometriniu-duomenu-rinkimo-sistema.

https://doi.org/10.1017/9781009321211.017 Published online by Cambridge University Press

of Preventive Measures, Official Register of Wanted Persons, Unidentified Corpses and Unknown Helpless Persons, Register of Suspected, Accused and Convicted Persons, Official Register of Criminal Acts, Register of Dactyloscopic Data, Register of DNA Data, Register of Foreigners, and Register of Events registered by the Police). However, in the description of the 'Modernisation of Register of Habitoscopic Data using advanced technologies of face recognition and identification tag search' project, it is stated that 'three new integration interfaces have been created: with the Integrated Criminal Procedure Information System (IBPS), the Register of Administrative Offences (ANR), and the Lithuanian National Second Generation Schengen Information System (N.SIS)'. In other words, the Register of Habitoscopic Data has interconnections with other registers that are not found in the relevant regulatory document.

The Ministry of the Interior of the Republic of Lithuania was officially asked to provide an explanation of the differences between the current regulatory framework for the operation of the Register of Habitoscopic Data and the declared updates to the register, which are said to have been already implemented.[27] However, no response was received.

Such a situation implies not only that the regulation of collection of facial images (which falls outside the scope of 'biometric data' definition) and the processing of such images to generate biometric data is not regulated properly, but also that the current practices (given no information is provided about any unpublished legal regulations – which is unlikely given the requirements of transparency in the field of human rights and data protection) are likely to be in breach of the existing legal basis for such activities. First, as already mentioned, the data and information, as regulated by the Order of the Minister of the Interior on the Register of Habitoscopic Data, would be limited only to facial images and their description, with digital processing using FRT not being mentioned. The use of FRT brings the activities of the

[27] On 14 June 2022, an official letter was sent from the Law Institute of the Lithuanian Centre for Social Sciences to the Ministry of the Interior kindly requesting to indicate the legal basis on which biometric personal data are processed in the Register of Habitoscopic Data and to indicate what security measures are applied in order to ensure the protection of biometric personal data based on the criteria established in the law; to specify the Register of Habitoscopic Data (including database archive) storage terms of biometric data (data processed by facial recognition technologies that allow identification of a specific person) and the legal basis for their regulation; to indicate whether there are integrations of the Register of Habitoscopic Data with other databases/registries (e.g., the register of events registered by the police or the traffic accident information system), to submit the legal act/s regulating Order/s No. 1V-440 linking of registers/databases not mentioned in the Order itself; to specify which data not mentioned in the Order are transferred between the Registers. Finally, it was asked to provide legal regulation (references to specific legal acts and their structural parts, and if these legal acts are not published publicly – to attach their copies), establishing restrictions on the processing of personal images obtained from other registers with FRTs and to describe how this is implemented in practice (e.g., if a person is suspected of having committed an administrative offence, will the image of the suspect from the available video/photo material be processed by facial recognition technology in all cases, and in which cases is this not done), and to indicate the specific legal regulation.

https://doi.org/10.1017/9781009321211.017 Published online by Cambridge University Press

Register to a different level of legal requirement – that is, the obligation to conform with the rules applicable to biometric data processing. Second, the interconnections between the Register of Habitoscopic Data and other registers are not clear. It appears that in practice there are links to more registers than provided in the relevant Order of the Minister of the Interior, however, it is not clear what data could be exchanged. It should also be noted that a special Order of the Commissioner General of the Police restricts the transfer of facial image data (received via public surveillance cameras) to state registers to situations when there is a need to verify or specify information on a particular criminal or administrative offence.[28] However, it is still plausible that all facial images of both recognised and unrecognised persons, who may be captured by video or photo cameras established for public surveillance by accident and without taking any part in an offence, could be automatically processed for facial biometric data.

14.4 PUBLIC ACCEPTANCE OF THE USAGE OF FRT BY GOVERNMENT AUTHORITIES IN LITHUANIA

To begin with, the issues surrounding FRT usage by Lithuanian government authorities are not commonly mentioned in media, NGOs, or social networks. Similarly, as with all advances in artificial intelligence (AI), FRT is welcomed positively as a facilitator of general life in Lithuania. For example, the Strategy of Artificial Intelligence in Lithuania encourages integrating AI, including FRT, into all economic sectors. Specifically, regarding the public sector, it is stated that AI will be helpful in the field of crime control, optimising the daily work of public institutions and improving the provision of public services.[29] In particular, the optimisation of work is a rather attractive promise for most institutions – for example, the Kaunas Information Technology School carried out the 'Attendance Marking Powered by Face Recognition' project, which revealed that teachers would save time significantly if attendance of students was checked by using FRT rather than manually.[30] Moreover, FRT was even suggested as a practical solution for simplifying the checking of persons who had been vaccinated against COVID-19, with proposals to use FRT instead of the official 'opportunities passport' system, which was declared to be

[28] Lietuvos Policijos Generalinis Komisaras, 'Order of the Commissioner General of the Police Department under the Ministry of the Interior of the Republic of Lithuania on the approval of rules for processing data captured by video surveillance in police institutions' (19 February 2020), Paras 3 and 4. Lietuvos Policijos Generalinis Komisaras, https://policija.lrv.lt/uploads/policija/documents/files/Vaizdo%20stebejimo%20duomenu%20tvarkymo%20taisykles.pdf.

[29] Ministry of Economics and Innovation of the Republic of Lithuania, 'Strategy of artificial intelligence in Lithuania' (n.d.), https://eimin.lrv.lt/uploads/eimin/documents/files/DI_strategija_LT(1).pdf.

[30] Paulius Briedis, 'Attendance marking powered by Face Recognition' (2022) (KA2 Strategic partnerships project, Introducing artificial intelligence to vocational schools in Europe No. 2020-1-LT01-KA202-078015), https://docs.google.com/presentation/d/1L6Gj5yI8mgR-V3g83OicVEbydoIYJ5_KmKsVsvX3wKM/edit?fbclid=IwAR0M7z5PuhnE2qNz1K42p61tPquS4O8dHK-ievqNY7FRHbjoFNleFW8b6po#slide=id.g12cc187cc22_2_842.

https://doi.org/10.1017/9781009321211.017 Published online by Cambridge University Press

'outdated'.[31] In Lithuania the case law on application of FRT is a rarity. However, a recent court decision directly relating to FRT usage demonstrates how the argument about convenience may easily transform into an argument about public interest. The State Data Protection Inspection challenged an order made by a university regarding the procedure for students' remote examinations and measures related to the processing of personal data in order to ensure fair behaviour during examinations. This document established that the following personal data will also be processed during the state-level emergency brought about by COVID-19: surveillance photos, facial biometric data, audio recording of the exam. In this case the court declared that the rules of the university were legitimate as they were necessitated by public interest.[32]

Quite a strong argument with the public in favour of FRT use is the possibility of increasing public safety. Municipal institutions boast that they have introduced surveillance cameras that increase the safety of citizens. For example, the Mayor of Marijampolė municipality publicly announced that the network of sixty-four video surveillance cameras installed in 2020 has raised security in the city to a new level:

> Let's start with the fact that stationary cameras were placed at all entrances to the city, monitoring the flow of cars and scanning their licence plates. It is extremely useful for investigating various crimes, such as thefts, robberies from homes or shops. At the same time, it also has a preventive effect, since thieves try to bypass the monitored cities – they don't want their vehicles or themselves to be captured.[33]

Or, for example, a local internet news portal of Mažeikiai district proudly presents:

> Almost half a dozen stationary and another fifteen mobile video surveillance cameras in Mažeikiai help to ensure the safety and order of residents in the city. With them, surveillance is performed in the busiest streets and intersections of the city, in public spaces, and near waste management container sites, and transmitted in real time to the monitoring console.[34]

It seems that residents are confident and satisfied with such usage of FRT in public places. People have even complained that the video cameras do not adequately ensure safety, as upon an accident the recording is too blurry or badly angled so that not all persons captured can be identified:

[31] Dovydas Vitkauskas, 'Galimybių pasą turėtų keisti veido atpažinimo Sistema' (7 October 2021), Delfi, www.delfi.lt/verslas/nuomones/dovydas-vitkauskas-galimybiu-pasa-turetu-keisti-veido-atpazinimo-sistema.d?id=88361491.

[32] LRT.lt, 'Teismas: Vilniaus universitetas galėjo naudoti veido atpažinimo funkciją per atsiskaitymus' (13 May 2022), www.lrt.lt/naujienos/mokslas-ir-it/11/1693760/teismas-vilniaus-universitetas-galejo-naudoti-veido-atpazinimo-funkcija-per-atsiskaitymus.

[33] Telia, 'Marijampolėje gyventojų saugumą užtikrina stiklinės akys: tokio poveikio nesitikėjo' (13 April 2022), Delfi.lt, www.delfi.lt/uzsakomasis-turinys/premium/marijampoleje-gyventoju-sauguma-uztikrina-stiklines-akys-tokio-poveikio-nesitikejo.d?id=89958475.

[34] Mažeikių rajono savivaldybė, 'Vaizdo stebėjimo kameros mieste – daugiau saugumo ir tvarkos' (14 January 2021), Budas.lt, www.budas.lt/regionu-naujienos/naujienos-mazeikiuose/41960-vaizdo-stebejimo-kameros-mieste-daugiau-saugumo-ir-tvarkos.

https://doi.org/10.1017/9781009321211.017 Published online by Cambridge University Press

> It is declared that Vilnius is safe, we see advertisements, billboards, how many cameras are attached. Oh, it turns out that when there is an incident in the middle of the day, not at night, not in a corner, not somewhere behind the trees, when we start to investigate, it turns out that those cameras are of very poor quality, hung up high. Here, perhaps, is the question I would like to raise – why do we need cameras, if, as declared, safe Vilnius is not safe at all in Cathedral Square?[35]

Moreover, FRT in public places is used not only for safety reasons, but also for fun: in Vilnius there was a two-year experiment in which researchers' devices measured the face temperature, breathing rate, heartbeat, and emotions of any passers-by. The explanation was that this experiment was intended to substitute for a public poll on how people feel at a given moment in a given place, as it was a much more precise way to do so.[36]

On the other side, certain aspects of FRT usage have also been criticised in the media. For example, it has been widely and critically discussed that Lithuanian institutions are using video surveillance cameras made in China, which raises doubts as regards the safety of the data recorded and potentially threatens state security.[37] Moreover, the potential for the misappropriation of FRT footage was revealed to the public in a well-known case concerning a policeman who had published online a video that had been recorded in a police car in which a drunk women took off her clothes.[38]

Nonetheless, these examples of the usage of FRT being publicly criticised are rather rare, and public attention is paid only to cases that raise state security issues or where there is a manifest infringement of professional duties. The overall attitude of Lithuanian society towards FRT usage seems to be positive – at least this is what can

[35] Živilė Kairytė, '16-metį vilnietės sūnų užpuolė Katedros aikštėje: skubiai prašo pagalbos' (30 August 2022), TV3.lt, www.tv3.lt/naujiena/gyvenimas/16-meti-vilnietes-sunu-uzpuole-katedros-aiksteje-skubiai-praso-pagalbos-n1185568.

[36] Made in Vilnius, 'Mokslininkai Vilniaus gatvėse matuoja praeivių emocijas, temperatūrą bei kvėpavimo dažnį' (24 December 2019), Delfi.lt, www.delfi.lt/miestai/vilnius/mokslininkai-vilniaus-gatvese-matuoja-praeiviu-emocijas-temperatura-bei-kvepavimo-dazni.d?id=83040699.

[37] Paulius Vaitekėnas, 'Kaune gyventojus stebi žmonių sekimu pagarsėjusios kinų kameros: fiksuos žmonių veidus ir KET pažeidimus' (29 January 2020), LRT.lt, www.lrt.lt/naujienos/eismas/7/1137677/kaune-gyventojus-stebi-zmoniu-sekimu-pagarsejusios-kinu-kameros-fiksuos-zmoniu-veidus-ir-ket-pazeidimus?fbclid=IwAR1VKjHQEWAWLV03d5IJJpvYCv09ZLlgovZtkGpfAJPiaLvFIgMxA23HFM0; Ignas Jačauskas, 'NKSC: kiniškos vaizdo stebėjimo kameros turi saugumo spragų' (29 May 2020), Diena.lt, www.diena.lt/naujienos/lietuva/salies-pulsas/nksc-kiniskos-vaizdo-stebejimo-kameros-turi-saugumo-spragu-969413; LRT tyrimai, 'Lietuvos vadovus saugo kameros, kurių bijo amerikiečiai' (29 January 2020), LRT.lt, www.lrt.lt/naujienos/lrt-tyrimai/5/1137518/lrt-tyrimas-lietuvos-vadovus-saugokameros-kuriu-bijo-amerikieciai?fbclid=IwAR2Y9BLDthGBeGX4RrNa9vozrDww6E3myMXU0iJFwJELIPTbe8znM-mVaKY; Valdemaras Šukšta, '"Kiniška akis" Kaune: nors palaiminimo miesto gatvėse naudoti kameras dar negauta, policija tyliai jas jau išmėgina' (19 November 2021), LRT.lt, www.lrt.lt/naujienos/lietuvoje/2/1541495/kiniska-akis-kaune-nors-palaiminimo-miesto-gatvese-naudoti-kameras-dar-negauta-policija-tyliaijas-jau-ismegina.

[38] Andrius Vaitkevičius, 'Į viešumą pateko Vilniaus policininkų darytas vaizdo įrašas – skandalas neišvengiamas' (29 January 2020), Lrytas.lt, www.lrytas.lt/lietuvosdiena/kriminalai/2020/01/20/news/i-viesuma-pateko-vilniaus-policininku-darytas-vaizdo-irasas-skandalas-neisvengiamas-13326794.

be seen from media sources. It seems that priority is given to the vast development of FRT and other AI technologies because the public can benefit from increased convenience and safety, while human rights issues related to threats to privacy, discrimination, or false accusation are left aside. Indeed, no civil society organisations in Lithuania prioritise threats posed by usage of FRT and AI. Therefore, it may be assumed that public discourse is driven by the position of state institutions and any developers' interests in this field – thus a critical standpoint is lacking.

14.5 WHAT IMPACT ON FRT USAGE BY LAW ENFORCEMENT INSTITUTIONS IS EXPECTED UPON THE APPLICATION OF THE EU ARTIFICIAL INTELLIGENCE ACT?

As has been noted, the fragmented regulatory basis and rather weak public control of FRT usage in Lithuania could lead to the uncontrolled usage of FRT in law enforcement. Hopefully, the application of the EU Artificial Intelligence Act may bring about some changes to this situation. In April 2021, the European Commission presented the draft Artificial Intelligence Act, which is intended to introduce high standards for an EU trustworthy AI paradigm. It sets out core horizontal rules for the development, trade, and use of AI-driven products, services, and systems across all industries within the territory of the EU. This proposal introduces a 'product safety regime' that is constructed around a set of four risk categories. It imposes requirements for market entrance and certification of high-risk AI systems through a mandatory CE-marking procedure. This pre-market conformity regime also applies to machine learning training, testing, and validation datasets. Thus, according to Mauritz Kop,[39] the draft AI Act combines a risk-based approach (based on the pyramid of criticality) with a modern, layered enforcement mechanism. This means that as risk increases, stricter rules apply.

Regarding the definition of 'biometric data' in the law enforcement area, the proposed AI Act makes a reference to the Law Enforcement Directive.[40] However, the draft Act provides separate definitions for 'remote biometric identification system', '"real-time" remote biometric identification system', '"post" remote biometric identification system', and so on., with a specific regime being applicable to these categories. For example, the draft Act states that it is prohibited to use the '"real-time" remote biometric identification systems' in publicly accessible spaces for the purpose of law enforcement, unless and in as far as such use is strictly necessary for one of the following objectives:

[39] Mauritz Kop, 'EU Artificial Intelligence Act: The European approach to AI' (2021) (2) *Transatlantic Antitrust and IPR Developments*, Stanford Law School, https://law.stanford.edu/publications/eu-artificial-intelligence-act-the-european-approach-to-ai.

[40] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (Com/2021/206 Final), Recital 7.

https://doi.org/10.1017/9781009321211.017 Published online by Cambridge University Press

(1) the targeted search for specific potential victims of crime, including missing children;
(2) the prevention of a specific, substantial, and imminent threat to the life or physical safety of individuals or of a terrorist attack;
(3) the detection, localisation, identification, or prosecution of a perpetrator or suspect of a criminal offence.[41]

As stated in the Explanatory Memorandum to the proposed Artificial Intelligence Act, the choice of a regulation as a legal instrument is justified by the need for a uniform application of the new rules, such as definition of AI, the prohibition of certain harmful AI-enabled practices and the classification of certain AI systems. The direct applicability of a Regulation, in accordance with Article 288 TFEU, should reduce legal fragmentation and facilitate the development of a single market for lawful, safe, and trustworthy AI systems. It is expected to introduce a set of harmonised core requirements regarding 'high-risk' AI systems and construct obligations for providers and users of those systems – improving the protection of fundamental rights and providing legal certainty for operators and consumers alike. At the same time, the provisions of the regulation must not be too prescriptive and should instead leave room for different levels of member state to take action regarding elements that do not undermine the objectives of the initiative, in particular the internal organisation of the market surveillance system and the uptake of measures to foster innovation.[42]

To summarise, the adopted Artificial Intelligence Act should bring more precision to the types of FRT used in law enforcement activities, and apply more controls to its use. However, the issue of transparency of FRT usage and making information available to the public or academics may still remain restricted as it is now, unless rising social pressures force such a practice to change.

14.6 CONCLUSIONS

There is quite a significant gap between the regulatory rules, which set requirements for FRT from a data protection perspective, and rules regulating the activities of separate law enforcement institutions and law enforcement activities. This may be because the usage of personal data, including facial images and their processing, was established in the specific laws regulating law enforcement much earlier than 2016, when the general data protection framework was established. Therefore, the Lithuanian legal framework clearly demonstrates that there are separate rules allowing the collection and processing of personal data (i.e., biometric data) in law enforcement activities, as well as separate rules that are more general and require

[41] Proposal for the Artificial Intelligence Act, Art. 5(1)(d).

[42] Explanatory Memorandum to the Proposal for the Artificial Intelligence Act (COM(2021) 206 final), para. 2.4.

https://doi.org/10.1017/9781009321211.017 Published online by Cambridge University Press

a specific protective regime to be applied for the collection and processing of personal, including biometric, data.

Notwithstanding the fact that in theory the standards of data protection in general seem to be sufficient to protect against the rapid progression of technologies processing personal (and biometric) data and the evident threats to privacy and other human rights they pose, it still seems that the specific requirements on processing of personal data, especially processing biometric data, are not yet fully included in the practices of law enforcement in Lithuania. Moreover, it may be seen that the practices used in the development and usage of the Register of Habitoscopic Data do not comply with the regulatory requirements, in particular with the rules regulating the establishment, structure, and use of habitoscopic data. Rules on processing and sharing biometric data contained in this Register are not sufficient to ensure its proper protection, as required in data protection laws and EU documents.

Regarding the public attitudes to the regulation and usage of FRT in law enforcement in Lithuania, it may be noticed that neither society nor NGOs working in the field of human rights show any particular interest in analysing or restricting the usage of FRT in law enforcement institutions. On the contrary, media sources indicate that society at large is satisfied with the fact that the number of surveillance cameras in public places is increasing, and feels that it is a good and acceptable development that the possibility particular persons in public spaces can be recognised is increasing, as this brings the feeling of safety and order.

Although the adopted EU Artificial Intelligence Act should bring some discipline and clarity to the national regulation of FRT systems as well, as the reasons for using FRT, there are still doubts as to whether the transparency of FRT usage will be increased if societal and organisational attention and interest regarding FRT remains at the same level.

https://doi.org/10.1017/9781009321211.017 Published online by Cambridge University Press