Ministry of Education and Science of Ukraine
National University of "Kyiv-Mohyla Academy"
Faculty of Law
Department of International and European Law

Master's Thesis

Master's Degree Program

"FACIAL RECOGNITION TECHNOLOGIES AND THEIR INFLUENCE ON HUMAN RIGHTS: INTERNATIONAL AND COMPARATIVE LAW ASPECTS"

Written by a second-year graduate student
Specialty 081 Law
Tetiana Avdieieva

Supervisor: Myroslava Antonovych
Doctor of Law, Associate Professor

Reviewer: _____

The Master's thesis grade: _____

Secretary: _____
"__" _____2022

Kyiv-2022

Міністерство освіти і науки України
Національний університет “Києво-Могилянська академія”
Факультет правничих наук
Кафедра міжнародного та європейського права

Магістерська робота
освітній ступінь – магістр

на тему: “**ТЕХНОЛОГІЇ РОЗПІЗНАВАННЯ ОБЛИЧ ТА ЇХ ВПЛИВ НА ПРАВА ЛЮДИНИ: МІЖНАРОДНІ ТА ПОРІВНЯЛЬНО-ПРАВОВІ АСПЕКТИ**”

Виконала: студентка 2-го року навчання,
Спеціальності 081 Право
Авдєєва Тетяна Сергіївна

Керівник Антонович М.М.,
Доктор права, доцент

Рецензент _____

Магістерська робота захищена з оцінкою
_____
Секретар ЕК_____
___ _____ 2022 р.

Київ-2022

Декларація академічної доброчесності

Я Авдєєва Тетяна Сергіївна, студентка 2 року навчання магістерської програми за спеціальністю «Право» факультету правничих наук НаУКМА підтверджую таке:

- написана мною кваліфікаційна робота на тему "*Facial recognition technologies and their influence on human rights: international and comparative law aspects*" відповідає вимогам академічної доброчесності та не містить порушень, передбачених п. 3.1. Положенням про академічну доброчесність здобувачів освіти у НаУКМА, зі змістом якого я ознайомлена;

- я заявляю, що надана мною для перевірки електронна версія роботи є ідентичною її друкованій версії.

13.06.2022		Авдєєва Т.С.
Дата	*Підпис*	*Прізвище, ініціали*

CONTENTS

LIST OF ABBREVIATIONS

ACHPR	African Charter on Human and People's Rights
AI	Artificial Intelligence
CIL	Customary international law
CJEU	Court of Justice of the European Union
CoE	Council of Europe
Convention 108+	Convention for the protection of individuals with regard to the processing of personal data
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
FRT	Facial recognition technologies
GDPR	General Data Protection Regulation
IAComHR	Inter-American Commission on Human Rights
IACtHR	Inter-American Court of Human Rights
ICCPR	International Covenant on Civil and Political Rights
IHRL	International human rights law
NGO	Non-governmental organisation
OECD	Organisation for Economic Co-operation and Development
OHCHR	Office of the UN High Commissioner for Human Rights
HR Council	UN Human Rights Council
HRC	UN Human Rights Committee

INTRODUCTION

Snowden's revelations of 2013 served as a turning point for conspiracy theories to become a new reality, raising a groundful concern regarding the bulk State interference with one's privacy. Interception of e-mails and phone communications, profiling of activists, recording of peaceful protests are the classic examples of State surveillance done under the auspices of national security and public order protection. Modern technologies made surveillance more sophisticated, all-encompassing, and intrusive. Biometric identification becomes easier given the incorporation of the FRT into the video cameras. They enable identification (comparing recorded individuals with a list of wanted persons), verification of identity (checking whether a particular individual is the one recorded), and categorisation (defining how many people of certain gender or ethnicity were recorded).[1] Such systems are often equipped with classificatory of facial expressions and emotions,[2] as well as AI algorithms detecting the obstructed or poorly lit targets. Accordingly, the FRT afford increased effectiveness, granting law enforcement additional powers in surveilling individuals.

Practical attitude to the FRT remains indefinite. Meta company refused to proceed with its application,[3] reasoning it by the excessive intrusiveness. Similarly, researchers under the UN Special Rapporteur Mandate outlined a growing concern of the FRT making it "*impossible for individuals to opt out of having their data captured*".[4] Yet, numerous States deploy such surveillance systems at the airports, on the border control, in the underground, overcrowded public spaces and even at school canteens, while pandemics triggered the development of the FRT tracking applications. Ukraine is not

[1] Tambiama Madiega and Hendrik Mildebrath, *Regulating facial recognition in the EU* (EPRS, 2021) 1-2.

[2] Joy Buolamwini and others, *Facial Recognition Technologies: A Primer* (Algorithmic Justice League, 2020) 2-6; European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement* (FRA, 2020) 7-8.

[3] Adi Robertson, 'Facebook is shutting down its Face Recognition tagging program' (*The Verge*, 2 November 2021) <https://cutt.ly/mJG47Jn> accessed 10 June 2022.

[4] Krisztina Huszti-Orbán and Fionnuala Ní Aoláin, *Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?* (Human Rights Center, University of Minnesota, 2020) 8.

an exception, actively implementing the "Safe City" program[5] and planning to extend the surveillance scale, making it more centralised and accessible to law enforcement.

Accordingly, the in-depth research into the nature, characteristics, and pitfalls of the State FRT surveillance for defence and security purposes is strictly necessary given the growing tendency toward its implementation by policymakers all around the globe. The recommendations based on this research may serve as guidance for all stakeholders to enhance the human rights protection within the State biometric surveillance. Hence, a **research issue** is whether the FRT are compatible with human rights from the international and comparative law perspectives?

Given the aforementioned, the legal relations emerging from the State installation of biometric surveillance constitute the **object** of this thesis**.** Simultaneously**,** the **subject matter** includes a legal framework regulating the FRT application and corresponding State responsibilities to respect and safeguard human rights.

Based on the identified object and subject, the **purpose** of the thesis implies outlining the applicable legal rules regulating the biometric surveillance applied by the State for the defence and security aims, and conducting the human rights compliance of current policies in the FRT. The accomplishment of this purpose requires framing the respective **objectives of the thesis**, which involve:

- Identifying applicable norms of the IHRL governing mass and targeted surveillance, analysing the compliance of the FRT with these requirements, as well as determining the current international regulations of this phenomenon;
- Investigating foreign practices of applying the FRT for the surveillance purposes, determining a legislative framework for such interference and conducting the human rights impact assessment of these technologies;
- Exploring the existing Ukrainian legal framework on the biometric surveillance and protection of personal data, determining Ukrainian practices of applying the FRT surveillance, and providing a set of recommendations on effective implementation of Ukrainian obligations under the IHRL.

[5] LB.ua, 'У Києві тестують програму розпізнавання облич за допомогою камер відеоспостереження' (*LB.ua*, 8 February 2019) <https://cutt.ly/mJ3jFTo> accessed 10 June 2022.

To achieve the declared objectives, the extensive list of both **general scientific** and **specific juridical methods** is to be applied. They include axiological and statistical methods, analysis and synthesis, comparative law and analogy methods, induction and deduction, formally legal and documentary analysis, legal modelling, which assist in revealing a causal link between the technical phenomena and their legal implications, enabling to make conclusions and draw hypothesises.

Lastly, regarding the novelty of this research, numerous scholars, including William Schabas, Joseph Cannataci, Ben Emmerson, Krisztina Huszti-Orbán, Joy Buolamwini, Mykhailo Kameniev and other prominent authors referred to in this thesis, have made a significant contribution to the development of the surveillance topic. At the same time, existent research briefly addresses the FRT application, paying critically little attention to the Ukrainian context. Thus, this thesis is designed to elaborate on the lacunas and provide the potential solution for existing inconsistencies.

CHAPTER 1
REGULATION OF SURVEILLANCE MEASURES AND THE FACIAL RECOGNITION TECHNOLOGIES UNDER THE INTERNATIONAL HUMAN RIGHTS LAW

1.1. General international human rights law rules governing mass and targeted surveillance measures

Bearing both negative and positive obligations, the States have the equipollent duty to refrain from excessive intrusion into the citizens' rights and to safeguard them against various threats. Rapid technological advancement made societies vulnerable not only to internal challenges but also to outer dangers. According to professor Schabas, the interference with one's rights depends on the individuals' expectations of privacy in a particular area, and the probability of being recorded or reported.[6] For example, permanent video monitoring with the possibility of tracking one's way or further processing of such data suffice for the privacy right to come into play. The same approach applies to metadata manifested in various pieces of information about the individual,[7] which under the CJEU's view attracts an equal protection compared to other personal data.[8]

The first solid discussions around the mass interception of communications emerged after Snowden revealed the UK-US exchange of personal data, secretly collected via the indiscriminate surveillance. This event caused an extensive societal reaction.[9] For example, the CoE Resolution directly condemned the secret laws and regulations on mass data collection, paying lots of attention to the essential procedural and material safeguards to be granted.[10] In a supplementary Report and Explanatory memorandum, the CoE stressed the devastating consequences, which include

---

[6] William A Schabas, *The European Convention on Human Rights: The Commentary* (OUP, 2015) 387.

[7] 'Necessary and Proportionate Coalition, Necessary & Proportionate Global Legal Analysis' (*EFF, Article 19*, May 2014) <https://cutt.ly/2JHw0hy> accessed 10 June 2022.

[8] Joint Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014] ECR I-238, paras 25-31.

[9] Luke Harding, 'Mass surveillance is fundamental threat to human rights, says European report' (*The Guardian*, 26 January 2015) <https://cutt.ly/MJHrlD5> accessed 10 June 2022.

[10] Council of Europe Resolution 2045 on Mass surveillance (2015), paras 7, 19.

undermining political opposition, persecution of activists and journalists.[11] An analogous position was advanced in the EU Resolution, qualifying the UK-US interception as "*the vast and systemic blanket collection of the personal data of innocent people, often including intimate personal information*" in breach of privacy and rule of law.[12] A final point included a call for termination of mass interception and processing of webcam imagery by any secret services,[13] which became a turning point for a large-scale discussion devoted to surveillance techniques.

As regards the EU judicial practice, in *Tele2 Sverige AB*, the CJEU called mass surveillance regimes very far-reaching and particularly serious since they are "*likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance*".[14] Similarly, in *Ministerio Fiscal* case, it outlined any interference by the public authorities with the already collected personal data, regardless of its sensitive character, as being a serious intrusion into privacy.[15]

The digitalisation caused the appearance of more comprehensive surveillance, which relies on automatic data processing, easing the access of the State to the one's data. As a result, in four 2020 cases, the CJEU stated that the EU legal framework precludes "*general and indiscriminate retention of traffic data and location data as a preventative measure*"[16] except for strictly defined cases, limited to threats to the national security and prevention of serious crimes. Moreover, where possible such measures shall be restricted to surveillance of targeted individuals, against whom a

[11] Council of Europe Report on Mass surveillance (2015) Doc 13734, para 53.

[12] European Parliament Resolution 2013/2188(INI) of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs [2013] OJ C 353 E, paras 10, 13.

[13] *Ibid*, para 26.

[14] Joined cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* [2016] ECR I-970, para 100.

[15] C-207/16 *Ministerio Fiscal* [2018] ECR I-788, para 51.

[16] C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* [2020] ECR I-790, paras 79-82; Joined Cases C-511/18, C-512/18 and C-520/18 *French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, and Igwan.net v Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l'Intérieur, and Ministre des Armées* [2018] ECR I-791, paras 119, 139.

"*valid reason to suspect*" exists.[17] Since previously the UN HRC called it "*excessively broad, highly intrusive surveillance powers on the basis of broad and insufficiently defined objectives*",[18] the common efforts of the EU and UN bodies led to the establishment of a strict threshold for mass surveillance, requiring the States to provide solid reasoning for such measures. However, the point for discussion appears where these standards overlap with the ECtHR jurisprudence.

The ECtHR provides a more detailed analysis in the area of mass surveillance. Starting from *Klass v Germany*, the Court dwelled upon the exceptional riskiness of uncontrolled and indistinctive interception of communications.[19] In *Weber and Saravia v Germany*, it called "*general surveillance measures without any specific prior suspicion in order to allow the institution of criminal proceedings against those being monitored … a fairly serious interference*",[20] yet recognising that particularly serious crimes might serve a ground for targeted surveillance. The same line of reasoning appeared in *Liberty and Others v the UK*, where the ECtHR stressed the absence of sufficient clarity in domestic law and unfettered discretion granted to executive authorities, making it impossible for individuals to foresee whether surveillance is applied and under which conditions.[21] The follow-up judgement in *Kennedy v the UK*, however, had a different finding. Since at the time of the complaint the State has already provided the Code of Practice for surveillance measures, the ECtHR considered it sufficient for the citizens to predict the potential interference.[22] The distinguishing feature of these precedents is that surveillance was based on the predefined conditions, towards certain subjects, in a limited number of cases.

[17] Joined Cases C-511/18, C-512/18 and C-520/18 *French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, and Igwan.net v Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l'Intérieur, and Ministre des Armées* ECR I-791, para 188.

[18] UNHRC 'Concluding observations on the fifth periodic report of France' (2015) UN Doc CCPR/C/SR.3193, para 12.

[19] *Klass and Others v Germany* App no 5029/71 (ECtHR, 6 September 1978), paras 58-59.

[20] *Weber and Saravia v Germany* App no 54934/00 (ECtHR, 29 June 2006), para 125.

[21] *Liberty and Others v the UK* App no 58243/00 (ECtHR, 1 July 2008), paras 64-65, 69.

[22] *Kennedy v the UK* App no 26839/05 (ECtHR, 18 May 2010), para 167.

However, the technologies develop quite rapidly, bringing new opportunities for law enforcement agents to collect data. Respectively, a line of three judgements against Russia, Hungary and the UK appeared. *Roman Zakharov v Russia* became an emblematic case on interception of phone communications, introduced by the Russian law enforcement for operational-search activities with no independent authorisation. The approach of the ECtHR slightly differed from the previous cases. It maintained that individuals are regarded as the victims of the secret surveillance only where they prove a special status, which puts them at risk of being monitored.[23] Further, the ECtHR elaborated that reasonable supervision shall be conducted when the measure is ordered, carried out or after its termination.[24] Also, a notification of surveillance is strictly necessary[25] – without a reasonable review and notification procedure an individual is deprived of the right to an effective remedy.

In *Szabó and Vissy v Hungary*, the secret anti-terrorist surveillance was also considered to be overly intrusive since it could cover virtually anyone in the State. The ECtHR stressed that a "*system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it*",[26] thus requiring a supervisory mechanism and safeguards built directly into the surveillance mechanism.[27] Moreover, it clarified that supervision of surveillance by "*a politically responsible member of the executive, such as the Minister of Justice*" is an insufficient guarantee against abuses, while the court authorisation and review are necessary.[28] As well, the ECtHR stressed the need to limit such measures in time and scope, cancelling them if "*the continued surveillance has no prospect of producing results*".[29] Accordingly, no surveillance measures can bear permanent or unlimited character.

---

[23] *Roman Zakharov v Russia* App no 47143/06 (ECtHR, 4 December 2015), para 171.

[24] *Ibid*, para 233.

[25] *Ibid*, para 234.

[26] *Szabó and Vissy v Hungary* App no 37138/14 (ECtHR, 12 January 2016), para 57.

[27] *Ibid*, para 58.

[28] *Ibid*, paras 75-77.

[29] *Ibid*, para 74.

With this case, the ECtHR finished a long line of consistent judgements devoted to the secret surveillance and its occasional incompatibility with the right to privacy, freedom of expression and the right to an effective remedy. The next stage, however, signalled a slight shift in the Court's position, broadening the monitoring powers of the State based on the margin of appreciation concept.

In 2021 the ECtHR addressed two crucial cases – *Big Brother Watch and Others v the UK* and *Centrum För Rättvisa v Sweden*. The first one emerged after Snowden disclosed the widely condemned UK content and metadata interception schemes, *e.g.* Facebook, Yahoo, Google entries and website histories monitoring. The information was also transferred to foreign intelligence agencies, such as the US secret services. Although this unprecedented case served as a ground for finding a breach of Articles 8 and 10 of the ECHR, the Court has surprisingly concluded that mass indistinctive and unconditional surveillance is not incompatible with human rights *per se*.[30] The ECtHR stepped away from its previous position requiring the suspicion of wrongdoing for the application of any surveillance measure. This shift in the position became a ground for extensive criticism from numerous NGOs, human rights defenders and independent experts[31] since it *de facto* allowed secret surveillance with a little if any notification of individuals. Another critical point touched upon the lowering of the ECtHR's standard compared to the CJEU's approach in *Schrems I. v Data Protection Commissioner*,[32] where it perceives mass surveillance as totally devastating for privacy. As well, it goes in contrast with the UN High Commissioner for Human Rights, who denied the compatibility of indiscriminate mass surveillance with human rights, given its lack of proportionality analysis.[33] These concerns are substantiated by the digitalisation and

[30] *Big Brother Watch and Others v the UK* Apps no 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021), paras 322-323.

[31] Big Brother Watch Team, 'UK Mass Surveillance Found Unlawful by Europe's Highest Human Rights Court' (*BBW*, 25 May 2021) <https://cutt.ly/xJHLCnP> accessed 10 June 2022; Privacy International, 'UK mass interception law violates human rights - but the fight against mass surveillance continues (from 2018)' (*Privacy International*, 24 May 2021) <https://cutt.ly/aJHZtR4> accessed 10 June 2022.

[32] Katitza Rodriguez, Cindy Cohn, and Karen Gullo, 'European Court on Human Rights Bought Spy Agencies' Spin on Mass Surveillance' (*EFF*, 26 May 2021) <https://cutt.ly/oJHC0VA> accessed 10 June 2022.

[33] UNCHR 'Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age' (2018) UN Doc A/HRC/39/29, para 17.

shifting of communications to online space. Namely, individuals' expectations of privacy, which serve as the basis for defining whether interference with the rights is present, become more and more blurred, while numerous conspiracy theories and fears regarding the permanent oversight on behalf of the State only grow in power and scope. As a result, the notion of democracy and safeguarding human rights diminishes its value, which is a particularly frightening tendency.

Recognising the permissibility of mass surveillance, the ECtHR developed an exhaustive list of safeguards, stressing that their need "*will be all the greater where the protection of personal data undergoing automatic processing is concerned*".[34] As regards the test developed, it involved the direct prescription of the nature of offences for surveillance, categories of individuals, whose communications can be supervised, duration of such measures, clarification of procedures for the personal data processing, precaution for transmitting data to the third parties, and circumstances for the destruction of data. Moreover, the Court insists on the application of the safeguards at each stage of the surveillance process.[35] This six-fold test reflects the previous practice of the ECtHR on surveillance issues, partly hinting at the preferrable character of limited and targeted surveillance rather than mass interception of communications. Yet, the tendency of accepting national security grounds as justifying indiscriminate monitoring and surveillance still gives rise to reasonable concerns regarding the "red lines" for the State's interference with the citizens' privacy and related rights. Finally, the Court has changed its position towards interception of journalistic materials – in the mentioned *Weber and Saravia v Germany* it held that only targeted surveillance over journalistic activities may trigger the State responsibility for interference with freedom of expression, while in this case, even indirect interception constituted a violation of Article 10 of the ECHR.

In *Centrum För Rättvisa v Sweden*, the State successfully passed the provided by law test, yet failed to provide appropriate safeguards on destroying unnecessary data, providing data to the foreign partners, having absence of effective *ex post facto* review.

---

[34] *Big Brother Watch and Others v the UK* Apps no 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021), para 330.

[35] *Ibid*, para 350.

The transmission of data to foreign security forces is compatible with Article 8 only if "*the foreign recipient of intelligence offers an acceptable minimum level of safeguards*",[36] which is an expected outcome reached by the Court. A disputable issue arises from the ECtHR recognising a notification of surveillance as unnecessary if individuals suspecting its application are granted a possibility to institute the court proceedings.[37] Although people often resort to legal nihilism, disregarding the protection to be afforded to their rights, it cannot lift the State's responsibility to fulfil its negative obligations. Moreover, if individuals can detect the surveillance measures only after instituting proceedings, it might lead to the overloading of the courts with applications regarding the potential surveillance, undermining the principle of judicial economy. Also, individuals checking the applicability of surveillance measures might not be subjected to them before the proceedings, yet become the object of monitoring afterwards. Thus, it would be more reasonable to impose the notification obligation rather than *ex post facto* court review. As the Court itself has pointed out, surveillance measures are often aimed at the interception of communications of foreigners,[38] complicating the access to the appropriate remedies and decreasing the level of safeguards in absence of notification procedures.

Contrary to indistinctive surveillance, targeted monitoring of individuals is considered to be more acceptable from the human rights perspective. The UN Special Rapporteur stressed that *per se* indistinctive systems amount to a systematic unjustified interference with human rights.[39] In contrast, the ECtHR in *Uzun v Germany* recognised the targeted GPS tracking based on suspicion of extremism as generally justifiable under Article 8 of the ECHR.[40] The targeted surveillance is tailored narrowly, being linked to the activities, background or threats posed by the specific individual. As follows from the UN High Commissioner Report, the duration of such

[36] *Centrum För Rättvisa v Sweden* App no 35252/08 (ECtHR, 25 May 2021), para 371.

[37] *Ibid*, paras 271-272.

[38] *Ibid*, para 258.

[39] UNCHR 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism' (2014) UN Doc A/69/397, paras 9-10, 52, 59.

[40] *Uzun v Germany* App no 35623/05 (ECtHR, 2 September 2010), para 69.

measures, the preconditions of their application, and the amount of collected data shall be limited under the strict necessity test.[41] An analogous position has been adopted by the CoE Parliamentary Assembly, which condemned the indistinctive monitoring of individuals, reciprocally stressing the need for targeted surveillance of suspects.[42] The reasoning implied the inefficiency of mass surveillance given the individualized contribution of persons to the crime commission. Namely, the State makes disproportionately large efforts to monitor numerous persons instead of using the same resources to specifically track several suspected individuals.

Consequently, mass surveillance is a highly criticised phenomenon, reaching little international approval, while targeted measures are considered more proportionate. Yet, unclarity is brought by the diverse approaches maintained throughout different legal regimes in the international arena, and by the regional human rights bodies. Given the latest shift in the ECtHR's approach, the FRT surveillance with a respective composition of databases is not itself incompatible with the IHRL merely due to its all-encompassing nature. However, it faces solid criticism both domestically and internationally, especially given the technical drawbacks of some developers.[43] Thus, it requires a balancing test on compatibility with specific requirements of the right to privacy, the freedom of expression, assembly and other groundful democratic values.

1.2. The implications of the facial recognition technologies for the personal data protection

Surveillance conducted via FRT usually concerns the video cameras with the supplementary databases, enabling the State authorities to identify, verify or categorize individuals. In the privacy dimension, such measures usually trigger the issues of video surveillance lawfulness, protection of biometric data collection and processing, the issues of legal and technical storage of data. All the listed challenges shall be addressed

[41] UNCHR 'Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age' (2018) UN Doc A/HRC/39/29, para 37.

[42] Council of Europe Report on Mass surveillance (2015) Doc 13734, para 11.

[43] Loprespub, 'Taming State Surveillance: Reconciling Camera Surveillance Technology with Human Rights Obligations' (*Hillnotes*, 16 March 2020) <https://cutt.ly/IJH2TfW> accessed 10 June 2022.

not only on the legislative level, *i.e.* development of the proper framework for similar operations but also on the practical plane.

1.2.1. The facial recognition technologies and standards for processing of the biometric data

The ECHR and the Convention 108+ do not specifically elaborate on the biometric surveillance, especially in the dimension of automated data processing. In the Explanatory Report to the Convention 108+, it is only stated that "*images processed by a video surveillance system solely for security reasons in a shopping area will not generally be considered as processing of sensitive data*".[44] Yet, despite being too modern for the traditional conventions, video surveillance issues have been addressed in more detail in the soft law guidelines and judicial decisions. Specifically, the ECtHR and CJEU practice directly deals with biometric data protection, defining the facial image as particularly sensitive information.[45] Moreover, in *S and Marper v the UK*, the ECtHR stressed that biometrics cannot be distributed in larger proportions than reasonably necessary even in exceptional circumstances,[46] while storage of illegally collected data amounts to a violation.[47] A strict position is also upheld regarding various methods of tracking without any groundful suspicion of criminal activities. In *Uzun v Germany*, the Court qualified tracking as opening more information about the behavioural features, thoughts and feelings than any other type of surveillance.[48]

In a similar vein, the EU legal framework distinguishes biometrics in physical (facial features, emotions *etc*) and behavioural characteristics (habits, personality traits,

[44] Council of Europe Explanatory Report to the Convention for the protection of individuals with regard to the processing of personal data (2018) CM(2018)2-addfinal, para 59.

[45] *Von Hannover v Germany (No 2)* Apps no 40660/08 and 60641/08 (ECtHR, 7 February 2012), paras 95-96; *Sciacca v Italy* App no 50774/99 (ECtHR, 11 January 2005), para 29; C-291/12 *Michael Schwarz v Stadt Bochum* [2013] ECR I-670, paras 31-32, 48-50.

[46] *S. and Marper v the UK* Apps no 30562/04 and 30566/04 (ECtHR, 4 December 2008), para 119.

[47] Максим Дворовий та інші, *Цифрові права чи громадське здоров'я: цифрові права під час пандемії COVID-19 в Україні - з урахуванням кращих практик Євросоюзу* (Інститут інноваційного врядування, 2021) 39.

[48] *Uzun v Germany* App no 35623/05 (ECtHR, 2 September 2010), para 52.

lifestyle *etc*), which could separately permit the unique identification of a person.[49] Nowadays the FRT can identify individuals even with covered faces, based only on one part of the body – the colour of eyes, hairstyle, eyebrows position and forms *etc*.[50] Also, the FRT incorporated into video surveillance enable tracking, thus serving a significant interference with one's feelings, emotions, lifestyle and other aspects of private life. Therefore, such technologies cover both physical and behavioural aspects of human life, being able to draw a full picture of one's identity.

The UN Special Rapporteur outlined numerous technological obstacles related to the biometric data collection, processing and storage,[51] which require an extensive analysis on compatibility with general principles in the data protection sphere. For example, a modern challenge is the FRT cameras with "fever detection" functions, described as "*a narrow COVID-tailored measure*", which albeit has been labelled as contributing to the creation of shadowy surveillance networks.[52] Such tendencies raise the growing concerns among human rights defenders regarding the normalization of the FRT for the completion of daily law enforcement tasks. Meanwhile, in *Escher and Others v Brazil*, the IACtHR underlined that instead of strengthening individuals' vulnerability new technologies shall push the States towards increasing their "*commitment to adapt the traditional forms of protecting the right to privacy to current times*".[53] Extensive analysis conducted by Cate and Dempsey shows that other human rights bodies, such as the ECtHR and OHCHR, insist on the additional prohibition of unfettered discretion for security services to avoid vague and declaratory legislative proposals.[54] Consequently, a special regulation with detailed procedural and material rules is required to consider the FRT existence in the human rights framework.

---

[49] European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement* (FRA, 2020) 5, 13.

[50] Tatsiana Ziniakova, *Privacy, Mass Electronic Surveillance, and the Rule of Law in Times of COVID-19* (World Justice Project, 2020) 10.

[51] UNCHR 'Report of the Special Rapporteur on the right to privacy' (2018) UN Doc A/HRC/37/62, paras 55, 125-126.

[52] Tatsiana Ziniakova, *Privacy, Mass Electronic Surveillance, and the Rule of Law in Times of COVID-19* (World Justice Project, 2020) 10.

[53] *Escher and Others v Brazil* (IACtHR, 6 July 2009), para 115.

[54] Fred H Cate and James X Dempsey, *Bulk Collection: Systematic Government Access to Private-Sector Data* (OUP, 2017) 368.

As follows from Madiega and Mildebrath's research on the FRT, nowadays several systems comprise their databases not only from the law enforcement materials but also by downloading the facial images from social media and other available resources.[55] The violations might occur when a collection of data is conducted without any authorisation, while expectations of privacy become nebulous. In this respect, the Italian Data Protection Authority called such automated processing of biometric data for the FRT a form of indiscriminate and overly intrusive surveillance technique.[56]

Considering the issues of biometric data collection, the grounds and preconditions for interference are also of paramount importance. For instance, in *TK v Asociaţia de Proprietari bloc M5A-ScaraA*, the CJEU outlined three requirements, making video surveillance compatible with the EU legal regime. They comprise the presence of the legitimate purpose for such limitations, the absence of reasonable alternatives and the balancing of the opposing interests (privacy and crime prevention).[57] If protection of national security and public order serves as a legitimate ground, a disputable issue in the FRT case arises about the alternative tools to reach the end sought. Additionally, a Joint Declaration of the UN and IAComHR Special Rapporteurs stressed a need to explicitly define the legislative boundaries for the scope and duration of surveillance measures,[58] which can be supplemented by mentioning of information types to be collected in each particular case (*i.e.* general personal data or sensitive materials, biometric data).[59] Without a specific legal regulation, such collection of personal data will breach the principle of foreseeability.

Moreover, a discussion arises as to the balance between protected and restricted rights. In this respect, two emblematic cases appeared in the ECtHR's jurisprudence. *Antović and Mirković v Montenegro* concerned the video surveillance in the university

---

[55] Tambiama Madiega and Hendrik Mildebrath, *Regulating facial recognition in the EU* (EPRS, 2021) 6-7.

[56] *Ibid*, 8.

[57] C-708/18 *TK v Asociaţia de Proprietari bloc M5A-ScaraA* [2019] ECR I-1064, paras 43-50.

[58] UN Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression and the Special Rapporteur for Freedom of Expression of the IAComHR, 'Joint Declaration on surveillance programs and their impact on freedom of expression' (2013), paras 8-9.

[59] 'Necessary and Proportionate Coalition, Necessary & Proportionate Global Legal Analysis' (*EFF, Article 19*, May 2014) <https://cutt.ly/2JHw0hy> accessed 10 June 2022.

auditoriums, which amounted to an excessive intrusion into the professors' rights. A breach of privacy occurred since monitoring was conducted both in the areas of access to official premises and in the amphitheatres, while one of the declared aims included surveillance of teaching.[60] Since no jeopardy for the rights was identified, while video recording cannot ensure effective teaching, the balance between the rights was failed. Contrastingly, *López Ribalda and Others v Spain*, addressing the video surveillance in the supermarket for prevention of criminal activities by the workers, ended up finding no violation of Article 8 of the ECHR. The difference implied the existence of a reasonable suspicion that wrongdoings were committed in *López Ribalda*,[61] while the absence of any such proof in *Antović and Mirković*. Accordingly, the results of the balancing exercise likewise differed depending on the nature of the threat.

Also, the minimum guarantees for collection of personal data, which under the EDPB[62] and CoE[63] view shall be provided to individuals, include a warning sign about conducting surveillance, a supplementary explanatory guide on the affected rights (*e.g.* posters, links to websites or QR-codes suffice),[64] and conforming to the principle of data minimisation. The right to explanation is usually interpreted broadly, covering not only legal but also technical notions and feasibilities.[65] Although generally the signs of video surveillance are provided in a form of a camera image, it resembles rather the States' attempt to decrease the human rights discussion rather than a real protective measure. Namely, the European Commission considered the deployment of the FRT causes an "*impossibility of moving in public space anonymously, or a conformism detrimental to free will*",[66] which serves as an undeniable threat to privacy and other freedoms. This position looks reasonable since the FRT deployment accompanied by

[60] *Antović and Mirković v Montenegro* App no 70838/13 (ECtHR, 28 November 2017), paras 58-60.

[61] *López Ribalda and Others v Spain* Apps no 1874/13 and 8567/13 (ECtHR, 17 October 2019), paras 123-124, 134.

[62] EDPB Guidelines 3/2019 on processing of personal data through video devices (2020) 26-27.

[63] Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108), 'Guidelines on facial recognition (2021)' (CoE, 2021) 11-12.

[64] Tambiama Madiega and Hendrik Mildebrath, *Regulating facial recognition in the EU* (EPRS, 2021) 13.

[65] Sandra Wachter, Brent Mittelstadt, and Luciano Floridi, "Why a Right to Explanation of AutomatedDecision-Making Does Not Exist in the GeneralData Protection Regulation" (2017) 7(2) International Data Privacy Law 1, 3-5.

[66] Tambiama Madiega and Hendrik Mildebrath, *Regulating facial recognition in the EU* (EPRS, 2021) 8.

a warning in the underground does not preclude people from using such transport, especially when they have no alternatives. Accordingly, this requirement remains a hypocritical attempt to show declaratory human rights compliance rather than an effective protective mechanism. Moreover, a technical explanation can be likewise hardly provided given the impossibility of actually verifying whether the system indeed processes the data in a declared manner. As a consequence, individuals are *de facto* always subjected to monitoring, which can even turn into tracking, if the coverage of the FRT video surveillance is large-scale (as usually happens in big cities). Consequently, people are practically deprived of the possibility to avoid the collection of their biometric data, which significantly undermines their privacy.

Apart from the collection of biometrics via the FRT surveillance, its processing likewise raises several legal issues. Article 9 of the GDPR prohibits the processing of personal data revealing the racial or ethnic origin and biometric data for "*uniquely identifying a natural person*".[67] Since the FRT's central task implies distinguishing individuals from the general crowd, processing biometrics is unavoidable, potentially falling under the given restriction. Any kind of such processing by the FRT may become inadmissible in a democratic society. Nevertheless, numerous EU States still apply such technologies relying on the absence of a direct and explicit prohibition.

Even if assuming general lawfulness of biometric data processing within the FRT surveillance, the aims of such processing are decisive to determine its compatibility with human rights. For instance, in *Lupker and Others v the Netherlands*, personal images were used exclusively for the identification of the alleged perpetrators and prohibited to be used for other purposes.[68] At the same time, in line with *Perry v the UK*, where non-consensual video surveillance with no specific cause or explanation amounted to a violation,[69] processing of biometrics for the FRT is not always justified. Namely, massive arrays of personal data are processed without proper notifications or

[67] European Parliament and of the Council Regulation 2016/679 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, Article 9.

[68] *Lupker and Others v the Netherlands* App no 18395/92 (EComHR, 7 December 1992), para 5.

[69] *Perry v the UK* App no 63737/00 (ECtHR, 17 July 2003), paras 42-43, 47.

any reasonable ground, for unclearly defined purposes and excessively interfering with the rights of data subjects. In *Shimovolos v Russia*, the ECtHR stipulated that general tracking of individuals suspected of illicit activities is permissible, while surveillance for establishing one's affiliation with human rights organisations or other lawful institutions is overly intrusive.[70] Hence, purposes for the processing of the lawfully collected data are decisive for the determination of the FRT compatibility with the privacy standards.

Another aspect of processing personal data in the FRT dimension directly concerns the programming and training of AI systems. Specifically, it requires large amounts of data with various facial characteristics, types of skin colour, identifications of emotions, ethnic peculiarities and interrelation of the given factors. To ensure the operability of the algorithms, AI requires the "*vast troves of real personal data*"[71] for the composition of the systems, its training and further deployment. Compared to other automatic or semi-autonomous systems, the FRT surveillance cannot operate with anonymised data for training purposes. Namely, a testing system shall provide for a significant variability and proximity to real-life circumstances. Otherwise, AI will have an unacceptably high false positives rate, making the system ineffective. Accordingly, most developers of the FRT technologies usually process biometrics without a proper regulation distinguishing operational and training phases. The draft responses to such legislative inconsistency have already been provided in France, proposing to establish different regulations for phases of development and deployment of AI systems.[72] However, no unified approach was crystalised on a global level.

Moreover, a problem arises regarding the systems' technical security, which remains under the constant threat of hacking, third-party illegal access, data interception or distortion, the potential misuse of devices or any other malpractice.[73]

---

[70] *Shimovolos v Russia* App no 30194/09 (ECtHR, 21 June 2011), para 66.

[71] Ronja Kniep, 'Another layer of opacity: how spies use AI and why we should talk about it' (*AboutIntel*, 20 December 2019) <https://cutt.ly/MJC6Tl4> accessed 10 June 2022.

[72] Jacques Follorou, 'France's tepid intelligence reform' (*AboutIntel*, 7 June 2021) <https://cutt.ly/cJVqMsO> accessed 10 June 2022.

[73] Council of Europe Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies (2013), para 6.

Numerous instances of reporting about massive hackers' attacks[74] on the FRT evidence their vulnerability to cyber threats. It manifests in the bad faith composition of the system from the stolen data as in the Clearview AI case[75] or manipulations with systems' self-learning functions. For example, in 2020 FRT passport identification system started malfunctioning following prolonged tricking with distorted or slightly modified images.[76] Those two cases evidence a strong need to properly compose the system and safeguard it technically. Moreover, it raises concerns regarding the general security of machine and deep-learning capacities, given the easiness of manipulations by such a function. Accordingly, stored information shall be safeguarded against improper changes, while AI patterns shall be reviewed in case of fundamental shifts in the algorithms' work.

Apart from technical security against external interference, the access and disclosure regimes require special regulation. In *Peck v the UK*, an attempt to commit suicide on the city street was recorded by the video surveillance and revealed to the local media, breaching the privacy of the individual despite the recording being made in a public space.[77] Similarly, the ECtHR found a violation in *Gaughran v the UK*, where a photo was stored in a local database with a mere possibility of being further transferred to law enforcement data banks and used by the FRT without any supervision or control.[78] To exemplify the contrary, in *Friedl v Austria* the ECtHR considered the usage of a photograph taken during a demonstration to verify sanitary norms and requirements maintained therein to be compatible with privacy rights since the State authorities limited their interference to observing a public event.[79] Therefore,

---

[74] Jurica Dujmovic, 'Opinion: Facial-recognition technology is one of the biggest threats to our privacy' (*MarketWatch*, 27 December 2021) <https://cutt.ly/OJVrHq8> accessed 10 June 2022.

[75] Jordan Valinsky and CNN Business, 'Opinion: Facial-recognition technology is one of the biggest threats to our privacy' (*CNN Business*, 26 February 2020) <https://cutt.ly/uJVrLfW> accessed 10 June 2022.

[76] Karen Haoarchive and Patrick Howell O'Neill, 'The hack that could make face recognition think someone else is you' (*MIT Technology Review*, 5 August 2020) <https://cutt.ly/VJVttvH> accessed 10 June 2022.

[77] *Peck v the UK* App no 44647/98 (ECtHR, 28 January 2003), paras 57-63, 87.

[78] *Gaughran v the UK* App no 45245/15 (ECtHR, 13 February 2020), paras 67-70, 86.

[79] *Friedl v Austria* App no 15225/89 (EComHR, 7 December 1992), paras 13-14.

a key aspect in determining the legality of data transmission is the purpose for its further usage and processing.

In this regard, the CoE in Declaration on Digital Tracking and other Surveillance Measures stipulates the need to prevent the distribution of the FRT to third parties and States with a low human rights record, which may undermine the privacy rights misusing such instruments.[80] Similar reasoning is advanced by numerous scholars, who stress the global effects of surveillance technologies and the necessity not only of their standardisation but also restricting distribution of technical projects to countries, which might abuse them.[81] Abstaining from such limitations States might face a case, when sharing of modern technologies undermines their own citizens' rights since surveillance often equally affects foreigners, while the FRT through a chain reaction get to the authoritarian regimes.

Finally, an important issue implies the protection of children's data, collection, processing and storage of which is subject to stricter rules and regulations. Particular caution is ascribed to the cases, where minors have been suspected of wrongdoings. According to the UN Special Rapporteur, it impairs the development of personality,[82] raising reasonable fears of constant monitoring and making their misconduct "unforgivable". Moreover, this rule equally applies not only to surveillance of alleged juvenile offenders but also to school tracking and monitoring of children with FRT. Namely, such measures require "*accountability, meaningful consent, purpose limitation, data minimization, transparency and security safeguards*",[83] the absence of which significantly undermines the rights of minors.

Thus, the deployment of the FRT surveillance creates numerous pitfalls regarding the collection of biometric data, its processing, storage and transmission to the third

[80] Council of Europe Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies (2013), para 8; UNCHR 'Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age' (2018) UN Doc A/HRC/39/29, para 25.

[81] Fred H Cate and James X Dempsey, *Bulk Collection: Systematic Government Access to Private-Sector Data* (OUP, 2017) 371.

[82] UNCHR 'Report of the Special Rapporteur on the right to privacy on Artificial intelligence and privacy, and children's privacy' (2021) UN Doc A/HRC/46/37, para 95.

[83] *Ibid*, para 109.

parties. Particularly, the inconsistencies arise from technical and legal perspectives making the current regulatory frameworks a risky legal environment for the operation of such systems.

1.2.2. Requirements for the existence of the independent supervisory bodies

Any type of surveillance necessarily needs supervision from an independent body, which manifests in both authorisation of applying tracking or monitoring measures, and constant general review of existing policies and practices in the sphere of surveillance. The CoE Commissioner for Human Rights stressed that oversight shall extend to new surveillance technologies, including evolving mechanisms and keeping pace with changing circumstances.[84] Thus, this requirement is applicable for the FRT and related biometric surveillance as the new forms of video monitoring.

The ECtHR underlined that any surveillance activity requires appropriate authorization either by a domestic court or by the independent body established under domestic law.[85] This rule, *inter alia*, applies in cases of secret surveillance, making it illegal without any oversight.[86] Although priority is given to judicial supervision, making it "*an important safeguard against arbitrariness*", a body independent of the executive[87] and authorities carrying out surveillance[88] satisfies this criterion. Since in cases of the mass FRT surveillance regular court applications significantly undermine the principle of judicial economy, establishing a separate body authorized to review such issues is a more reasonable solution. Likewise, to ensure the absence of overload

[84] Aidan Wills, 'Democratic and effective oversight of national security services' (Council of Europe Commissioner for Human Rights, 2015) 37.

[85] *Big Brother Watch and Others v the UK* Apps no 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021), para 351; UNCHR 'Report of the Special Rapporteur on the right to privacy on Right to privacy' (2019) UN Doc A/HRC/40/63, para 47.

[86] 'Necessary and Proportionate Coalition, Necessary & Proportionate Global Legal Analysis' (*EFF, Article 19*, May 2014) <https://cutt.ly/2JHw0hy> accessed 10 June 2022.

[87] *Big Brother Watch and Others v the UK* Apps no 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021), paras 357-358, 413; *Centrum För Rättvisa v Sweden* App no 35252/08 (ECtHR, 25 May 2021), paras 249-250, 271.

[88] UNCHR 'Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age' (2018) UN Doc A/HRC/39/29, para 40.

within a judicial system, an internal supervisory mechanism is proposed to be implemented on the horizontal level,[89] which applies to the installation of the FRT by the municipal authorities and enterprises. As was mentioned before, neither political figures, such as the Minister of Justice nor government-controlled institutions suffice for independent supervision.[90] Additionally, adequate resources shall be granted to such institutions for the performance of their functions efficiently and in a human right-compliant manner.[91] Thus, not only a technical capacity of the supervisory body is necessary, but also its ability to practically review the FRT's flaws, properly addressing the legal and technical issues. For example, if a supervisory organ has no access to the initial algorithms of the FRT in video surveillance or is short of human resources to observe the network of the FRT cameras around a particular region, the effectiveness of the body becomes very low.

When judges authorize the surveillance measure, they shall understand "*the potential implications of their decisions, particularly in terms of the technology to be employed and the consequences of using that technology*".[92] A similar requirement applies to the members of the oversight bodies, which along with the judges, need training, resources and technical explanatory guides on the functioning of the modern surveillance technologies. Moreover, the UN Special Rapporteur stresses the need not only to understand the algorithm of such systems but also to "*comprehend and digest*" them,[93] identify threats, assess the degree of the risks *etc*. Apart from a necessary qualification ascribed to the individuals comprising a supervisory organ, a third-party independent expertise might be beneficial for understanding the FRT functioning. In this respect, a special legal mechanism for involving independent experts shall be developed and implemented.

---

[89] *Ibid*, para 31.

[90] *Szabó and Vissy v Hungary* App no 37138/14 (ECtHR, 12 January 2016), paras 75-77.

[91] UNHR Council 'The right to privacy in the digital ' (2017) UN Doc A/HRC/34/L.7/Re; Necessary and Proportionate, 'International Principles on the Application of Human Rights to Communications Surveillance' (Necessary and Proportionate, 2014) 9.

[92] UNCHR 'Report of the Special Rapporteur on the right to privacy' (2017) UN Doc A/HRC/34/60, para 28.

[93] *Ibid*.

In the aforementioned *Centrum För Rättvisa*, the ECtHR also developed the main requirements for the functionality of independent bodies, including supervision accessibility to anyone suspecting surveillance or notified of it, compulsory prior authorization, oversight of ongoing surveillance and *ex post facto* review. Furthermore, the regulation shall be developed with a solid statutory basis in domestic law,[94] not via secondary legislation inclined to frequent and unfavourable human rights changes. Another aspect implies the capacity of the supervisory body to penalize violations and abuses. Otherwise, the policies of the supervisory body will be unenforceable, making its existence inefficient and standards – declaratory.

The authorisation of surveillance, in the HRC's view, totally depends on the circumstances of each particular case, having no universal recipe of necessary monitoring, tracking or interception.[95] Case-by-case reasoning of necessity is interpreted by numerous scholars as requiring individualized scrutiny, which *de facto* rejects the idea of mass surveillance.[96] However, the main requirement still is the existence of the prior authorisation for the collection of biometrics, which is obligatory for both law enforcement and security services. Namely, even situations of absolute secrecy shall not preclude or postpone independent overview and authorisation. A negative example can be found in the US, where the Foreign Intelligence Surveillance Court operates in near-total secrecy, which opens the space for abusive practices in favour of the State.[97] Such a supervisory mechanism significantly sophisticates the appeal procedure, making the oversight untransparent and thus inefficient.

In cases of the FRT, its deep and machine learning function leads to rapid changes in the systems' composition. Respectively, a periodic review is necessary for ensuring the proper functioning of the FRT mechanism, and the absence of malfunctioning,

---

[94] UNCHR 'Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age' (2018) UN Doc A/HRC/39/29, para 33.

[95] UNCHR, General Comment №16 'Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation' (1988) UN Doc HRI/GEN/1/Rev.9 (Vol. I), para 8.

[96] Fred H Cate and James X Dempsey, *Bulk Collection: Systematic Government Access to Private-Sector Data* (OUP, 2017) 371; UNCHR 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism' (2014) UN Doc A/69/397, para 46.

[97] ACLU, 'End Mass Surveillance under the Patriot Act' (*ACLU*, 2015) <https://cutt.ly/VJVttvH> accessed 10 June 2022.

abuses or misuses of the technology. A regular review of surveillance systems requires both legal and technical contributions. The main pitfall implies a necessity to ensure correspondence of the FRT description and technical features, since members of the supervisory bodies can rarely check the sophisticated algorithms. Moreover, given the amounts of data necessary for the creation of similar systems, it is often unfeasible to establish an efficient human oversight.

Additionally, one of the most widely-spread problems is an absence of adequate enforcement and incentive to adopt the relevant international requirements and implement them in practice, controlling the compatibility of existing systems with such standards on the technical level.[98] In this respect, supervisory bodies can be granted the powers to cooperate with technical giants, providing them with guidelines on basic principles for the development of the FRT. Namely, the creation of the multistakeholder platform for the exchange of best practices and experience in the development, regulation and testing of systems will ease the cooperation of governments, private actors developing and implementing the FRT, as well as independent experts interested in the maintenance of human rights standards throughout the whole life-cycle of such systems. Furthermore, it might ensure the equal requirements for surveillance systems from the technical perspective, regulating the market of the FRT not only in surveillance issues but also in other areas. Also, it will assist in safeguarding the market against potentially dangerous or abusive mechanisms.

Accordingly, even a formal satisfaction of the criterion on a supervisory body with independent oversight cannot lift numerous practical difficulties related to interaction with various the FRT, their understanding and timely resolution of problems regarding the excessive or unlawful collection of biometrics. Thus, until a clear technical oversight can be established, the FRT surveillance remains in a grey zone for a qualitative review and authorisation.

[98] Will Schrepferman, 'Supervising Surveillance: Applying International Law to the Global Surveillance State' (*Harvard International Review*, 11 November 2020) <https://cutt.ly/BJNwJvV> accessed 10 June 2022.

1.3. Potential adverse effects on human rights arising from the facial recognition technologies

The composition of the FRT implies an assessment of identifying biometric features, processing of which is often on the verge of distinction by race, ethnicity, nationality, gender and other protected grounds. On the one hand, effective identification of suspected criminals is impossible without extensive analysis of the listed characteristics. On the other, it often creates the risks of discriminatory treatment, which can be unintentionally incorporated into the system during the development stage, or deliberately reached in the course of its deployment.

1.3.1. Risks of discriminatory treatment within the surveillance measures application

Discrimination is explicitly outlawed by all existing human rights conventions, including the ICCPR, the ECHR and other regional documents. Under the well-established approach, "*apparently neutral rule resulting in individuals being put at a particular disadvantage*" nevertheless remains unlawful.[99] Less favourable treatment results from a measure "*in whole or in part*" because any negative effect produced by the limitation can be discriminatory.[100] In *Horváth and Kiss v Hungary*, the ECtHR underlined that even the restriction, which may put more than one group at disadvantage, is disproportional.[101] Thus, either deliberate or unintentional, the FRT application as a restriction on privacy, freedom of movement and other fundamental rights shall comply with a prohibition of unequal treatment.

Given the all-encompassing character of the FRT in surveillance systems, they can indistinctively target a large number of individuals, categorising them and further

---

[99] Torkel Opsahl, *Equality in Human Rights Law* (Kehl am Rhein NP Engel Verlag, 1988) 61; Lord Lester of Herne Hill and Sarah Joseph, *Obligations of Non-discrimination* (OUP, 1995) 575; *Case Concerning Rights of Nationals of the US in Morocco (France v the US)*, Judgment, ICJ Reports 1952, 176, 186; *Rupert Althammer v Austria*, Communication no 803/1998, UN Doc CCPR/C/74/D/803/1998 (2002), para 10.2; C-188/15 *Asma Bougnaoui and Association de défense des droits de l'homme (ADDH) v Micropole SA* [2017] ECR I-204, para 32; *D.H. and Others v the Czech Republic* App no 57325/00 (ECtHR, 13 November 2007), paras 180, 184.

[100] C-83/14 *CHEZ Razpredelenie Bulgaria AD v Komisia za zashtita ot diskriminatsia* [2015] ECR I-480, para 76.

[101] *Horváth and Kiss v Hungary* App no 11146/11 (ECtHR, 23 January 2013), para 110.

tracking such persons. Interception of communications depends primarily on a reasonable suspicion, knowledge of technical characteristics of the device and time-frame for interference, being linked to the identity of a specific person. However, the FRT is a more comprehensive system of identification, analysing every person, who has features close to ones incorporated into the database of "wanted" individuals. Being inclined to categorization, the FRT can target not only particular persons but also groups of people based on a certain unifying feature. Accordingly, certain issues regarding potential discriminatory treatment might arise, covering both deliberate monitoring of some groups based on gender, the colour of skin or affiliation with a certain community, and unintentional mismatching due to the systems' flaws, improper programming or testing gaps.

As regards the development and testing phases, effective performance of the FRT functions requires adequate programming, enabling a system to identify individuals with the highest probability (since decisions about matches with a database are never a definitive result, but a percentage of similarity).[102] In this respect, an important issue implies amounts of data for training the system and establishing the proper threshold for the false positives and negatives. If a threshold is high for the most similar images, false positives decrease with false negatives simultaneously increasing.[103] For example, where a permissible percentage of similarity for a "successful match" is fixed at 80%, more people can be labelled as similar to the sample image. However, the bigger number of people who are identified as a match, the more mistakes a system can do. If 5000 persons are labelled as similar to the template image, law enforcement will be stuck with analysing such amounts of data to find a missed individual or a suspected offender. Thus, sometimes even a small false positives rate might have significant practical implications for the system's efficiency. Finally, the EU Agency for Fundamental Rights stressed the interdependence between the successful operation of

[102] European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement* (FRA, 2020) 9.

[103] Patrick Grother, Mei Ngan, and Kayee Hanaokai, "Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification" (2018) 8238 NIST Pubs, 24-25.

the FRT and the quantities of real cases filled in the system.[104] Accordingly, the absence of necessary sample data or its underrepresentation often leads to the mistakes, increasing the false positives rate. Such a situation is particularly dangerous when the issue relates to the identification of persons from vulnerable or marginalized groups.

The main problem emerging from improper programming of the FRT in the dimension of discriminatory practices includes mirroring the existent societal biases. Namely, the development of biometric surveillance can "*exacerbate exclusion and reproduce racial, gender, class, and other inequalities*",[105] which have deeply rooted in everyday life, becoming part of the social canvas. However, not only the traditional improper perception of the protected groups amplifies the institutional discrimination, but also the lack of representative data. For example, Indian practice shows that iris recognition systems are not adjusted to ageing making several mistakes in identification, while in Israel data on Palestinians is frequently skipped during the FRT programming, leading to the policies of segregation.[106] This problem does not always depend on the technical obsoleteness of the FRT or deliberate omissions to include relevant information. Sometimes national developers simply lack data to compose the system in a balanced manner. Thus, the relevant issue is the degree of a discriminatory component in the FRT algorithms and the potential for debiasing of the system.

Notwithstanding grounds for possible bias differ, *i.e.* race, ethnicity, gender, religion or class, an overall pattern of data underrepresentation is the same. To clarify, the system is more precise in face identification within 800 samples of the Caucasian type of face than among only 300 Asian samples. Respectively, many available options directly affect the accuracy, impacting the false positives and negatives rate. Additional difficulty arises if the lack of qualitative relevant data overlaps with the environment unfavourable for identification,[107] *e.g.* images obtained via video surveillance are

---

[104] European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement* (FRA, 2020) 9-10.

[105] Privacy International, 'Biometrics collection under the pretext of counter-terrorism' (Privacy International, 28 May 2021) <https://cutt.ly/1JMrPw8> accessed 10 June 2022.

[106] *Ibid.*

[107] José Sánchez del Río and Cristina Conde, "Face-based recognition systems in the ABC e-gates" (2015) 340-346 9th Annual IEEE International Systems Conference 340, 341.

brightness, clothes partly hiding or tinting a face, object occlusion, illumination. To exemplify, excessive light will negatively affect the identification of the very fair-skinned individuals, while lack of light negatively influences the system's capacities in identifying dark-skinned persons.[108] Another problem is the large age discrepancies between the sample image in the benchmark database and one's real-life appearance. These flaws significantly decrease the effectiveness the FRT for law enforcement purposes, hinting at the technical imperfectness of surveillance systems akin to the unresolved legal issues. Since the quality of images cannot be easily controlled or adjusted, especially in street video surveillance, the effectiveness of facial and emotion recognition decreases to the pure analysis of the silhouettes.

According to the UN Special Rapporteur, extensive biometric surveillance targeted at racial, ethnic and indigenous groups often negatively influences interpersonal and familial relationships, undermining religious practices.[109] For instance, it happened with Muslim communities in some North American and East Asian countries, where religion, an indefeasible attribute of ethnicity, serves as a ground for structural discrimination reaching the level of profiling. As regards emotion recognition, the FRT are usually "*exhibiting insufficient levels of sensitivity to cultural and other differences in ways in which people behave and emote*",[110] making such technology imprecise and often very intrusive. Furthermore, body language often varies depending on the region, the most well-known example of which is the difference in nodding interpretation among nations (Bulgarians perceive it as a sign of rejection, while most other Europeans give it a polar meaning). Hence, attempts to implement emotion recognition in the FRT surveillance give rise to more pitfalls, while its effectiveness is close to zero since the appearance of a person cannot precisely point

[108] European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement* (FRA, 2020) 27.

[109] UNCHR 'Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance' (2017) UN Doc A/HRC/35/41, paras 72-74.

[110] Krisztina Huszti-Orbán and Fionnuala Ní Aoláin, *Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?* (Human Rights Center, University of Minnesota, 2020) 25.

to national or cultural origin. Cumulatively the dangers and inconveniences nowadays outweigh the benefits for law enforcement search and monitoring operations.

Another issue concerns the potential for gender discrimination. According to Buolamwini and Gebru, gender-classification algorithms usually have a mistake rate between 20 and 34%, which is exacerbated by a combination of racial biases present in FRT.[111] A similar conclusion is reached by other researchers,[112] who identified the analysis of dark-skinned women's faces as the most inaccurate compared to other data categories. For example, they are usually misgendered, mismatched with the original images or not even recognized by the system as a sample for analysis, falling behind the pre-coded characteristics.[113] It evidences the low FRT performance in cases, where training data and benchmark images data sets are lacking diversity or where the FRT is oriented at a specific market, being rather exclusive. Namely, systems are narrowly tailored to the societies with a certain prevailing gender or racial type, becoming unsuitable for other markets and even discriminating against foreigners or non-binary people within the same social environment.

The problem of discriminatory identification is only amplified regarding the LGBTQI+ communities. Such data is lacking either due to their general underrepresentation among societies, the reluctance of the developers to consider such data during testing phases, or fear of providing it in certain regions due to persecution. Even where the States are trying to facilitate surveillance of the LGBTQI+ community via the FRT,[114] purposefully targeting its members, data is never objective and definite, reinforcing existing biases and distorting the algorithms' functioning. A similar treatment is often experienced by other minority groups. To exemplify, Muslims are

---

[111] Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification" (2018) Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81 77-91, 85.

[112] Jurica Dujmovic, 'Opinion: Facial-recognition technology is one of the biggest threats to our privacy' (*MarketWatch*, 27 December 2021) <https://cutt.ly/OJVrHq8> accessed 10 June 2022.

[113] Joy Boulamwini, 'How well do IBM, Microsoft, and Face++ AI services guess the gender of a face?' (*Gender Shades*, 2018) <https://cutt.ly/KJMagRB> accessed 10 June 2022.

[114] Naseem Tarawnah, 'Mass surveillance, press crackdowns, and punishing prisoners of conscience – impunity reigns in MENA' (*IFEX*, 8 September 2021) <https://cutt.ly/wJMaOH2> accessed 10 June 2022.

extensively monitored and profiled under terrorism-related laws,[115] while deficiency of relevant data leads to frequent mismatching and wrong accusations. In the same vein, non-nationals, refugees and asylum seekers are underrepresented in the FRT developed on the national data sets. This leads to the political, social and economic exclusion of minority communities, making them marginalized and alienated, escalating existent tensions within societies, and creating grievances that can be "*conductive to recruitment of terrorists*".[116] In this respect, the CoE Guidelines on the FRT provide that developers shall "*avoid mislabelling, thereby sufficiently testing their systems, identifying and eliminating disparities in accuracy, notably with regard to demographic variations in skin colour, age and gender*".[117] Hence, the composition of the FRT cannot abstain from consideration of vast amounts of diversified data even if the primary market remains a national one. Although Hacker contends that legal norms propose an easy justification for certain kinds of algorithmic discrimination, being hardly applicable to relations between the private entities,[118] the FRT deployment by public authorities still triggers the prohibition of discriminatory treatment even on the level of composing a system.

Pre-programmed biases in the FRT on the development and testing phases mostly concern technical rather than legal issues. Yet, apart from composition, the discriminatory element appears in the deployment stage,[119] especially if the Stated with low human registers are trying to abuse the algorithms.

Experts point out that the FRT application in policing, border control and security services frequently causes life-changing repercussions.[120] For example, the US law

---

[115] UNCHR 'Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance on Combating racism, racial discrimination, xenophobia and related intolerance and the comprehensive implementation of and follow-up to the Durban Declaration and Programme of Action' (2017) UN Doc A/72/287, paras 39-41.

[116] *Ibid*, paras 44-45.

[117] Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108), 'Guidelines on facial recognition (2021)' (CoE, 2021) 9.

[118] Philipp Hacker, "Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination Under EU Law" (2018) 55 Common Market Law Review 1143, 1164-1165.

[119] Tambiama Madiega and Hendrik Mildebrath, *Regulating facial recognition in the EU* (EPRS, 2021) 7.

[120] Tonya Riley, 'UN calls for human rights safeguards on artificial intelligence' (*CyberScoop*, 15 September 2021) <https://cutt.ly/TJMfzQY> accessed 10 June 2022.

enforcement charged a dark-skinned person due to the FRT mismatch, which has further led to the lifting of accusations.[121] Mismatching becomes even more dangerous in cases of asylum seekers,[122] where refusal causes not only discomfort in a form of unsubstantiated court proceedings, but also a possibility of deportation. Given a tendency to perceive machine-based decisions as more trustworthy, unfavourable legal repercussions of the FRT application become more and more widespread. Madiega and Mildebrath stipulate that the FRT's inability to give definite results leads to alteration of the traditional presumption of innocence due to the incidence of the high false positives.[123] Moreover, usage of the FRT images as evidence requires a review of the legal framework, including the predefined degree of similarity, verification of the images' authenticity, admissibility of evidence, supplementary evidence issues *etc*. Accordingly, the FRT regulation is required before its application as a ground for charges or accusations, while such systems shall never be the only source of evidence given their probable rather than definite result.

Another potential space for abuse is the FRT application for profiling purposes aimed at the performance of law enforcement and security services tasks. In this respect, the ECtHR in *Timishev v Russia* declared racial and ethnic profiling a manifestation of unjustifiable practice,[124] while the IACtHR characterized it as a stereotype-driven policy "*to single out individuals or groups in a discriminatory way based on the erroneous assumption that people with such characteristics are prone to engage in specific types of crimes*".[125] Namely, profiling often leads to disproportionate selective arrests,[126] prosecutions and overrepresentation of targeted groups in the criminal justice system, in entrance and asylum rejection cases. Racial, ethnic, gender

[121] Tonya Riley, 'Momentum builds on federal oversight of facial recognition tech after reported abuses' (*CyberScoop*, 15 July 2021) <https://cutt.ly/LJMfIiZ> accessed 10 June 2022.

[122] OSCE ODIHR, 'Border Management and Human Rights' (OSCE, 2021) 19-20.

[123] Tambiama Madiega and Hendrik Mildebrath, *Regulating facial recognition in the EU* (EPRS, 2021) 7.

[124] *Timishev v Russia* Apps no 55762/00 and 55974/00 (ECtHR, 13 December 2005), paras 56-59.

[125] *Case 12.440, Report No 26/09 Wallace de Almeida (Brazil)* (IAComHR, 20 March 2009), para 143.

[126] UNCHR 'Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance' (2015) UN Doc A/HRC/29/46, para 63.

or any other profiling based on a protected characteristic causes enhanced harm if conducted via the FRT.

Since profiling feature is a constituent of the FRT surveillance, being a necessary element of the databases, the UN Special Rapporteur recommended "*review, repeal and prohibit legislation that facilitates States to monitor*" gender-nonconforming communities and other vulnerable groups.[127] Specifically, the FRT shall not be purposefully used for suppressing or persecuting certain groups. In China, such technologies constantly detect the Uighur minority for further unlawful arrests and detentions, while the Israeli Blue Wolf system in the same vein tracks Palestinians to maintain effective control over the disputed territories.[128] These two examples show how prima facie neutral and useful systems can be easily abused to reinforce governmental discriminatory policies. However, even democratic governments might potentially make use of such technologies, deliberately targeting vulnerable groups. And the biggest problem is the impossibility to define the stage, at which something went wrong. Namely, in dealing with the FRT scientists usually face a so-called "black box" phenomenon,[129] which precludes detection of discriminatory decisions in absence of the system's reasoning for the taken steps. Thus, an outer review is difficult, opening space for uncontrolled usage of the FRT with the only reliance on the high legal and technical qualifications of the supervisory bodies.

Lastly, self-learning algorithms superimposed on the biased system only strengthen the discriminatory application, making cases of unequal treatment unpredictable and, therefore, even more dangerous. A function creep – "*the gradual widening of a technology beyond its original, intended purpose, just because the possibility exists*"[130] may significantly distort its original purpose and the primarily incorporated values. One of the proposed ways to address the problem of structural

[127] UNCHR 'Report of the Special Rapporteur on the right to privacy' (2020) UN Doc A/HRC/43/52, para 53.

[128] Omar Shakir and Maya Wang, 'Mass surveillance fuels oppression of Uighurs and Palestinians' (*Aljazeera*, 24 November 2021) <https://cutt.ly/RJ1zek4> accessed 10 June 2022.

[129] Tambiama Madiega and Hendrik Mildebrath, *Regulating facial recognition in the EU* (EPRS, 2021) 20.

[130] Privacy International, 'Biometrics collection under the pretext of counter-terrorism' (Privacy International, 28 May 2021) <https://cutt.ly/1JMrPw8> accessed 10 June 2022.

inequalities and reproduction of biological essentialism is debiasing.[131] However, reinforced and more frequent tests of the FRT cannot clear the discriminatory functioning of the algorithms since they also depend on the authorities' perception of discrimination. They are often substantiated by a complex and comprehensive nature of the system, verification of which from a debiasing perspective is hardly possible. Accordingly, human rights organisations are proposing to establish red lines, prohibiting some types of AI tools, unable to be filtered from biases.[132] Biometric surveillance systems, including the FRT, are put on the list of such tools, seriously threatening human rights not only because of their potential for discrimination but due to the wide space for abuse open to any authority resorting to such techniques. Therefore, establishing the FRT compatibility with human rights requires both a balancing exercise on technical benefits and flows and an assessment of dangers stemming from abusive application for the persecution of vulnerable and marginalised groups.

1.3.2. Impact on the rights to freedom of expression and assembly

An indirect impact of the FRT extends far beyond correcting the technical vulnerabilities, developing unbiased systems and ensuring the security of the relevant data banks. The most dangerous side effects, which define the FRT danger rate in the human rights dimension, still relate to its application, accessibility of abusive practices and potential safeguards against malicious repercussions. Apart from discriminatory implications, the FRT also has a general impact on other basic rights, including freedom of expression and freedom of assembly. As the ECtHR's Guide on Article 10 stipulates, placing journalists under surveillance regardless of its targeted or indistinctive character by default triggers free speech rights.[133]Although it primarily

[131] Agathe Balayn and Seda Gürses, 'Beyond Debiasing: Regulating AI and its inequalities' (*EDRi*, 21 September 2021) <https://cutt.ly/2J1xfw1> accessed 10 June 2022.

[132] EDRi, 'Civil society calls for AI red lines in the European Union's Artificial Intelligence proposal' (*EDRi*, 12 January 2021) <https://cutt.ly/UJ1nlR4> accessed 10 June 2022.

[133] ECtHR, Guide on Article 10 of the European Convention on Human Rights (CoE/ECtHR, 30 April 2021), paras 348-349.

relates to the special subjects, such as journalists, activists and political dissidents, any individual might suffer from the FRT surveillance influencing one's free speech.

Monitoring measures frequently ruin the special protection granted to confidential communications, including exchange of lawyers', medical and commercial secrets, disclosure of one's intimate information or even classified State-related materials. Since the FRT indiscriminately intercepts any communication, including the exchange of private opinions and ideas, it may influence the quality of the expressed political beliefs, social positions and affiliation with certain communities.[134] Notwithstanding that effective oversight might decrease the negative impact from a legal standpoint, it cannot change the perception of the devastatingly intrusive nature of surveillance in the eyes of a reasonable person. As a result, a chilling effect occurs, diminishing the information environment and creating numerous obstacles to the free flow of opinions.

The chilling effect concerns a negative influence of the restrictions,[135] which discourages people from expressing themselves in any manner.[136] The consequences of this phenomenon usually include attempts to self-censor protected expressions,[137] fearing repressions, persecutions, unlawful prosecution or any other type of applicable penalty.[138] As follows from emblematic ECtHR's judgement in *Navalnyy v Russia*, the chilling effect is only exacerbated if opinion leaders, politicians, activists or other public figures are disproportionately affected.[139] Such implications are especially dangerous in the States with a low human rights record, where silencing human rights defenders, politicians and NGOs dissuades opposition supporters and other vulnerable groups. According to CoE Report on mass surveillance, authors, journalists and civil

---

[134] Amnesty International Report 45/002/2014 'Amnesty International submission to the intelligence and security committee's privacy and security inquiry' (Amnesty International, 7 February 2014), para 6.

[135] Venice Commission Opinion no 831/2015 'On articles 216, 299, 301 and 314 of the Penal Code of Turkey, adopted by the Venice Commission at its 106th plenary session' (2016) CDL-AD(2016)002, para 27.

[136] *Lingens v Austria* App no 9815/82 (ECtHR, 8 July 1986), para 44; *Laurent Pech, The Concept of Chilling Effect: Its Untapped Potential to Better Protect Democracy, the Rule of Law, and Fundamental Rights in the EU* (Open Society Foundation, 2021) 4.

[137] *Vajnai v Hungary* App no 33629/06 (ECtHR, 8 July 2008), para 54.

[138] Elvin Ong, "Online Repression and Self-Censorship: Evidence from Southeast Asia" (2019) 56(1) Government and Opposition 1, 7.

[139] *Navalnyy v Russia* Apps no 29580/12, 36847/12, 11252/13, 12317/13 and 43746/14 (ECtHR, 15 November 2018), para 152.

society activists are reluctant to "*write, speak, or pursue research about certain subjects … or to communicate with sources or friends for fear that they will endanger their counterparts by so doing*".[140] The same position is addressed by the UN Special Rapporteur, stressing that concerns exist regarding the potential sanctions not to the targets of surveillance, but towards their networks of contacts.[141] Thus, interception of activists' communications and monitoring of their networks inevitably influences their campaigns, making them less successful with people withdrawing under the fear of subsequent prosecution.

Moreover, NGOs cannot effectively perform their public watchdog function,[142] being deprived of their sources of information, *e.g.* when addressing crimes conducted by public authorities, disclosing data on massive human rights violations or investigating corruptive links. Without tenacious reporting by civil society, digital-forensic investigations of non-governmental researchers and the media analysis of the FRT surveillance impact on free speech and informing society on technologies implications becomes impossible,[143] as well as independent assessment of such systems by international specialised bodies. In this respect, the UN Special Rapporteur underlined that surveillance can never be used for "*the muzzling of any advocacy of multiparty democracy, democratic tenets and human rights*",[144] which implies *de facto* illegality of any technology with a strong chilling effect upon freedom of expression. Since the FRT surveillance might trigger a fear of persecution based on the delivery of unpopular, nonconformist or recusant opinions, it requires a critical analysis in the free speech dimension, which likewise relates to a practical possibility to safeguard the sources of information. For the purposes of this thesis, a more detailed review of the

[140] Council of Europe Report on Mass surveillance (2015) Doc 13734, para 97.

[141] UNCHR 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on surveillance and human rights' (2019) UN Doc A/HRC/41/35, para 21.

[142] Article 19, 'ARTICLE 19 tells Strasbourg Court that mass surveillance is incompatible with the Convention' (*Article 19*, 24 April 2019) <https://cutt.ly/hJ1WWJE> accessed 10 June 2022.

[143] UNCHR 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on surveillance and human rights' (2019) UN Doc A/HRC/41/35, para 1.

[144] *Ibid*, para 26.

FRT technical capacities will be conducted regarding the journalistic sources, given their most vulnerable character towards the chilling effect.

A general approach maintained by the regional human rights bodies implies enhanced protection for the physical safety of journalists, their sources and materials, as well as any kind of secret communications. The ECtHR in *Telegraaf Media Nederland Landelijke Media B.V. and Others v the Netherlands* stipulated that supervisory bodies "*cannot restore the confidentiality of journalistic sources once it is destroyed*",[145] thus their non-disclosure shall be prioritized, limiting the cases of revealing identities to an inevitable minimum. It is particularly relevant for cases involving whistleblowers, who share materials on wrongdoings of public authorities, therefore, being the primary targets for persecution. In this regard, the ICCPR, the UN Convention against Corruption and numerous soft law instruments elaborate on the need to protect whistleblowers from legal reprisals and disciplinary actions, given their contribution to "*breaking illegitimate rings of secrecy*" around the State affairs.[146]

Contrary to the ordinary video surveillance, the FRT analyses the facial features of any individual in a visible radius, incorporating the obtained biometric map with a unique "face-print" into the database.[147] If tracking journalists via ordinary video requires knowledge of the relative location and time of the expected meeting, the FRT only needs to download the template image. The system subsequently identifies the routes and interlocutors – especially, well-known individuals with publicly accessible images suitable for comparison. Moreover, automatic identification enables to obtain a result in a matter of seconds without any human effort or proactive steps. Hence, the confidentiality of sources is *de facto* destroyed from the moment individuals appear on the same screen having a conversation, which makes the FRT a dangerous and overly intrusive tool. This way numerous media workers and their sources have been

[145] *Telegraaf Media Nederland Landelijke Media B.V. and Others v the Netherlands* App no 39315/06 (ECtHR, 22 November 2012), para 101.

[146] 'Necessary and Proportionate Coalition, Necessary & Proportionate Global Legal Analysis' (*EFF, Article 19*, May 2014) <https://cutt.ly/2JHw0hy> accessed 10 June 2022.

[147] Hussain Syed, 'How Human Rights is Facing up to Mass Surveillance' (*The British Institute of Human Rights*, 2019) <https://cutt.ly/LJ1RaRZ> accessed 10 June 2022.

identified and persecuted. To exemplify, in Azerbaijan, Morocco, Mexico and India dozens of journalists were targeted by surveillance systems, which forced them to abstain from reporting and turn to self-censorship.[148] One of the main reasons was that they never felt safe about their security and security of their sources, only proving the all-encompassing nature of the FRT and its devastating impact on free speech.

Apart from freedom of expression, the FRT surveillance likewise influences the right to peaceful assembly, often depriving individuals of confidence in their safety before the State and other members of the society. As follows from the ICCPR General Comment №37, surveillance technologies are generally inclined to infringe the rights of assembly participants and bystanders by causing a chilling effect.[149] For example, the retention of personal data extracted from the images taken during demonstrations, a permanent or systematic record of activists[150] and their profiling for law enforcement purposes create a reasonable fear of potential persecution. A danger also exists regarding the insecurity of databases, when activists' profiles are obtained by the aggressive counter-movements due to hacking of the systems. As a result, activists, leaders of minority communities and representatives of NGOs might become the targets of violence, harassment, provocations and blackmailing by non-State actors (in addition to potential persecution by the State). This only aggravates the fears, having a devastating impact on the freedom of assembly. Accordingly, both legislative and policy regulations shall be oriented at the protection of activists, providing solid limitations for circumstances and reasons of the recording, limiting the storage of biometrics to a necessary minimum in time, scope and conditions,[151] as well as ensuring technical security against the third-party interference.

---

[148] Amnesty International, 'Joint Open Letter: States Must Implement Moratorium on Surveillance Technology' (*Pen America*, 27 July 2021) <https://cutt.ly/0J1Ro0u> accessed 10 June 2022.

[149] UNCHR, General Comment №37 'Article 21 (Right to Peaceful Assembly)' (2020) UN Doc CCPR/C/GC/37, para 10.

[150] Venice Commission and OSCE/ODIHR Guidelines on Freedom of Peaceful Assembly (3rd Edition) (2019) CDL-AD(2019)017, para 172.

[151] UNHR Council 'Joint report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association and the Special Rapporteur on extrajudicial, summary or arbitrary executions on the proper management of assemblies' (2016) UN Doc A/HRC/31/66, para 76.

Anonymous participation in public gatherings, crystalised in the ICCPR General Comment №37,[152] implies the usage of face coverings or other disguises to hide the identity becomes hardly possible, given the FRT's ability to recognise faces regardless of masks atop. For example, Chinese companies have already developed such systems as a rapid response to COVID-19, proving their practical efficiency in numerous protests.[153] If previously numerous authorities were criticised for the ordinary audiovisual recording of participants, the FRT real-time surveillance "*dramatically increased the capacity to identify [them] in an assembly in an automated fashion*".[154] Thus, facial and emotion recognition destroys the anonymity notions within the public gatherings, undermining the longstanding values and constituents of this democratic institute. Similarly, when the future assembly has a Facebook or Instagram public page, it becomes very convenient to identify the coordinators and create administrative and practical obstacles for them to proceed with organising the protest. Respectively, a complex character of surveillance techniques disables any secret exchange of data for legitimate purposes (including whistleblowing, journalistic investigations, private business communications *etc*), which likewise covers the cases of public gatherings.

Since public authorities are technically connected to mutually integrated databases, they can track individuals anywhere the FRT surveillance is deployed, identifying persons in a matter of seconds via access to centralized open or confidential data banks. For example, data collected and preserved in a battlefield context for further counter-terrorism trials remains available for law enforcement,[155] being suitable for filling in the FRT to apprehend such a person. However, the same algorithm applies to the activists' photos taken during demonstrations for verifying sanitary conditions

---

[152] UNCHR, General Comment №37 'Article 21 (Right to Peaceful Assembly)' (2020) UN Doc CCPR/C/GC/37, paras 60-61.

[153] Martin Pollard, 'Even mask-wearers can be ID'd, China facial recognition firm says' (*Reuters*, 9 March 2020) <https://cutt.ly/ZJ1PySg> accessed 10 June 2022.

[154] UNCHR 'Report of the United Nations High Commissioner for Human Rights on impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests' (2020) UN Doc A/HRC/44/24, para 34.

[155] UN Counter-Terrorism Committee Executive Directorate, 'Guidelines to facilitate the use and admissibility as evidence in national criminal courts of information collected, handled, preserved and shared by the military to prosecute terrorist offences' (UNCTED, 2019) 13, 16.

(as happened in the aforementioned *Friedl v Austria*).[156] Thus, the FRT can be misused for persecuting political dissidents or opposition activists without any technical obstacle, while its complex application with other biometric surveillance tools enables not only subsequent persecution but also prevention of unfavourable gatherings. Namely, leaders of social movements can be easily tracked via social media and subsequently apprehended via the FRT street surveillance based on their images from public campaigns. Also, the FRT enables tracking potential activists,[157] facilitating disruption of demonstration via blocking of the most widely used routes for occasional would-be participants (especially for protests of the regional scale). Another space for abuse is collecting data on active participants at the first demonstration for thwarting further public gatherings, as often happens with State campaigns against environmental protests described in detail by the UN Special Rapporteur.[158] Following the State FRT surveillance targeting protesters and activists, the public gatherings coordination level significantly decreases, making them disorganized, sparsely populous and ineffective, which discourages people from further participation.

Lastly, the FRT surveillance might become a suitable tool for the persecution of activists beyond the context of public gatherings or protection of sources for free speech purposes. In cases of discriminatory persecution, individuals are followed based on possession of a protected characteristic, which sometimes leads to occasional mismatching. However, activists, members of NGOs, investigators, political dissidents are targeted due to their personality, which makes such kind of surveillance narrowly tailored and purely deliberate. For example, a well-known Pegasus software is aimed at journalists, human rights defenders and opposition politicians,[159] profiling them and facilitating the systematic repressions in Israel. Conducting a large-scale assessment of this system, Al-Haq noticed an alarming tendency to share malicious technologies

[156] *Friedl v Austria* App no 15225/89 (EComHR, 7 December 1992), paras 13-14.

[157] UNCHR, General Comment №37 'Article 21 (Right to Peaceful Assembly)' (2020) UN Doc CCPR/C/GC/37, para 61.

[158] UNCHR 'Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association on exercise of the rights to freedom of peaceful assembly and of association as essential to advancing climate justice' (2021) UN Doc A/76/222, paras 34, 85-86.

[159] 'Use of spyware to surveil journalists and human rights defenders. Statement by UN High Commissioner for Human Rights Michelle Bachelet' (UN, 19 July 2021) <https://cutt.ly/eJ1Xhs9> accessed 10 June 2022.

among States inclined to misuse them to silence unfavourable voices and track dissidents.[160] Also, the relative efficiency of the FRT surveillance leads to its massive application even in the States, which declare themselves as complying with the human rights requirements. In 2020, the participants of the famous US Black Lives Matter protest were subjected to such technologies, which has been proven by arrest warrants addressed several weeks after the public gathering.[161]

A global response to these situations manifested in numerous calls to review governmental surveillance policies, abstaining from the application of highly intrusive technologies. Firstly, statements condemning the FRT were produced on the civil society level with a further expansion to international governmental organisations. Consequently, the key stakeholders are trying to develop a unified response regarding the legality of such technologies and the potential for their application in limited circumstances. Although there is no comprehensive binding document on a global scale yet, the existing initiatives are nevertheless worth analysing.

1.4. International initiatives on the regulation of the facial recognition technologies

A complex analysis of the threats and pitfalls in the FRT surveillance triggered an extensive debate around its regulation, restrictions for its usage and guarantees to be applied. Probably the most detailed and comprehensive research, covering national practices from all over the globe, was done by the UN Special Rapporteur dealing with the right to privacy. In the 2018 Draft Legal Instrument, professor Joseph Cannataci perfectly outlined the framework by defining smart surveillance systems via autonomous decision-making and actuation, limiting covert and overt surveillance measures to the competence of specifically authorized State organs, thus disabling

[160] Al-Haq, 'Spyware Surveillance of Palestinian Human Rights Defenders' (*Al-Haq*, 8 November 2021) <https://cutt.ly/TJ1Ck66> accessed 10 June 2022.

[161] Amnesty International, 'Surveillance city: NYPD can use more than 15,000 cameras to track people using facial recognition in Manhattan, Bronx and Brooklyn' (*Amnesty International*, 3 June 2021) <https://cutt.ly/PJ1CIu9> accessed 10 June 2022.

private-sector monitoring and collection of data.[162] Although addressing the general requirements of transparency, oversight and effective remedies, he specifically stressed the impossibility of deploying mass surveillance systems without an independent external human rights impact assessment, as well as ensuring that the error rate does not fall below the accepted threshold.[163] Notwithstanding the listed limitation still cannot amount to outlawing FRT surveillance, they became a solid start for a tendency of restricting AI-driven surveillance. Particularly, the requirements towards the technical requirements and characteristics, outer conclusions on human rights compliance, and numerous procedural guarantees hinted at a complicated route for the deployment of the FRT surveillance. Following this Draft Legal Instrument, the UN Special Rapporteur's approach turned out to be even more restrictive with far-reaching criticism of the discriminatory potential of FRT and affect recognition surveillance.[164]

In 2020, a similar position was pronounced by the UN General Assembly, which openly called AI-driven surveillance a particularly dangerous phenomenon, which requires large amounts of private data to be fed, while providing few guarantees against abuse and chilling effect.[165] As a result, it exhorted the States to review existing practices and procedures on profiling, automated decision-making, machine learning and biometric technologies, granting individuals suffering from unlawful surveillance an effective remedy. It became a precondition for a detailed analysis of such surveillance's devastating impacts in the 2020 Report of the UN High Commissioner for Human Rights Michelle Bachelet. Particularly, the FRT surveillance is described as a system, that "*despite remarkable accuracy gains in recent years, still prone to errors*",[166] perpetuating discrimination on gender, racial and other grounds. This, in

[162] UN Special Rapporteur on the right to privacy, Draft Legal Instrument on Government-led Surveillance and Privacy (Managing Alternatives for Privacy, Property and Internet Governance, 10 January 2018) 8, 11-12, 15-17.

[163] *Ibid*, 21, 23.

[164] UNCHR 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on surveillance and human rights' (2019) UN Doc A/HRC/41/35, para 12.

[165] UNGA 'Resolution 75/176 on the right to privacy in the digital age' (2020) UN Doc A/RES/75/176, paras 7-8.

[166] UNCHR 'Report of the United Nations High Commissioner for Human Rights on impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests' (2020) UN Doc A/HRC/44/24, paras 31-32.

turn, drove the UN High Commissioner for Human Rights to question the necessity and proportionality of deploying the FRT for security purposes during the public gatherings *per se*,[167] irrespective of the circumstances of surveillance, which became the first official doubting of the FRT's general lawfulness. Even if in absence of an absolute treaty or customary prohibition the States are resorting to such surveillance mechanisms, they shall limit it only to targeted individuals, immediately removing all other segments of data. The issue of the technical possibility to conduct surveillance in this manner remains disputable though.

The UN response to the FRT surveillance proceeded with the 2021 UNESCO Recommendation on the Ethics of AI, which specifically addressed transparency of biometrics processing, the right to control and erase records of personal data, dwelled upon the need for adequate supervision and impact-assessment.[168] However, an important novelty implied a proposal to ban social scoring and mass surveillance, including AI-driven systems, which are overly invasive and cannot fit into the mechanism of legal accountability.[169] Moreover, the most technologically advanced States were called upon to conduct a meaningful exchange of information to ensure fairness and equality throughout the whole AI system life cycle.[170] The UNESCO recommendations became the first comprehensive document on AI-driven systems, providing concrete steps for addressing the risks and adverse impact of such technologies. Subsequently, an even more restrictive approach was proposed by the UN Special Rapporteur, who expressed serious concerns regarding real-time biometric recognition, potential profiling and grave breaches of privacy.[171] Accordingly, the UN Special Rapporteur encouraged to establish a general moratorium on AI systems, the

[167] *Ibid*, para 35.

[168] UNESCO, 'UNESCO member states adopt the first ever global agreement on the Ethics of Artificial Intelligence' (UNESCO, 25 November 2021) <https://cutt.ly/yJ1NKOt> accessed 10 June 2022.

[169] UNESCO, Recommendation on the ethics of artificial intelligence (UNESCO, 2021), paras 26, 36, 72.

[170] *Ibid*, para 28.

[171] UNCHR 'Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age' (2021) UN Doc A/HRC/48/3, paras 26-27.

risks for human rights in which significantly overweigh the benefits,[172] while the States possessing such technologies shall abstain from distributing them to the countries, where abuses against vulnerable groups might take place.

Except for the centralized UN efforts, regional human rights bodies also made a significant contribution to restricting the wide-scale application of intrusive surveillance techniques. The CoE legal framework comprises several acts addressing the standards for deployment of modern technologies in the security sphere, among which two documents specifically concern AI-driven systems and the FRT. The 2020 Recommendation on the human rights impacts of algorithmic systems stipulates that the dangers stemming from digital tracking of persons based on their identity and behaviour exist throughout the entire life-cycle of AI-driven surveillance tools.[173] Based on these recommendations, in 2021 the CoE produced a more specified Guideline on Facial Recognition. Advancing the standards of algorithms' reliability, accuracy and traceability, this document also proposes a moratorium on the application of the FRT surveillance in uncontrolled environments given the serious risks of mismatching, abuses and a high false positives rate.[174] An even more restrictive approach is maintained toward affect recognition. Finally, the Guidelines specifically mention establishing a supervisory authority and consulting it whenever an initiative to design or deploy the FRT surveillance emerges.[175] Commenting on the necessity of the Guidelines, the CoE Secretary General called the FRT suitable for both "*helping to navigate obstacles in everyday lives"* and *"empowering state authorities … to monitor and control important aspects of our lives – often without our knowledge or consent*",[176] which makes the balancing exercise and legal regulation not an option, but a pressing need to effectively safeguard the rights at stake.

---

[172] *Ibid*, para 59(c)(d).

[173] Council of Europe Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems (2020), para 4.

[174] Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108), 'Guidelines on facial recognition (2021)' (CoE, 2021) 5.

[175] *Ibid*, 8.

[176] CoE, 'Facial recognition: strict regulation is needed to prevent human rights violations' (CoE, 28 January 2021) <https://cutt.ly/vJ1MVWO> accessed 10 June 2022.

In response to the growing debates, the CoE Committee of Ministers established the Ad hoc Committee on Artificial Intelligence,[177] mandated to draft an international instrument addressing issues of AI regulation and ethics. The Committee organised the multistakeholder consultations, distributing a questionnaire among the States, NGOs, academics, and independent experts. The FRT for law enforcement was considered as positively impacting human rights by 43 respondents against being called one of the greatest threats for them by 164 respondents.[178] Interestingly, the benefits of the FRT were marked primarily by the State sector, while risks and dangers were mostly outlined by human rights defenders and academics, who stressed systems' biases, disregard for cultural distinctions and serious psychological harm to affected individuals.[179] As a result, the respondents relatively equally shared their voices on the options of banning the FRT surveillance in public places and allowing it, with a slightly bigger number of individuals considering the full-scale moratorium as an appropriate response.

Another jurisdiction extensively elaborating on the FRT surveillance is the EU legal framework, where numerous detailed regulatory proposals can be identified throughout the last couple of years. Starting from the EDPB Guidelines on video surveillance, the issues of biases based on different demographics and pre-existing societal prejudices were addressed in line with the notion of reasonable expectations of the data subject regarding the potential surveillance and processing of one's biometrics.[180] Importantly, the Guidelines detailed the issues of proper notifications of surveillance (including unambiguous mentioning of the area covered by the camera), also clarifying that entering a marked monitored area does not suffice as informed consent in situations, where one is needed for a recording.[181] Lastly, the document dwells upon the rectification of biometrics and anonymization of personal data,

[177] Ad hoc Committee an Artificial Intelligence (CAHAI), Deputies' 1353rd meeting (CM/Del/Dec(2019)1353/1.5) (11 September 2019 - 31 December 2021).

[178] CAHAI, 'Analysis of the Multi-Stakeholder Consultation' (CAHAI, 23 June 2021), 19, 25.

[179] *Ibid*, 26-27.

[180] EDPB Guidelines 3/2019 on processing of personal data through video devices (2020), paras 4, 36.

[181] *Ibid*, paras 46, 77, 113.

stressing that "*the constitution of databases could represent an equal if not even bigger threat*" than video surveillance itself.[182] Accordingly, the requirements include effective protection of data banks, including via noise-additive methods, irreversible blurring of odd templates and removal of materials, processing of which no longer serves a legitimate purpose. Compared to other similar regulations on the European level, these Guidelines provide not only a general outline of technical weaknesses but also a line of solutions relevant for developers and deployers of video surveillance systems. Moreover, contrary to a mere criticism expressed on the UN level, the EDPB proposes the States consider alternatives to the FRT surveillance, especially where their application can be substituted by less intrusive technologies without substantial harm to the end sought.

Further, the European Commission White Paper on AI became a supplementary material to the video surveillance guidelines comprehensively addressing the FRT.[183] Publication of the White Paper caused a chain reaction within the EU legal framework, leading to the appearance of the Resolution from the European Parliament, numerous public statements, research and open calls to impose a moratorium on the FRT surveillance until the development of the strict rules and standards.[184] Finally, the discourse ended up with the drafting of the Proposal for a regulation of AI by the European Commission, proving the strict and clear limitations on the FRT use.

The Proposal divided AI-driven technologies into four categories based on a solid risk methodology, prohibiting or restricting their use depending on the threat to human safety and fundamental rights. For instance, social scoring and categorisation are prohibited under any circumstances due to the unacceptable riskiness and inflicting groundful rights and dignity of persons.[185] Real-time biometric surveillance, allowing

---

[182] *Ibid*, paras 84, 90, 103.

[183] European Commission White Paper on Artificial Intelligence - a European approach to excellence and trust (2020) COM(2020)65final, 21.

[184] Tambiama Madiega and Hendrik Mildebrath, *Regulating facial recognition in the EU* (EPRS, 2021) 23, 25.

[185] European Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (AI Act) and Amending Certain Union Legislative Acts (2021) COM/2021/206final, Article 5; European Commission Explanatory Memorandum to AI Act (2021) COM/2021/206final, para 5.2.2.

for identification occurring "*instantaneously, near-instantaneously or in any event without a significant delay*", was classified as a high-risk AI system.[186] Accordingly, it was permitted for usage only based on the authorisation of the supervisory body in three "*exhaustively listed and narrowly-defined situations*", where public interest outweighs potential dangers.[187] They involve a targeted search for the victims of a crime (including children); prevention of imminent and substantial threats to life or property of individuals or averting the terrorist attacks; and detection, localisation, identification or prosecution of perpetrators or suspects of criminal offences. Nowadays this Proposal remains one of the most detailed and comprehensive expected regulations, which is based on a correspondence of threats and benefits of the FRT. Moreover, it enables the systems developers and deployers to operate in legal terms, avoiding double qualifications of the same systems due to dissimilarities in legal and technical notions.

However, even such position against the FRT surveillance was considered overly soft. Commenting on this Proposal, the EDPB and the EDPS stressed that intrusive forms of surveillance, negatively affecting human dignity, must be classified as prohibited under any circumstances.[188] Among the provided examples these bodies paid particular attention to remote biometric identification systems and the FRT surveillance undermining the expectations of anonymity in public spaces. The same restriction relates to emotion recognition and tools categorizing individuals from their biometrics. A critical response to the FRT surveillance was also expressed by the OSCE, which called it a significant challenge to democratic values. Specifically, it stated that facial and emotion recognition technologies were not "*developed under a human rights-centred approach*", thus requiring strict limitations and safeguards.[189]

---

[186] European Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (AI Act) and Amending Certain Union Legislative Acts (2021) COM/2021/206final, para 8 of the Preamble.

[187] *Ibid*, paras 18-19 of the Preamble, Article 5, Annex III.

[188] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (AI Act) (18 June 2021), paras 28, 30, 32.

[189] OSCE, 'Summary Report: A Human Rights-Centred Approach to Technology and Security' (OSCE, 8 November 2019) 1-2.

Similarly, the OECD Principles on AI outlined a need to respect human rights, establishing a prohibition on technologies deliberately or accidentally infringing human rights.[190] Thus, most governmental organisations are inclined to directly or indirectly oppose the large-scale application of the FRT surveillance given the high risks and lack of safeguards.

Prominent scholars, researchers from both legal and technical fields, independent experts and other academics have also expressed their worries about the tendency of rapid and uncontrolled deployment of the FRT. One of the most extensively researched topics is a bias level, which leads most scholars, including Leslie, Christakis and Becuywe, to consider it rather inflicting than useful for real-life application, especially in absence of any fixed and unified standards.[191] Moreover, the conclusions of the academics, specialised in the technical field, substantiate the dismay regarding the unreliability of the FRT and their unpredictable decisions in cases, where machine and deep learning are deployed.[192] Akin to that, according to Kostka, Steinacker and Meckel, public perception of the FRT surveillance significantly depends on the level of their knowledge about operations of such technology and its impact on their rights.[193] The more individuals know about surveillance, the better protection against abuses they expect, which, in turn, can serve as an efficient instrument for combating legal nihilism among the population. Even those scholars, who generally support the idea of implementing the FRT surveillance, usually stress that limitations are needed for cases of minorities and minors,[194] while the deployment of such systems without an adequate legal framework anyway becomes an abusive practice. Respectively, there

---

[190] OECD Principles on AI <https://cutt.ly/VJ16vPp> accessed 10 June 2022, Principle 1.2.

[191] David Leslie, 'Understanding bias in facial recognition technologies' (The Alan Turing Institute, 2020) 24-25; Theodore Christakis and Mathias Becuywe, 'Pre-Market Requirements, Prior Authorisation and Lex Specialis: Novelties and Logic in the Facial Recognition-Related Provisions of the Draft AI Regulation' (*European Law Blog*, 4 May 2021) <https://cutt.ly/0J0Wdf1> accessed 10 June 2022.

[192] Lucas Introna and Helen Nissenbaum, 'Facial Recognition Technology: A Survey of Policy and Implementation Issues' (Lancaster University Management School Working Paper, 2009) 44-47.

[193] Genia Kostka, Léa Steinacker and Miriam Meckel, "Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States" (2021) 30(6) Public Understanding of Science 671, 675.

[194] Jawahitha Sarabdeen, "Protection of the rights of the individual when using facial recognition technology" (2022) 8(3) Helyon 1, 8.

is a relatively unified position regarding the outrageously abusive practice of applying the FRT surveillance in unregulated legal environments, especially where technologies themselves are far from perfect in their effectiveness rate.

NGOs and other civil society actors, in their turn, became the engines for banning the FRT surveillance. Particularly, they delivered numerous public statements,[195] drafted amicus curiae to the competent human rights bodies,[196] prepared reports on the States' breaches of human rights due to the FRT application,[197] launched large-scale social campaigns[198] and supported numerous local organisations aimed at the advocacy of banning biometric surveillance. The efforts became relatively effective, when they reached an international level with a campaign of Reclaim Your Face,[199] uniting various stakeholders at the EU level and beyond. These human rights defenders' contributions have led to a shift in attitude to the FRT among the largest developers, *i.e.* Facebook has restricted facial recognition in photos downloaded on the platform.[200] Although a single step probably cannot change a tendency toward deployment of surveillance by authoritarian governments, it might, at least, decrease their capacity to process biometrics unlawfully obtained from social media. Furthermore, general concern around the FRT jeopardizing human rights deter numerous States with a well-developed AI industry from the deployment of such surveillance mechanisms.

---

[195] Joy Buolamwini, 'We Must Fight Face Surveillance to Protect Black Lives' (*OneZero*, 3 June 2020) <https://cutt.ly/FJ0nuvt> accessed 10 June 2022; ACLU, 'Coalition letter calling for a federal moratorium on face recognition' (*ACLU*, 3 June 2019) <https://cutt.ly/KJ0nbsR> accessed 10 June 2022.

[196] '13 Principles for a Human Rights Respecting State Surveillance Framework' (*EFF*, 10 September 2020) <https://cutt.ly/aJ0vDqj> accessed 10 June 2022; Privacy International, 'PI's submission to the UN Human Rights Committee regarding France's compliance with ICCPR' (*Privacy International*, 20 July 2021) <https://cutt.ly/TJ0b4i4> accessed 10 June 2022.

[197] Carolina Goncalves Berenger, Laura O'Brien and Peter Micek, 'OSCE Mission to Skopje supports face recognition on-site training for border police officers' (Access Now, 10 September 2020) <https://cutt.ly/iJ0voTg> accessed 10 June 2022.

[198] Amnesty International, 'Ban dangerous facial recognition technology that amplifies racist policing' (*Amnesty International*, 26 January 2021) <https://cutt.ly/WJ0zAbF> accessed 10 June 2022; Access Now, 'Open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance' (*Access Now*, 21 December 2021) <https://cutt.ly/dJ0zX1Q> accessed 10 June 2022.

[199] Reclaim Your Face campaign <https://cutt.ly/xJ0xuFm> accessed 10 June 2022.

[200] Adi Robertson, 'Facebook is shutting down its Face Recognition tagging program' (*The Verge*, 2 November 2021) <https://cutt.ly/qJ0xjWe> accessed 10 June 2022.

Notwithstanding extensive criticism addressed by prominent scholars, local authorities and international policy-making bodies regarding the safety of the FRT surveillance, such systems are actively implemented in practice. For instance, the UN Special Rapporteurs frequently express their concerns regarding threats to human rights stemming from the FRT surveillance. Simultaneously, the UN Security Council openly advocated for the States to "*develop and implement systems to collect biometric data, which could include … facial recognition … to responsibly and properly identify terrorists*",[201] implying approval of the FRT irrespective of their indistinctive character and collateral effect upon individuals unrelated to terrorism. A similar approach is maintained by the OSCE, which itself contributed to the education of local police officers on the FRT surveillance against transnational organized crime within Mission to Skopje.[202] The Venice Commission in the Guidelines on Freedom of Peaceful Assembly although condemning the negative impact of the FRT, tracking and breach of anonymity, still insists on the development of the legislative framework for the deployment of listed tools rather than their absolute prohibition.[203] Hence, the Venice Commission decided to adopt a milder approach than most human rights bodies, leaving the space for adjusting domestic legislation to the FRT and imposing technical limitations, not an absolute ban.

Another emblematic example of a dual attitude is the EU legal space, where a strong opposition towards the FRT surveillance on the organisational level is counterbalanced by relative negligence towards detected dangers within the national jurisdictions. Namely, the EU Member States massively deploy complex surveillance systems to monitor and filter out asylum seekers, migrants and persons threatening national security.[204] Generally, the problem exists where the mandates of the institutions governing the security and defence do not overlap with the competence of

[201] UNSC Resolution 2396 (2017) UN Doc S/RES/2396(2017), para 15.

[202] OSCE, 'OSCE Mission to Skopje supports face recognition on-site training for border police officers' (OSCE, 30 November 2016) <https://cutt.ly/oJ0c2RY> accessed 10 June 2022.

[203] Venice Commission and OSCE/ODIHR Guidelines on Freedom of Peaceful Assembly (3rd Edition) (2019) CDL-AD(2019)017, paras 71, 172.

[204] European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement* (FRA, 2020) 14.

the bodies dealing with human rights matters. For instance, Interpol concentrates on the apprehension of criminals on the watchlist, while human rights protection remains a secondary issue. Accordingly, there is no balanced approach to the FRT application by the bodies with different priority tasks, not even mentioning different structures within the same organization.

Nowadays the FRT developers and States deploying such technologies are striving to balance the security interests with relative protection of individuals, experiencing the surveillance effects. At the same time, the issue of technical, procedural and time difficulties are often considered. For example, experts describe non-AI facial recognition as ineffective, overly time-consuming and inaccurate for the performance of law enforcement tasks.[205] Simultaneously, the AI-driven programs are often filled with technical biases, thus forcing the States to choose between efficiency and human rights protection. However, indifference towards security issues undermines the democratic values in the same vein neglection of human rights does. Hence, a reasonable solution for the security and defence problem is still needed with consideration of the least intrusive and most effective option.

***

Despite having numerous forms and manifestations, mass surveillance remains a very disputable phenomenon, described as a highly intrusive practice by most international judicial and policy bodies. Although the recent ECtHR practice does not outlaw mass surveillance as such, priority still must be given to targeted monitoring and tracking practices.

AI-driven biometric surveillance usually undermines the right to privacy, overprocessing personal data and being incapable of meaningfully controlling amounts of information loaded therein from various sources. Its operation breaches all existing data protection standards if the FRT tools are deployed without authorization and periodic review of specialized supervisory bodies. A reasonable concern is also raised regarding the violation of the prohibition on discriminatory treatment, given numerous

[205] The Jerusalem Post Staff, 'Ex-Mossad head: AI facial recognition tech superior to fingerprinting' (*The Jerusalem Post*, 21 December 2021) <https://cutt.ly/5J18aga> accessed 10 June 2022.

flaws occurring due to the underrepresentation of vulnerable and marginalized groups. Moreover, the application of the FRT surveillance negatively impacts other rights and freedoms, causing a chilling effect on the freedom of expression and assembly.

Nowadays most stakeholders are paying significant attention to the threats stemming from biometric identification, calling for its suspension until a legal framework is developed by the authorized international bodies. Hence, a global response in recent years is shifting to restriction of real-time FRT surveillance with a tendency towards the absolute prohibition of such technology given its legal risks and technical unreliability.

CHAPTER 2.
EXISTING DOMESTIC PRACTICES REGULATING THE FACIAL RECOGNITION TECHNOLOGIES

Active deployment of the FRT is gaining the global scale with no region being set aside, *i.e.* AI-driven surveillance is widely applied in Israel, Singapore, the South African Republic, Belgium, Hungary, South Korea and many other States.[206] Intensive competition between the global producers, such as the US, China and Japan,[207] force the States to increase investments in the FRT surveillance industry with a subsequent need of testing newly developed systems.

Being disputable, AI-driven surveillance, accompanied by the lack of specialised regulation, has led to numerous privacy concerns.[208] This issue became especially sharp for the liberal democracies, which according to Feldstein's research, deploy the FRT surveillance in 10% more cases than autocratic or quasi-autocratic governments.[209] Contrastingly to the latter, though, democracies are obliged to reason their decisions to apply AI-driven tools and ensure the existence of safeguards. Albeit, the requirement of reasoning does not always mean its practical presence, leading to extensive criticism of the States with a high human rights record for "overcaring" about the security matter. For instance, the EU States are frequently described as hiding beyond the counterterrorism notions to conduct large-scale AI-driven surveillance.[210] For the purposes of this thesis, five States with different approaches to the deployment of the

[206] Moussa Sangare, 'Mass Surveillance in the Post-Covid-19 World: A Test for the United Nations' (*Global Policy*, 18 May 2020) <https://cutt.ly/qJ0RTR0> accessed 10 June 2022; Tony Roberts and others, Surveillance Law in Africa: a review of six countries (Institute of Development Studies, 2021) 21-35; 'У Південній Кореї протестують технологію розпізнавання облич, щоб відстежувати хворих на Covid' (*Українська правда*, 13 December 2021) <https://cutt.ly/5J0R85X> accessed 10 June 2022; Will Schrepferman, 'Supervising Surveillance: Applying International Law to the Global Surveillance State' (*Harvard International Review*, 11 November 2020) <https://cutt.ly/oJ0TyDP> accessed 10 June 2022.

[207] Moussa Sangare, 'Mass Surveillance in the Post-Covid-19 World: A Test for the United Nations' (*Global Policy*, 18 May 2020) <https://cutt.ly/qJ0RTR0> accessed 10 June 2022.

[208] '13 Principles for a Human Rights Respecting State Surveillance Framework' (*EFF*, 10 September 2020) <https://cutt.ly/aJ0vDqj> accessed 10 June 2022.

[209] Steven Feldstein, 'The Global Expansion of AI Surveillance' (Carnegie Endowment for International Peace, 2019) 10.

[210] Wiebke Lamer, "From sleepwalking into surveillance societies to drifting into permanent securitisation: Mass surveillance, security and human rights in Europe" (2017) 1 Global Campus Human Rights Journal 393, 394.

FRT surveillance were chosen to check whether the risks vary depending on the general level of human rights protection.

2.1. The Chinese practice

China, remaining the leader among the countries deploying the FRT, has nine cities on the list of the 20 most-surveilled cities in the world.[211] Moreover, the FRT is also used by the State authorities for verification of the ID photos and for cross-checking of images on different documents, which is done by such applications as Face++.[212] However, the main pitfall is that most companies are closely supervised by the central government, simultaneously being the largest producers of the technology for Uganda, Algeria, Serbia and numerous States in Central Asia.[213] To exemplify, the New York Times investigation revealed that Ecuadorian Chinese-made surveillance comprises 16 monitoring centres with 3,000 people being employed to operate the systems.[214] Similarly, Chinese company Huawei provides AI-driven surveillance in more than 50 States worldwide.[215] This, in turn, proves the wide coverage and impact of Chinese technologies on the privacy, security, and labour market of numerous States. Accordingly, the suspicion regarding the potential access of the Chinese authorities to the biometrics collected beyond its borders is not groundless, making them unreliable for mass use. Moreover, since at some markets the Chinese producers gain a monopolistic position, lowering prices and providing the most beneficial proposal for the local governments. Hence, the developing States often have no reasonable alternatives to the FRT produced in the authoritarian regime.

---

[211] Charlie Campbell, "The Entire System Is Designed to Suppress Us.' What the Chinese Surveillance State Means for the Rest of the World' (*Time*, 21 November 2019) <https://cutt.ly/3J0GTEy> accessed 10 June 2022.

[212] Amanda Lentino, 'This Chinese facial recognition start-up can identify a person in seconds' (*CNBC*, 16 May 2019) <https://cutt.ly/yJ0GG7X> accessed 10 June 2022.

[213] Loprespub, 'Taming State Surveillance: Reconciling Camera Surveillance Technology with Human Rights Obligations' (*Hillnotes*, 16 March 2020) <https://cutt.ly/IJH2TfW> accessed 10 June 2022; Steven Feldstein, 'The Global Expansion of AI Surveillance' (Carnegie Endowment for International Peace, 2019) 2.

[214] Paul Mozur, Jonah M Kessel and Melissa Chan, 'Made in China, Exported to the World: The Surveillance State' (*The New York Times*, 24 April 2019) <https://cutt.ly/sJ0HtHL> accessed 10 June 2022.

[215] Steven Feldstein, 'The Global Expansion of AI Surveillance' (Carnegie Endowment for International Peace, 2019) 1.

As regards the Chinese environment itself, the "Sharp Eyes" project implies the installation of approximately 600 million the FRT cameras,[216] aiming to cover 100% of public spaces.[217] According to the recent estimates, such several cameras will allow the State to recognize 1,4 billion people in 1 second. Moreover, the self-learning capacities of most FRT will enable them to rapidly adjust to the changing surroundings. For instance, in response to COVID pandemics and the obligation to wear face coverings in public places, the Chinese developers created the systems able to identify persons in masks.[218] Since the COVID restrictions significantly limited the freedom of movement, surveillance was widely used for tracking individuals and identifying those, who breach the quarantine regime, may be the carrier of the virus or contacted such people.[219] As several studies show, such companies as Huawei are frequently developing intrusive techniques tailored to the needs of the authoritarian governments, while further implementing them in other States (as happened with the FRT adjusted to facial coverings).[220] Thus, not only promotion of allegedly governmentally-controlled technologies is conducted, but also the general advocacy of the FRT surveillance as a tool for maintaining security and public order.

Although the application of AI-driven surveillance intensifies, the Chinese regulation in this area is far from perfect. Being indirectly regulated by the Cybersecurity Law, providing for the standards for the processing of the biometrics, the FRT is not specifically framed in any national regulatory act.[221] In this respect, the national security laws also partly cover the FRT surveillance, expanding the government's ability of massive monitoring the Hong Kong citizens to halt political

---

[216] Тетяна Авдєєва, 'Чи легально встановлювати на міських вулицях камери із системою розпізнавання облич?' (*ЦЕДЕМ*, 30 June 2021) <https://cutt.ly/5J0HhBO> accessed 10 June 2022

[217] Dave Gershgorn, 'China's 'Sharp Eyes' Program Aims to Surveil 100% of Public Space' (*CSET*, 2 March 2021) <https://cutt.ly/yJ0HbV4> accessed 10 June 2022

[218] Ольга Кротовська, '"Великий брат спостерігає": в Китаї розробили систему, яка розпізнає обличчя навіть у масках' (*PG*, 10 March 2020) <https://cutt.ly/3J0HIOj> accessed 10 June 2022

[219] Moussa Sangare, 'Mass Surveillance in the Post-Covid-19 World: A Test for the United Nations' (*Global Policy*, 18 May 2020) <https://cutt.ly/qJ0RTR0> accessed 10 June 2022

[220] Steven Feldstein, 'The Global Expansion of AI Surveillance' (Carnegie Endowment for International Peace, 2019) 14

[221] Tambiama Madiega and Hendrik Mildebrath, *Regulating facial recognition in the EU* (EPRS, 2021) 33

subversion.[222] Only in 2021, the National Information Security Standardisation Technical Committee of China shared a draft of the Security Requirements of Facial Recognition Data,[223] setting recommendations for the FRT collection of personal data. However, the absence of solid regulation leaves the standardisation of the AI sphere primarily for the self-regulatory bodies and the industry itself, making technologies different in security and human rights compliance rates. Notwithstanding China's Supreme People's Court decision, providing for the need for consumers' consent to use the FRT in supermarkets, airports and other commercial venues,[224] it still is inapplicable to the State's practices. In contrast, the distinguishing feature in this area is the mandatory access of the State to the producers' networks and the requirement of opening the source code or encryption keys upon the authorities' request,[225] which makes personal data permanently accessible to the Chinese law enforcement. This rule Since no targeted regulation for the FRT is drafted, the citizens remain deprived of any procedural safeguard against abuses.

One of the most well-known abusive FRT applications, practised by the Chinese authorities, is the identification of the Uighur minority for their further apprehension and persecution.[226] All new FRT developments are *de facto* tested on Uighur people,[227] *e.g.* previously criticised Huawei developed the FRT able to trigger "Uighur alarm" oppressing the minority harder than ever before.[228] The same attitude is maintained towards the Turkish Muslims, who are often subjected to discriminatory and inhumane

---

[222] Will Schrepferman, 'Supervising Surveillance: Applying International Law to the Global Surveillance State' (*Harvard International Review*, 11 November 2020) <https://cutt.ly/BJNwJvV> accessed 10 June 2022.

[223] Hunton Andrews Kurth, 'China Publishes Draft Security Standard on Facial Recognition' (*National Law Review*, 29 April 2020) <https://cutt.ly/7J0H13A> accessed 10 June 2022.

[224] Eva Dou, 'China built the world's largest facial recognition system. Now, it's getting camera-shy' (*The Washington Post*, 30 July 2021) <https://www.washingtonpost.com/world/facial-recognition-china-tech-data/2021/07/30/404c2e96-f049-11eb-81b2-9b7061a582d8_story.html> accessed 10 June 2022.

[225] Paul Mozur, 'China's Internet Controls Will Get Stricter, to Dismay of Foreign Business' (*The New York Times*, 7 November 2016) <https://cutt.ly/3J0JfoF> accessed 10 June 2022.

[226] Alfred Ng, 'How China uses facial recognition to control human behavior' (*CNET*, 11 August 2020) <https://cutt.ly/1J0C4Vq> accessed 10 June 2022.

[227] Jane Wakefield, 'AI emotion-detection software tested on Uyghurs' (*BBC News*, 26 May 2021) <https://cutt.ly/tJ0VqON> accessed 10 June 2022.

[228] Jurica Dujmovic, 'Opinion: Facial-recognition technology is one of the biggest threats to our privacy' (*MarketWatch*, 27 December 2021) <https://cutt.ly/OJVrHq8> accessed 10 June 2022.

treatment following their arrests based on the FRT surveillance results.[229] The justification for such actions provided by the Chinese government in the fight against "*separatism, terrorism, and extremism*". Recently, the authorities have implemented the emotion recognition systems, which are more intrusive into privacy and capable of breaching the right not to self-incriminate.[230] Akin to that, the Chinese authorities have other AI-driven surveillance tools, which often are mutually interconnected. For instance, the bid-data platform Police Cloud indiscriminately collects personal data from any accessible source, such as supermarkets and health records. Most biometrics also are incorporated into the systems of social scoring,[231] based on which the Chinese people can be rejected in permission to leave the State or organise public events. Personal data of individuals, violating the social and legal rules, are often located on billboards for public shaming.[232] Respectively, such practices have a devastating influence on people's identity formation, creating a chilling effect not only on a limited group of rights but on the integrity of the Chinese as human beings.

Another misuse of the FRT implies controlling the tourists' compliance with the quarantine requirements via the MorChana application, which notifies authorities within 30 minutes after leaving the designated observation zone.[233] Being connected to the general surveillance database, it contributes to mass monitoring and tracking of individuals, adding the facial templates of foreigners to the general banks with biometrics. As a result, the profiling operations extend far beyond the Chinese borders, while a collection of data from abroad systems enables training recognition functions of the FRT more effectively. Given the fact that a primary use of such systems implies malicious aims, the higher efficiency is – the more harm can be done.

---

[229] Kenneth Roth and Maya Wang, 'Data Leviathan: China's Burgeoning Surveillance State' (*HRW*, 16 August 2019) <https://cutt.ly/tJ0VqON> accessed 10 June 2022.

[230] Article 19, 'Emotion Recognition Technology Report' (*Article 19*, 2021) <https://cutt.ly/tJ0Vdrg> accessed 10 June 2022.

[231] Олександр Мельник, 'Китай став першою країною планети, де поліції видали смарт-окуляри' (*Na Chasi*, 8 February 2018) <https://cutt.ly/8J2ErrE> accessed 10 June 2022.

[232] Paul Mozur, 'Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras' (*The New York Times*, 8 July 2018) <https://cutt.ly/gJ2EkPk> accessed 10 June 2022.

[233] The Phuket, 'MorChana to have face recognition integrated, warn officials of foreigners outside designated Sandbox zones' (*The Phuket News*, 10 October 2021) <https://cutt.ly/5J2ED8P> accessed 10 June 2022.

Importantly, numerous technologies have also been developed or modernized by the European companies (especially, German, French and Swedish ones), which have been criticised for supplying the authoritarian regimes with effective tools for discrimination and humiliation. In this manner, the European developers have been described as "*a multi-billion Euro industry that is flourishing by selling its wares to human rights abusers*",[234] which significantly affected their reputation in the more democratic States. Although numerous systems do not work as intended,[235] they still make it possible to track specific individuals and massively profile persecuted minorities. Thus, a horrific pattern of human rights abuses in China is based on both national and European contributions, which only strengthen the oppressive policies.

The responses to the Chinese practices are polarized. The initiative to finally build the trade and infrastructure network connecting Asia, Europe, Africa, and beyond (Belt and Road Initiative) drives most stakeholders into cooperation with China.[236] Although this program provides for active use of AI technologies for smart cities' infrastructure, data centres, cable networks and satellites, Chinese loans and sharing of technological developments overweigh the risks of potential interference and unlawful data collection in the eyes of the trading partners. For instance, China is actively promoting the FRT surveillance across the African States in exchange for collecting biometrics in the African region.[237] Accordingly, by deploying Chinese AI-driven monitoring systems worldwide, the government can *de facto* control individuals beyond its borders and lawfully obtain the data samples of people of colour to enhance the FRT capacities.

On the other hand, numerous governments establish export control on the FRT surveillance to avoid their use for violation of the minority rights. For example, Japan developed strict human rights requirements for the export of AI-driven technologies

---

[234] Amnesty International, 'EU companies selling surveillance tools to China's human rights abusers' (Amnesty International, 21 September 2020) <https://cutt.ly/JJ2RkDt> accessed 10 June 2022.

[235] Kenneth Roth and Maya Wang, 'Data Leviathan: China's Burgeoning Surveillance State' (*HRW*, 16 August 2019) <https://cutt.ly/tJ0VqON> accessed 10 June 2022.

[236] Huimin Li, Human Rights in the Age of Surveillance: China's Expansion of Technological and Normative Power (New York University, May 2020) 47.

[237] Lynsey Chutel, 'China is exporting facial recognition software to Africa, expanding its vast database' (Quartz Africa, 25 May 2018) <https://cutt.ly/TJ0VLgg> accessed 10 June 2022.

abroad.[238] Similarly, large companies, such as Amazon and Microsoft are trying to ban the FRT to prevent it from getting into the wrong hands.[239] However, the availability of the basic technology makes these efforts rather declaratory, showing the goodwill of the actors to abstain from human rights breaches, rather than practically effective.

Lastly, the UN Special Rapporteur has expressed particular concern regarding the Chinese use of the FRT, stressing a need to enhance human rights protection.[240] Unfortunately, little influence can be done by the soft power of the UN institutions for safeguarding vulnerable and marginalized groups in authoritarian or quasi-authoritarian regimes. This reasonably leads to the question: whether the cooperation with such regimes shall at all be permitted in AI and related technologies dimension?

2.2. The Russian practice

As several studies reveal, almost 8 million cameras in Russia were installed by the commercial organisations to protect property, while only about 4,5 million cameras operate in hospitals, educational institutions and the governmental premises, being financed from the State budget.[241] Primarily more than 100,000 cameras in Moscow were equipped with the FRT, gradually increasing their number to 175,000 as the technology showed its effectiveness in identifying protesters.[242] Russia is also trying to launch the digitalisation of the public and commercial services, including the FRT payment systems deployed by the State organs and business enterprises. For instance, in Moscow the first mass-scale FRT payment was deployed in the underground at more

[238] Liam Gibson, 'Japan bans facial recognition tech exports due to China's human rights abuses' (*Taiwan News*, 3 January 2022) <https://cutt.ly/HJ0VO8A> accessed 10 June 2022.

[239] Eva Dou, 'China built the world's largest facial recognition system. Now, it's getting camera-shy' (*The Washington Post*, 30 July 2021) <https://www.washingtonpost.com/world/facial-recognition-china-tech-data/2021/07/30/404c2e96-f049-11eb-81b2-9b7061a582d8_story.html> accessed 10 June 2022.

[240] Krisztina Huszti-Orbán and Fionnuala Ní Aoláin, *Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?* (Human Rights Center, University of Minnesota, 2020) 6.

[241] Kristyna Foltynova, 'We See You! How Russia Has Expanded Its' (*Radio Free Europe*, 19 January 2021) <https://cutt.ly/9J2RITv> accessed 10 June 2022.

[242] HRW, 'Russia Expands Facial Recognition Despite Privacy Concerns' (*HRW*, 2 October 2020) <https://cutt.ly/VJ2R1Sl> accessed 10 June 2022.

than 240 stations,[243] being activated via the application containing persons' facial images, bank and transport cards. Although Moscow's Department of Information Technology repeatedly ensured that collected images will not be disclosed to law enforcement,[244] no legal guarantees and predefined procedures exist up to this date. As follows from the authorities' reports, 221 criminals were identified by the FRT during one month,[245] which allegedly proves the effectiveness of the AI-driven surveillance, but also proves the law enforcement access to the databases. Moreover, the 2020 investigation shows that Moscow FRT cameras can be hijacked for $200,[246] which leaves the biometrics contained therein vulnerable to trading on the dark web, manipulations during the election periods, and illegal tracking of individuals. The emblematic example is the lawsuit of Roskomsvoboda activist, who not only noticed her personal data on the black market[247] but also revealed that storage terms are not complied with (available data covered periods longer than two to five days).[248] Thus, *de facto*, the technically unfeasible systems increase the risk of abuse from both the State authorities and private parties possessing malicious intentions, which is usually improperly addressed by the Russian domestic courts.

According to the public surveys, 47% of Moscow residents rather support video surveillance in public places, while 42% treat it rather negatively, fearing the potential persecution and violations of privacy.[249] Interestingly, some respondents even noticed that the low quality of cameras makes their installation a waste of money since such

---

[243] Pjotr Sauer, 'Privacy fears as Moscow metro rolls out facial recognition pay system' (*The Guardian*, 15 October 2020) <https://cutt.ly/uJ2TiKX> accessed 10 June 2022.

[244] Ian Carlos Campbell, 'Moscow adds facial recognition payment system to more than 240 metro stations' (*The Verge*, 15 October 2021) <https://cutt.ly/GJ2T5SM> accessed 10 June 2022.

[245] Игорь Савкин, 'Система распознавания лиц в метро Москвы помогла найти преступников' (*Kod.ru*, 12 August 2021) <https://cutt.ly/JJ2YpuR> accessed 10 June 2022.

[246] Russell Brandom, 'Moscow's facial recognition system can be hijacked for just $200, report shows' (*The Verge*, 11 November 2020) <https://cutt.ly/3J2Yz6I> accessed 10 June 2022.

[247] Никита Королев, 'Лицом к лицу лица не опознать' (*Коммерсантъ*, 25 September 2020) <https://cutt.ly/xJ2YPqc> accessed 10 June 2022.

[248] Анна Кузнецова, 'Суд не увидел нарушения закона в неконтролируемой слежке за москвичами' (*РосКомСвобода*, 24 December 2020) <https://cutt.ly/eJ2Y2Iv> accessed 10 June 2022.

[249] Левада-центр, 'Видеонаблюдение в публичных местах' (*Левада-центр*, 20 August 2020) <https://cutt.ly/4J2Uu2z> accessed 10 June 2022.

systems are unable to meaningfully identify the alleged criminals or prevent crimes. Thus, people are caring more about the inefficiency of the systems rather than the security of their biometrics and privacy. In addition to Moscow, the Russian authorities planned to install the FRT surveillance in the public spaces of the 10 other cities with the list of areas for deployment remaining confidential.[250] And this, again, deprives activists and personal data protection lawyers of the opportunity to conduct the human rights compliance test of the systems in general and verify the legal grounds for their deployment in certain areas specifically.

Similar to most other States, Russia also reasoned the mass installation of the FRT surveillance by the need to control the compliance with the quarantine requirements, ensuring that COVID-positive people stay off the streets.[251] As follows from several public statements, the cameras reported those, who violated the observation regime even if a person left home to take out the garbage or buy some food.[252] It shows that the FRT were not adequately programmed to address the basic social needs of lonely people, who cannot rely on relatives in receiving the life-necessary supply. Moreover, the Russian authorities also failed to explain the manner, in which the database of COVID-positive people was formed and incorporated into the FRT. Thus, the human rights defenders were deprived of the possibility to verify the legality of the biometrics processing.

Akin to that, Russia widely deploys the FRT cameras in educational institutions, a number of which already amounts to more than 43,000 systems. The main reasons for the installation of such technologies included not only the security of schools from evil-intentioned passers-by but also monitoring of children's movements. As well as in other cases, no special regulation for such processing of minors' data is developed, thus amplifying the risks of data misuse or its insecure storage.

---

[250] Никита Королев, 'Регионы узнают в лицо' (*Коммерсантъ*, 25 September 2020) <https://cutt.ly/LJ2Ubxp> accessed 10 June 2022.

[251] Moussa Sangare, 'Mass Surveillance in the Post-Covid-19 World: A Test for the United Nations' (*Global Policy*, 18 May 2020) <https://cutt.ly/VJ2UGQP> accessed 10 June 2022.

[252] Sarah Rainsford, 'Coronavirus: Russia uses facial recognition to tackle Covid-19' (*BBC News*, 4 April 2020) <https://cutt.ly/gJ2UNdN> accessed 10 June 2022.

As regards the regulatory framework, most international human rights organisations notice an alarming trend of the unregulated FRT deployment in Russia,[253] drawing parallels with the Chinese approach. Particularly, the Russian law on personal data affords protection to information related to identifiable persons,[254] while Moscow's IT Department stated about the anonymisation of biometrics gathered by the video surveillance and, respectively, the inapplicability of the data protection laws.[255] Importantly, this position was even upheld by the Moscow courts[256] with the procedure for processing biometrics by the FRT surveillance remaining classified. Akin to that, in 2020 the Russian parliament adopted the Law on experimenting with AI,[257] which lifts the applicability of most data protection regulations to AI testing. At the same time, most testing is conducted in the streets with the FRT processing of the real biometrics, not its laboratory samples. The government encouraged to extend the powers of the Russian law enforcement even more by easing their access to the FRT databases and footage collected by the FRT. However, even without the legal extension of the police powers, the FRT surveillance is still employed in a semi-legal manner. For example, the OVD Info report has outlined at least 7 court orders,[258] allowing the use of the PARSIVE system to identify the faces of the protesters. Apart from that, there are numerous classified databases with biometrics of individuals, their ID card data, the history of arrests and convictions *etc*. Respectively, the human rights defenders are precluded from reasonable assessment of the legality and proportionality

[253] HRW, 'Russia: Broad Facial Recognition Use Undermines Rights' (*HRW*, 15 September 2021) <https://cutt.ly/HJ2Irxz> accessed 10 June 2022.

[254] The Russian Federation Federal Law on Personal Data of 2006 (№152-ФЗ) <https://cutt.ly/TJ2Imgx> accessed 10 June 2022.

[255] РосКомСвобода, 'Разбор: можно ли деанонимизировать протестующих при помощи камер?' (*РосКомСвобода*, 18 February 2021) <https://cutt.ly/EJ2I81C> accessed 10 June 2022.

[256] РосКомСвобода, '"РосКомСвобода" обжаловала решение суда в деле о неконтролируемой видеослежке' (*РосКомСвобода*, 7 April 2021) <https://cutt.ly/eJ2Otfz> accessed 10 June 2022.

[257] The Russian Federation Federal Law on conducting an experiment to establish special regulation in order to create the necessary conditions for the development and implementation of AI technologies in the subject of the Russian Federation - the city of federal significance Moscow and amending Articles 6 and 10 of the Federal Law "On Personal Data" of 2020 (№123-ФЗ) <https://cutt.ly/OJ2OmPV> accessed 10 June 2022.

[258] OVD Info, 'How Authorities Use Cameras and Facial Recognition against Protesters' (*OVD Info*, 2022) <https://cutt.ly/uJ2PrhK> accessed 10 June 2022.

of the law enforcement actions. And, most importantly, neither judicial nor legislative safeguards are developed or expected to be developed.

Lacking a proper legal framework, the Russian authorities repeatedly resorted to the abusive practices of the FRT application, while instances of malfunctioning were not resolved properly. For instance, Sergey Mezhuyev was mistakenly detained by the police due to the misidentification by the FRT surveillance,[259] being searched and fingerprinted despite the acknowledgement of the error. Another case involved the apprehension of an individual in the mall based on the results from the FRT cameras, which also turned out to be the system's malfunctioning.[260]

Yet, despite being a significant inconvenience, misidentification still is not the main problem of the FRT surveillance. To exemplify, the Russian authorities applied the FRT cameras to prosecute political opposition and apprehend individuals after the peaceful protests.[261] According to the various reports, some individuals and even passers-by at the demonstrations were stopped by the police or received a notice several days after the public gathering.[262] For example, approximately 180 court cases were initiated within the week following the Moscow pro-Navalnyy protests, which is 18 times more than the ordinary number of apprehended persons during the public gatherings.[263] Other activists, vice versa, were stopped before the demonstration for

[259] РосКомСвобода, 'История Сергея Межуева: первый кейс по ошибке системы распознавания лиц в метро' (*РосКомСвобода*, 19 November 2020) <https://cutt.ly/yJ2PxgH> accessed 10 June 2022.

[260] РосКомСвобода, '"Думаете, если вы ведёте обычную жизнь, вас не могут нажатием одной кнопки подвести под статью?"' (*РосКомСвобода*, 16 December 2020) <https://cutt.ly/eJ2NlYo> accessed 10 June 2022.

[261] Александр Бородихин, '"Скрыться невозможно". Как активиста "Другой России" задержали в метро по сигналу с видеокамеры, опознавшей его по ориентировке Центра "Э"' (*Медиазона*, 10 October 2018) <https://cutt.ly/dJ2NU0J> accessed 10 June 2022; Robyn Dixon, 'Russia's surveillance state still doesn't match China. But Putin is racing to catch up.' (*The Washington Post*, 17 April 2021) <https://www.washingtonpost.com/world/europe/russia-facial-recognition-surveillance-navalny/2021/04/16/4b97dc80-8c0a-11eb-a33e-da28941cb9ac_story.html> accessed 10 June 2022.

[262] РосКомСвобода, 'Система распознавания лиц теперь ищет протестующих' (*РосКомСвобода*, 4 February 2021) <https://cutt.ly/qJ213SI> accessed 10 June 2022; OVD Info, 'Позиция ОВД-Инфо по массовым преследованиям в связи с акциями 23 января' (*OVD Info*, 29 January 2021) <https://cutt.ly/lJ208H8> accessed 10 June 2022; OVD News, 'Полиция всю неделю задерживает предполагаемых участников акций 21 апреля. Данные ОВД-Инфо' (*OVD News*, 24 April 2021) <https://cutt.ly/QJ22aYO> accessed 10 June 2022.

[263] OVD Info, 'How Authorities Use Cameras and Facial Recognition against Protesters' (*OVD Info*, 2022) <https://cutt.ly/uJ2PrhK> accessed 10 June 2022.

being on the list of "*repetitive participants of unsanctioned protests*".[264] As a result, numerous individuals abstain from participation in the opposition public gatherings – if previously they risked being apprehended during the event, being able to escape the arrest and hide their face under the covering, now the risk period is not limited by the peaceful protest itself, but extends far beyond it. This, in turn, creates the fear of being prosecuted at any moment, giving rise to the chilling effect on a large spectrum of human rights and freedoms.

Furthermore, the absence of a legal procedure for using the FRT camera footage as evidence in the court or during the interrogation. In this manner, the apprehended student was able to access the recording from the demonstration during the court proceedings, while the police interrogations included only the officers' report on recognizing a person on the video.[265] However, it is important to note that some cases were successful for the protesters since the courts were unable to establish the similarity between the video footage and the face of the accused individuals.[266] Based on the indefinite status of evidence, the court also declared one case inadmissible.[267] Albeit, the practice of rejecting the FRT results as evidence is still not extensive and rather exceptional. Therefore, in most cases, the protesters remain under the constant threat of excessive fines and imprisonment terms.

Akin to that, the UN Special Rapporteur stressed that Russian FRT and biometric technologies have reportedly been transferred to several Central Asian governments,[268] where the quasi-authoritarian regimes employ them to discriminate and oppress minorities. Respectively, the Russian FRT industry creates significant human rights

---

[264] РосКомСвобода, 'Разбор: можно ли деанонимизировать протестующих при помощи камер?' (*РосКомСвобода*, 18 February 2021) <https://cutt.ly/EJ2I81C> accessed 10 June 2022.

[265] OVD Info, 'How Authorities Use Cameras and Facial Recognition against Protesters' (*OVD Info*, 2022) <https://cutt.ly/uJ2PrhK> accessed 10 June 2022.

[266] OVD News, 'Последствия акций протеста из-за заключения Навального. Хроника, часть 2' (OVD News, 22 April 2021) <https://cutt.ly/kJ24eos> accessed 10 June 2022.

[267] OVD Info, 'How Authorities Use Cameras and Facial Recognition against Protesters' (*OVD Info*, 2022) <https://cutt.ly/uJ2PrhK> accessed 10 June 2022.

[268] Krisztina Huszti-Orbán and Fionnuala Ní Aoláin, *Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?* (Human Rights Center, University of Minnesota, 2020) 35.

risks not only for its citizens but also for other States, which might enhance their abusive practices with the employment of the modern technologies.

In response to all violations, numerous international organisations criticised the use of the FRT by the Russian authorities due to the breach of confidentiality.[269] The Russian human rights defenders also signalised the absence of the review mechanism, ineffectiveness and corrupted nature of the Russian courts, calling for the ban of the FRT surveillance until the proper legal framework is developed.[270] As a consequence, the activists even filed an application with the ECtHR,[271] claiming the illegality of the Russian video monitoring practices. Simultaneously, the human rights defenders launched a petition calling for the ban of the FRT.[272] Thus, although the scale of breaches is incomparable to the Chinese discriminatory policies and oppression of minorities, absence of the effective oversight and review still opens the door for numerous abuses, a number of which gradually raises given the irresponsibility of the State for the violations.

2.3. The US practice

FRT are widely deployed across the US in different security areas, starting from the iPhone unlocking via identifying the owner's face and ending up with the processing of intercepted Yahoo! video chats (a large proportion of which depicts nudity and other deeply intimate information).[273] As follows from Garvie, Bedoya and Frankle's research, in 2016 roughly half of the US citizens already had their biometrics incorporated into the FRT databases.[274] Only New York City is equipped with more

[269] Радіо Свобода, 'Human Rights Watch розкритикувала плани Росії розширити застосування системи розпізнавання облич' (*Радіо Свобода*, 2 October 2020) <https://cutt.ly/6J2MEUv> accessed 10 June 2022.

[270] 'Кампания против распознавания лиц' (*Bancam.ru*) <https://cutt.ly/rJ2MLrK> accessed 10 June 2022.

[271] Anastasiia Kruope, 'Moscow's Use of Facial Recognition Technology Challenged' (*HRW*, 8 July 2020) <https://cutt.ly/gJ21ekt> accessed 10 June 2022.

[272] Umberto Bacchi, 'Face for sale: Leaks and lawsuits blight Russia facial recognition' (*Reuters*, 9 November 2020) <https://cutt.ly/iJ21Wvk> accessed 10 June 2022.

[273] Amnesty International, 'Two Years after Snowden: Protecting Human Rights in an Age of Mass Surveillance' (*Amnesty International*, 4 June 2015) 3.

[274] Clare Garvie, Alvaro Bedoya and Jonathan Frankle, 'The Perpetual Line-Up: Unregulated Police Face Recognition in America' (*Georgetown Law Centre on Privacy and Technology*, 18 October 2016) <https://cutt.ly/AJ0ORhf> accessed 10 June 2022.

than 15,280 cameras, which have been identified by the volunteers around Manhattan, Brooklyn and the Bronx.[275] Interestingly, no official data on the number of the FRT cameras are provided, while the New York Police Department reported the use of AI-driven surveillance more than 22,000 times since 2017 without any detalisation of the specific instances.[276] Not only everyday surveillance is set in the US, but FRT cameras are also targetedly used to identify protesters, as happened during the 2021 Capitol riots.[277] Even more, AI-driven surveillance is promoted as a highly effective technology by the airports,[278] whereas numerous states have adopted the FRT to identify individuals applying for unemployment benefits.[279] However, all successful practices are often accompanied by the polar calls to ban the FRT surveillance on the federal level, making the US a perfect case for exploring its impact on human rights.

In contrast to other States, the US developed a legal framework for cross-border surveillance, covering the collaboration with foreign authorities, detailed guidance on data processing and specific grounds for interference.[280] Large corporations regularly request the government to put the FRT among the permissible monitoring tools,[281] though remaining unsuccessful in their strivings. However, the legislation on extraterritorial surveillance only partly resolves the problem of AI under-regulation. Back in 2014, the HRC declared the US surveillance techniques unforeseeable on the conditions and objectives of their application, deprived of the safeguards and

[275] Amnesty International, 'Surveillance city: NYPD can use more than 15,000 cameras to track people using facial recognition in Manhattan, Bronx and Brooklyn' (*Amnesty International*, 3 June 2021) <https://cutt.ly/VJ0OAnJ> accessed 10 June 2022.

[276] *Ibid*.

[277] Drew Harwell and Craig Timberg, 'How America's surveillance networks helped the FBI catch the Capitol mob' (*The Washington Post*, 2 April 2021) <https://www.washingtonpost.com/technology/2021/04/02/capitol-siege-arrests-technology-fbi-privacy/> accessed 10 June 2022.

[278] Tom Simonite, 'Face Recognition Is Being Banned—but It's Still Everywhere' (*Wired*, 22 December 2021) <https://cutt.ly/nJ0O4X2> accessed 10 June 2022.

[279] Andrew Kenney, 'Colorado Will Use ID.me Tech Platform to Verify Unemployment Applications, Review Fraud Flags' (*CPR News*, 13 January 2021) <https://cutt.ly/8J0PeWL> accessed 10 June 2022.

[280] Charles Doyle, *Extraterritorial Application of American Criminal Law* (Congressional Research Service, 2016) 40.

[281] Will Schrepferman, 'Supervising Surveillance: Applying International Law to the Global Surveillance State' (*Harvard International Review*, 11 November 2020) <https://cutt.ly/BJNwJvV> accessed 10 June 2022.

independent oversight.[282] Additionally, the lack of a consistent approach toward the liability of the national security agencies has been identified as a significant regulatory gap.[283] Specifically, they are applying the technology without any supervision or even notification of the surveillance existence.

In response to this problem, a range of proposals emerged dwelling upon the enaction of a Commercial Facial Recognition Act of 2019,[284] which intended to generally prohibit the FRT from collecting data without the notification and consent. Also, in 2019 research devoted to commercial the FRT showed unequal performance of AI on different demographics,[285] which signalized its problematic use in such a multinational country as the US. Respectively, numerous states initiated banning of the FRT surveillance[286] to avoid unfavourable discriminatory effects and prevent its abusive application. This initiative was actively supported by human rights NGOs, activists and journalistic organisations. As a reasonable consequence, it has reached the federal level, being addressed in the Facial Recognition and Biometric Technology Moratorium Act. This document, in particular, proposed to outlaw the FRT and other biometric technologies for federal entities (with the ban being possible to be lifted only by the Congress), as well as prohibit the use by federal authorities of data collected by the FRT and establish a procedure for a redress action in case of violations.[287] Simultaneously, it allows local authorities to decide the issue of applying the FRT themselves. This legislative proposal has not yet been approved, though having a powerful lobby.

---

[282] Yuval Shany, 'On-Line Surveillance in the case-law of the UN Human Rights Committee' (*The Federmann Cyber Security Research Center – Cyber Law Program*, 13 July 2017) <https://cutt.ly/4J0PB4D> accessed 10 June 2022.

[283] Tambiama Madiega and Hendrik Mildebrath, *Regulating facial recognition in the EU* (EPRS, 2021) 33.

[284] US Commercial Facial Recognition Privacy Act of 2019 (S.847) <https://cutt.ly/HJ0At7I> accessed 10 June 2022.

[285] Patrick Grother, Mei Ngan and Kayee Hanaoka, *Face Recognition Vendor Test (FRVT). Part 3: Demographic Effects* (Internal Report 8280, National Institute of Standards and Technology Interagency, 2019) 71.

[286] Михайло Каменєв, 'Гостре око Старшого Брата' (*РІПР*, 4 November 2017) <https://cutt.ly/hJ0ARc0> accessed 10 June 2022; Steve Neavling, 'New legislation would ban facial recognition on federal level, withhold funds from cities like Detroit that use it' (*MetroTimes*, 15 June 2021) <https://cutt.ly/tJ0AO4W> accessed 10 June 2022; Associated Press, 'Worcester bans city use of facial recognition technology' (*New York Post*, 15 December 2021) <https://cutt.ly/mJ0AGkX> accessed 10 June 2022.

[287] US Bill "To prohibit biometric surveillance by the Federal Government without explicit statutory authorization and to withhold certain Federal public safety grants from State and local governments that engage in biometric surveillance" (116th Congress, 2019-2020).

Why do the initiatives to ban the FRT surveillance become the domineering vision in the US? First of all, the US government approaches technical security very critically. To illustrate, the Chinese company Hikvision was put on the sanction list due to the possible access of the third parties to the collected biometrics.[288] Luckily, the US created a favourable environment for the local producers, such as IBM, which can cover both national and foreign markets.[289] Thus, national security matters do not become a cornerstone issue for the deployment of the FRT surveillance in the US.

Nevertheless, any security limitation does not exclude the mass practical failures and the malfunctioning of the AI-driven systems irrespective of the producers' origin. For instance, people of colour have already been wrongfully arrested and prosecuted due to misidentification by the FRT cameras,[290] including the targeted apprehensions of activists after the Black Lives Matter protests.[291] Although the domestic authorities have repeatedly claimed monitoring tools to be effective against the terrorist attacks, in fact, in *Klayman v Obama* the government failed to mention any successful case,[292] thus proving that security matters serve only as a shield for abusive practices. Moreover, the US is often accused of collaborating with organisations violating personal data protection rules,[293] therefore legitimizing their policies and approaches to biometrics and its processing (including scandalous Clearview AI). In this respect, several federal agencies have already received letters from lawmakers, who called to cease using the Clearview AI as the controversial FRT.[294] Notwithstanding an immediate termination of cooperation with the company did not happen, the authorities

---

[288] Михайло Каменєв, 'Гостре око Старшого Брата' (*РІПР*, 4 November 2017) <https://cutt.ly/hJ0ARc0> accessed 10 June 2022.

[289] Steven Feldstein, 'The Global Expansion of AI Surveillance' (Carnegie Endowment for International Peace, 2019) 2.

[290] Kashmir Hill, 'Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match' (*The New York Times*, 29 December 2020) <https://cutt.ly/jJ0A5hx> accessed 10 June 2022.

[291] Amnesty International, 'The World is Watching: Mass Violations by US Police of Black Lives Matter Protesters' Rights' (*Amnesty International*) <https://cutt.ly/AJ0StxN> accessed 10 June 2022.

[292] *Klayman v Obama* 957 F Supp 2d. 1 (2013).

[293] Jeremy Hainsworth, 'US 'mass surveillance' company challenges B.C. privacy watchdog order' (*Pique*, 24 January 2022) <https://cutt.ly/hJ0Sluy> accessed 10 June 2022.

[294] Russell Brandom, 'Lawmakers call on feds to drop Clearview AI facial recognition contracts' (*The Verge*, 9 February 2022) <https://cutt.ly/2J0SmuU> accessed 10 June 2022.

promised to assess the quality and human rights compliance of the system. Yet, the conclusion, which can be made from the described processes implies the structural problems on both governmental and private industry levels, which are trying to advance technically beneficial solutions without a proper legislative basis.

Following numerous instances of the FRT surveillance malfunctioning and misapprehension of individuals based on mismatches with the law enforcement database, NGOs and human rights defenders have expressly urged to ban the real-time AI-driven biometric surveillance. Numerous American organisations join the open statements urging the prohibition of such technology.[295] Moreover, the American Civil Liberties Union instituted court proceedings against the US administration, calling to recognise mass surveillance as unconstitutional.[296] The main claims include the foreclosure of the State surveillance programme and the erasure of all collected data. Apart from the governmental policies, the civil society sector has also criticised private companies, such as Clearview AI,[297] exhorting to ban the FRT due to the outrageous violation of the personal data processing rules. Simultaneously, the Union also addressed President Biden with an open letter,[298] encouraging him to join the advocacy campaign against the FRT surveillance. Respectively, the movement against AI-driven surveillance gains the scale proportionately to the number of the outstanding scandalous cases of its misuse.

Despite the legitimate goals, declared by the US executive authorities, the FRT surveillance remains a practically unreliable instrument for the prevention of malicious activities. Such negative effects cannot be mitigated by the democratic environment, where AI-driven systems are deployed. Thus, the safeguards against abuses or

---

[295] 'Civil Rights Concerns Regarding Law Enforcement Use of Face Recognition Technology' (New America, 3 June 2021) <https://cutt.ly/TJ0DBGY> accessed 10 June 2022.

[296] РБК-Україна, 'Правозахисники подали до суду на уряд США за масове стеження' (*РБК-Україна*, 12 June 2013) <https://cutt.ly/wJ0DSMf> accessed 10 June 2022.

[297] Nick Statt, 'ACLU sues facial recognition firm Clearview AI, calling it a 'nightmare scenario' for privacy' (*The Verge*, 28 May 2020) <https://cutt.ly/bJ0DRcK> accessed 10 June 2022; Russell Brandom, 'French regulator tells Clearview AI to delete its facial recognition data' (*The Verge*, 16 December 2021) <https://cutt.ly/bJ0DRcK> accessed 10 June 2022.

[298] VoaNews, 'Правозахисники у США закликали Байдена виступити проти використання технологій розпізнавання облич урядом' (*VoaNews*, 17 February 2021) <https://cutt.ly/hJ0DrBz> accessed 10 June 2022.

malfunctioning hardly depend on the general human rights protection framework but are rather linked to the very nature of technology.

2.4. The UK practice

Similar to the US and Chinese practices, the UK has a long-standing history of applying various surveillance techniques, which has repeatedly brought the State to the ECtHR. Akin to the classic tools, such as interception of communications and ordinary video surveillance, the UK government decided to deploy the real-time FRT. To illustrate, London's Metropolitan Police already uses CCTV cameras to search for individuals on the wanted list via AI-driven technologies.[299] Importantly, in the UK FRT surveillance has even been tested in real-life situations via street cameras,[300] which implies the lack of any guarantees, specialised regulations and safeguards against data leakage. Namely, AI-driven surveillance was deployed by the South Wales Police at mass events, such as the UEFA Champions League Final and music concerts. In contrast to other States, the UK police specifically designed the watchlists comprised of individuals, who "*are perceived to pose a serious risk to public safety*", have previous convictions for serious offences, "*individuals of possible interest to police*", and images of police officers for testing purposes.[301] A general assessment of the categories shows them to be overly vague, leaving the law enforcement a wide margin of appreciation in determining the risk rate of the individuals and accessibility of the public events for them. Furthermore, despite several claims of very low false positives amounting to 0,1%, the independent investigation revealed an 81% inaccuracy rate,[302] making the deployed in the UK FRT an unreliable mechanism.

---

[299] Kelly Hine and Robert Fleet, 'Information is key to public support for police use of facial recognition technology' (*The Conversation*, 15 December 2021) <https://cutt.ly/wJ9qpgK> accessed 10 June 2022.

[300] European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement* (FRA, 2020) 3.

[301] Bethan Davies, Martin Innes and Andrew Dawson, *An evaluation of South Wales police's use of automated facial recognition* (Cardiff Universities' Police Science Institute, Crime and Security Research Institute, 2018) 12-13.

[302] Alexander Martin, 'Police force to roll out '81% inaccurate' live facial recognition' (*SkyNews*, 24 January 2020) <https://cutt.ly/oJ9wsOi> accessed 10 June 2022.

Another practice recently introduced in the UK by law enforcement was the FRT mobile application, which can be used by police officers to identify individuals even if they try to mislead them.[303] Contrary to the video surveillance in the streets, this application is always applied with human supervision, being designed for confirmation of the identity rather than establishing it by the system itself. Thus, it might serve as a less intrusive alternative for law enforcement purposes. Yet, the UK, as well as several other countries, faced the problem of the illegal composition of the systems by the private companies. Specifically, the UK Information Commissioner's Office criticised the use of the Clearview AI due to unlawful collection of information from social media, being factually and legally incorrect.[304] Moreover, the company proposed its services to UK law enforcement, which led to numerous misapplications of the FRT.

Apart from that, the UK authorities are actively deploying the FRT in schools and other educational institutions. It does not always take the form of surveillance – for instance, students can pay for their school lunches by scanning faces, which allegedly speeds up the queues.[305] This technology is assumed to be based on one's consent, being applied to specific individuals, who are willing to get some service only. However, there are still numerous concerns about the protection of the children's data and absence of the effective oversight – the UK department of education holds no data on the FRT deployment in schools. Specifically, the research shows the low human rights literacy level among the younger generation,[306] signalizing the significant privacy risks – starting from the issue of informed consent, and ending up with the general technical illiteracy of many children. In response to technological novelties in the British schools, the UK Information Commissioner's Office initiated the

[303] Kelly Hine and Robert Fleet, 'Information is key to public support for police use of facial recognition technology' (*The Conversation*, 15 December 2021) <https://cutt.ly/wJ9qpgK> accessed 10 June 2022.

[304] Rob Davies, 'US facial recognition firm faces £17m UK fine for 'serious breaches'' (*The Guardian*, 29 November 2021) <https://cutt.ly/lJ9iQoZ> accessed 10 June 2022.

[305] Cynthia O'Murchu, 'Facial recognition cameras arrive in UK school canteens' (*The Irish Times*, 21 October 2021) <https://cutt.ly/vJ9oA0N> accessed 10 June 2022.

[306] The Conversation, 'A Generation Growing Under Surveillance: The Dangers of Facial Recognition In Schools' (*Interesting Engineering*, 14 November 2021) <https://cutt.ly/GJ9p4p6> accessed 10 June 2022.

investigation into the FRT use,[307] causing a pause in AI-driven tools application in the educational institutions.

Simultaneously, as the large UK survey shows, most people feel comfortable with using the FRT in everyday life despite the lack of legal safeguards and frequently underexplained mechanism of AI-driven surveillance functioning.[308] For instance, only 29% are against the deployment of the FRT by police forces, while 55% call for the establishment of the regulated use of AI-driven surveillance by law enforcement. At the same time, the application of the FRT for commercial use faces more objections. Three potential explanations for this phenomenon might be found: the higher trust in the good faith of the State compared to the private sector, enhanced fears of terrorist activities, or the low level of human rights and digital literacy. Nevertheless, the public attitude also significantly depends on the existence of the legislative regulation, providing for the rules, exceptions and safeguards.

The primary regulation for the surveillance measure includes the Investigatory Powers Act,[309] which established the Investigatory Powers Commissioner's Office authorized to conduct oversight over the monitoring techniques. Additionally, the Protection of Freedoms Act created the institutes of the Surveillance Camera Commissioner and the Biometrics Commissioner,[310] neither of whom consider the FRT surveillance as being governed by the current UK legislation. Back in 2015, the UN HRC stressed a negative tendency to make a distinction between the domestic and foreign UK surveillance, noting that much weaker safeguards are afforded to the domestic practices.[311] It has led to the Investigatory Powers Tribunal recognizing the unlawful spying on several NGOs, which triggered the review of the scope of discretion

[307] Sally Weale, 'ICO to step in after schools use facial recognition to speed up lunch queue' (*The Guardian*, 18 October 2021) <https://cutt.ly/AJ9avBA> accessed 10 June 2022.

[308] 'Beyond face value: public attitudes to facial recognition technology' (*Ada Lovelace Institute*, 2 September 2019) <https://cutt.ly/4J9aOwD> accessed 10 June 2022.

[309] UK Investigatory Powers Act of 2016 <https://cutt.ly/UJ9a95S> accessed 10 June 2022.

[310] UK Protection of Freedoms Act of 2012 <https://cutt.ly/nJ9svLg> accessed 10 June 2022.

[311] Yuval Shany, 'On-Line Surveillance in the case-law of the UN Human Rights Committee' (*The Federmann Cyber Security Research Center – Cyber Law Program*, 13 July 2017) <https://cutt.ly/4J0PB4D> accessed 10 June 2022.

granted to the UK law enforcement.[312] One of the main issues, which the applicant advanced was an absence of any clarity on the type and amount of collected data, as well as conditions, under which such collection can be done. Lastly, the Tribunal found the violation in absence of any independent and effective oversight.

Subsequently, the surveillance topic expanded to comprise several judicial decisions, assessing the FRT legality. Particularly, in *R (Bridges) v Chief Constable of South Wales Police and Others* the court found that AI-driven surveillance amounts to a significant intrusion into one's privacy,[313] breaching it without a solid legislative regulation, and maintenance of the proportionality principle.[314] Namely, the law enforcement authorities are not allowed to collect more information than is reasonably necessary for the achievement of the legitimate goal. Another issue, raised in this case, concerned those, who may be put on the watch list within the FRT database, and subsequently monitored by the police.[315] Specifically, the court stressed that such an exclusive list shall be predefined at the legislative level.

At the same time, the UK Information Commissioner's Office *de facto* permitted the use of the FRT by the police subject to surveillance is necessary, proportionate and of "*demonstrable benefit to the public*".[316] Although UK law enforcement ensures the deletion of images that do not match the watchlists, it does not exclude the processing of biometrics *per se*. Moreover, the dubious cases, where the percentage of similarity is relatively high, still imply the storage of such a template for further human assessment. And, given the low quality of the deployed FRT, it is expected to have numerous cases of doubtful identification. Accordingly, the removal of data, which does not fit, is a declaratory assurance rather than a practically applicable standard. Thus, in absence of the legislative regulation and with several court cases recognizing

---

[312] Bill Goodwin, 'UK spies face landmark challenge over mass surveillance in human rights court' (*Computer Weekly*, 7 November 2017) <https://cutt.ly/bJ9dmfi> accessed 10 June 2022.

[313] *R (Bridges) v CC South Wales Police and Others* [2020] EWCA Civ 1058, paras 148-149.

[314] Robin Hopkins, 'Key points from the Bridges facial recognition appeal' (Panopticon, 3 September 2020) <https://cutt.ly/DJ9hNj5> accessed 10 June 2022.

[315] *R (Bridges) v CC South Wales Police and Others* [2020] EWCA Civ 1058, paras 90-96.

[316] David Meyer, 'Privacy, bias and safety: On facial recognition, Berlin and London choose different paths' (*Euractiv*, 2 February 2020) <https://cutt.ly/CJ9myCQ> accessed 10 June 2022.

the illegality of video surveillance, the executive authorities are looking for ways to justify the FRT application. And the positive societal reaction evidences the relative effectiveness of the justification provided.

However, the expert community, including the human rights defenders, journalists and privacy lawyers, have repeatedly stressed the emerging chilling effect and overall intrusiveness of the employed surveillance techniques. Specifically, it has reached the ECtHR's level in the mentioned *Big Brother Watch and Others v the UK*, while the FRT surveillance is already heatedly discussed among the human rights organisations. Thus, another challenging case might be expected with a detailed guideline on this matter being provided by the international judicial body. At the same time, the UK is expected to join the pan-European network of police facial recognition under the EU-UK Trade and Cooperation Agreement.[317] It means that despite the ongoing legal debates on AI-driven surveillance and its regulation, the practical application is promoted and even incorporated into international treaties. Moreover, even a huge number of the domestic supervisory bodies do not efficiently safeguard against unauthorized interference with privacy due to both the legal and technical imperfectness of the AI systems. Thus, even the complex human rights protection frameworks are not able to fully address and mitigate the risks.

2.5. The German practice

German experience serves as one of the most emblematic shifts in the approach toward the FRT surveillance. During the 2017 G20 summit the Hamburg police actively used the FRT to identify potential criminal activity, which further was criticised by the Data Protection Commissioner of Hamburg due to the absence of an explicit legal basis for biometric surveillance.[318] In 2018 the Berlin police together with 300 volunteers tested three different FRT at the train stations, publishing a report with

[317] Frank Hersey, 'UK can join EU biometric surveillance without Parliamentary scrutiny: Statewatch' (*Biometric Update.Com*, 20 January 2022) <https://cutt.ly/7J9wRdm> accessed 10 June 2022.

[318] Germany, Datenschutzrechtliche Prüfung des Einsatzes einer Gesichtserkennungssoftware zur Aufklärung von Straftaten im Zusammenhang mit dem G20-Gipfel durch die Polizei Hamburg (Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, 2018) 5-7.

a finding that approximately 80% of individuals were identified accurately.[319] Though, it is important to note that the law enforcement stressed a need for a separate law regulating the FRT, the absence of which makes AI-driven surveillance an abusive practice. Based on the 2018 experiments with the FRT surveillance at the Berlin-Südkreuz station, in 2020 the German Minister of Interior declared the government's intention to deploy AI-driven surveillance at 134 railway stations and 14 airports.[320] Simultaneously, the 20% mistake rate has been called "*a minimal percentage of false positives*",[321] which reasonably raises the concerns regarding the FRT's future application and use as a piece of evidence in the court proceedings. Nevertheless, the German authorities decided that the FRT might become an improved technical possibility for the local law enforcement authorities, raising the efficiency of police officers by shifting responsibility to review the CCTV cameras records from individuals to an automated system. At the beginning of 2021, Germany even employed Cognitec System to conduct border checks via the FRT applications,[322] which could allegedly speed up the verification at the airports and other border control stations.

No specific legislation, tailored to the AI-driven surveillance, was introduced, whereas the existing legal framework addresses the monitoring powers of the law enforcement authorities only in general terms. For instance, the Law on improving cooperation in the field of constitutional protection expands the surveillance powers of intelligence in the cyberthreat dimension.[323] Also, the Law on international foreign telecommunications reconnaissance of the Federal Intelligence Service allows the

---

[319] Germany, "Biometrische Gesichtserkennung" des Bundespolizeipräsidiums im Rahmen der Erprobung von Systemen zur intelligenten Videoanalyse durch das Bundesministerium des Innern, für Bau und Heimat, das Bundespolizeipräsidium, das Bundeskriminalamt und die Deutsche Bahn AG am Bahnhof Berlin Südkreuz (Bundespolizeipräsidium Potsdam, 18 September 2018) 20.

[320] Philipp Grüll, 'Germany's plans for automatic facial recognition meet fierce criticism' (*Euractiv*, 10 January 2020) <https://cutt.ly/iJ9nJVq> accessed 10 June 2022.

[321] David Meyer, 'Privacy, bias and safety: On facial recognition, Berlin and London choose different paths' (*Euractiv*, 2 February 2020) <https://cutt.ly/CJ9myCQ> accessed 10 June 2022.

[322] Tony Kingham, 'Cognitec Technologies to Capture Facial Images at German Borders' (Border Security Report, 25 August 2021) <https://cutt.ly/GJ9mnam> accessed 10 June 2022.

[323] German Law to improve cooperation in the field of constitutional protection came into force (2015) <https://cutt.ly/3J9Qe4H> accessed 10 June 2022.

intelligence service to process the communications of non-EU citizens outside Germany when the interception point is in Germany without any judicial oversight.[324] None of the listed legislative acts, though, allow for the automated processing of biometrics or their uncontrolled bulk collection in public places. Accordingly, the idea to deploy the FRT surveillance on transport stations faced lots of criticism from the perspective of the protection of constitutional rights.

The only existing regulatory practice on the FRT nowadays implies the decisions of the German courts. One of them is connected with the FRT application during the G20 summit, where the appeal court has found it illegal, while the second decision implied an injunctive order against the Cologne Police to cease video surveillance of Breslauer Platz and its side streets in Cologne.[325] Additionally, the Hamburg Data Protection Authority recognised the Clearview AI as violating the domestic data protection laws and the GDPR.[326] Both court cases reflect the tendency of prohibiting the FRT surveillance in absence of a solid legal basis with the necessary guarantees against abuse. Also, the decision to outlaw Clearview AI shows that the limitations are intended to be imposed not only from the legal perspective (lawful processing of information by the State bodies) but also on the technical plane (implying the technically correct and good faith functioning of the systems). Following these findings by the judicial and supervisory authorities, the new government decided to advance the ban on the FRT surveillance. Particularly, this position was inspired by the European Commission Proposal on AI regulation,[327] but the German government went even further requiring to outlaw any real-time biometric identification regardless of the circumstances for its use. One of the main reasons was the German striving to preserve anonymity in public spaces and ensure the free performance of the rights without any chilling effect. The potential effect might be also found in the sanctions imposed by

[324] *1 BvR 2835/17* (Judgment of the First Senate of 19 May 2020), para 294.

[325] Tambiama Madiega and Hendrik Mildebrath, *Regulating facial recognition in the EU* (EPRS, 2021) 12.

[326] Hamburg Data Protection Authority, Consultation prior to an order pursuant to Article 58(2)(g) GDPR (2020).

[327] Melissa Heikkilä, 'German coalition backs ban on facial recognition in public places' (*Politico*, 24 November 2021) <https://cutt.ly/PJ9IrDB> accessed 10 June 2022.

the EU on the FRT technologies produced in the authoritarian regimes,[328] which are usually employed due to their low pricing and accessibility. Particularly, the tracking of the origin and links of the producing companies with the authoritarian States is often complicated, which makes deployment of the AI-driven surveillance even riskier for privacy (given the potential transfer of biometrics abroad).

Even more, the German authorities called to "*reject comprehensive video surveillance and the use of biometric recording for surveillance purposes*",[329] meaning absolute prohibition on mass surveillance amounting to processing of biometrics (which also covers the usual video surveillance). The governmental initiative was backed up by the powerful human rights defenders' lobby manifested in the internationally coordinated campaign Reclaim Your Face.[330] And this example is one of few, where the voice of the civil society and the State authorities is so consolidated on the disputable privacy topic. Apart from the domestic policies, the idea of banning the FRT surveillance is also promoted on the EU level, thus expanding the influence beyond the purely national borders. Thus, Germany may become the first State to officially and explicitly outlaw the AI-driven biometric surveillance, simultaneously limiting any kind of mass monitoring. Even if its impact would not suffice for changing the whole European attitude, this case might serve as a guide for other countries, willing to enhance the human rights protection framework and limit the surveillance tools to a possible minimum.

***

The dangers stemming from the FRT surveillance significantly depend on the human rights protection rate of the country, where they are used. Particularly, the States with a low human rights record and "traditional" discriminatory and abusive practices adjust FRT to exacerbate the violations of the fundamental rights and freedoms. However, as the research shows, not only China and Russia are inclined to use AI-

[328] Council Implementing Regulation (EU) 2020/2129 of 17 December 2020 implementing Article 8a(1) of Regulation (EC) No 765/2006 concerning restrictive measures in respect of Belarus (2020) OJ L 426 I, ANNEX 1.

[329] EDRi, 'New German government calls for European ban on biometric mass surveillance' (*EDRi*, 1 December 2021) <https://cutt.ly/tJ9Sf43> accessed 10 June 2022.

[330] Reclaim Your Face campaign <https://cutt.ly/xJ0xuFm> accessed 10 June 2022.

driven surveillance to track minorities, and vulnerable groups and persecute protesters. A similar approach was maintained in the US, where the human rights protection framework is perceived as being more solid.

Another finding is that most States regardless of their democracy and rule of law index lack the proper legislative framework for the FRT surveillance application. Hence, citizens are deprived of the necessary safeguards, where they suspect abuse of powers, disproportionate intrusion into their privacy, or possibility of the uncontrolled tracking based on their public activity. Although the risks are higher in the States, where human rights breaches remain an ordinary phenomenon, other countries also face risky legal situations with uncontrolled use of surveillance techniques.

Lastly, the perception of the FRT surveillance by the citizens depends on the explainability of the systems' work, transparency of their installation places, and the conditions for using information from the databanks. The less informed societies usually have fewer concerns regarding potential human rights abuses, which leads to further deployment of the intrusive surveillance. At the same time, a more transparent FRT application expeditiously signalises the dangers, forming an objective perception of such technologies among ordinary citizens and decision-makers. In most cases, it leads to the initiatives of banning risky real-time biometric identification systems, as the German example shows.

CHAPTER 3.
REGULATORY FRAMEWORK FOR THE FACIAL RECOGNITION TECHNOLOGIES IN UKRAINE

3.1. Legal regulation of personal data protection and surveillance measures in Ukraine

Ukrainian legal framework on personal data operates with a range of legislative safeguards, ensuring the protection of biometrics, confidentiality and one's integrity. The Law of Ukraine on Personal Data Protection enshrines the basic standards for consensual processing of data, which pursues legitimate purposes and complies with the principles of data minimization.[331] The current law prohibits the processing of data related to ethnic and national origin, political and religious beliefs, and affiliation with lawfully established associations.[332] This reasonably echoes Ukrainian anti-discrimination law, outlawing unequal treatment of individuals based on protected grounds.[333] Thus, limitation on the processing of sensitive data serves as an additional safeguard against discriminatory tactics, employed by the public and private actors.

At the same time, the exceptional cases where such processing is allowed include the explicit consent, data processing for medical or labour purposes, providing the legal services, keeping military records of conscripts, or where the case concerns data explicitly made public by the data subject.[334] The latter ground opens the venture for misuse, enabling data managers and owners to process the data from publicly available social media pages. Subsequently, such companies as Clearview AI create umbrella databases, uniting the information from all over the world, which can further be hacked or shared with non-democratic governments. Hence, framing this notion among the lawful grounds for sensitive data processing creates several risks to individuals' privacy. Akin to that, the personal data subject is granted the right to know about the

[331] Law of Ukraine on Personal Data Protection (2014) <https://cutt.ly/YJ9JCM5> accessed 10 June 2022, Article 6.

[332] *Ibid*, Article 7(1).

[333] Law of Ukraine on Principles of Preventing and Combating Discrimination in Ukraine (2013) <https://cutt.ly/SJ9Kjre> accessed 10 June 2022, Articles 1, 5, 6.

[334] Law of Ukraine on Personal Data Protection (2014) <https://cutt.ly/YJ9JCM5> accessed 10 June 2022, Article 7(2).

processing of one's data, access such data, deny its processing, request its rectification and removal, and be protected from automated decision-making, which has legal consequences.[335] However, researchers noticed that Ukrainian legislation does not qualify facial images as a form of personal data,[336] making the requirement of certification or attestation inapplicable to the FRT recognizing faces or vehicles.

The biggest problem with data protection legislation in Ukraine remains Its fragmented and outdated character, addressing mostly the legal challenges existing in 2010-2012 rather than current outstanding issues. This problem has been repeatedly raised by the civil society,[337] international community[338] and business industry.[339] As a reasonable consequence, the Draft Law №5628 on personal data protection was registered in 2021, directly aimed at shifting the focus to the European standards under the Convention 108+, the GDPR and the ECtHR's practice. The experts' feedback on this document was predominantly positive,[340] although some concerns were expressed regarding the regulation of video surveillance. In particular, the neither technical nor legal difference is made between ordinary surveillance and the FRT, which *de facto* enables law enforcement to operate the FRT surveillance regardless of the circumstances. This, in turn, might directly contravene the provisions of the European Commission's Proposal on AI regulation, which legitimizes the FRT use in three exceptional cases. Moreover, no mechanism is provided for the removal of data on a particular person from the general recordings of demonstrations or other public gatherings. Accordingly, the main principles of data processing are underexplained and non-clarified in the area of surveillance regulation. Meanwhile, it is proposed to

---

[335] *Ibid*, Articles 8, 20.

[336] Тетяна Авдєєва, 'Чи легально встановлювати на міських вулицях камери із системою розпізнавання облич?' (*ЦЕДЕМ*, 30 June 2021) <https://cutt.ly/5J0HhBO> accessed 10 June 2022.

[337] ЦЕДЕМ, 'Захистити персональні дані: новий законопроєкт' (*ЦЕДЕМ*, 9 June 2021) <https://cutt.ly/cJ90bfL> accessed 10 June 2022.

[338] CoE, 'Новий законопроєкт про захист персональних даних – експертні консультації за підтримки спільного проєкту ЄС та Ради Європи' (*CoE*, 20 November 2020) <https://cutt.ly/2J90DUN> accessed 10 June 2022.

[339] Юлія Бруско, 'Законопроєкт про захист персональних даних подано до Верховної Ради України' (*Sayenko Kharenko*, 14 June 2021) <https://cutt.ly/7J92ra8> accessed 10 June 2022.

[340] Тетяна Авдєєва та інші, 'Індекс регулювання онлайн-простору 2021' (*Інтерньюз-Україна*, 2021) <https://cutt.ly/IJ99vBm> accessed 10 June 2022.

supplement the legislation on personal data protection with the law,[341] establishing the Regulator in this area. This body will supervise the policies of developers of technologies, conduct an independent oversight over the mass processing of personal data by law enforcement and other authorities. Also, the Regulator can be empowered to authorize AI-drive surveillance, serving as the first instance for appeal of excessive or illegal intrusions.

Apart from the general framework for the protection of personal data, surveillance issues are addressed in the special laws defining the powers of law enforcement. In this respect, the National Police has recently been empowered with a capacity to supplement its registers and databases of the Ministry of Internal Affairs with information taken from information-communication systems, while data about any interaction with such systems remain in their electronic archives.[342] Importantly, no court order is needed for the collection of information. Although being introduced in the law devoted to strengthening the law enforcement capacities in martial law, this particular amendment will remain in force even in peaceful times. Since information-communication systems, according to the Law on Protection of Information in Information-Communication Systems,[343] comprise video surveillance, potentially extending even to the FRT databases, the law enforcement authorities *de facto* are granted unlimited powers not only to review this information but also to permanently integrate it into their data banks. Also, the National Police was empowered use to "*software for analytical processing of photo and video information, including for the identification of persons and license plates of vehicles*".[344] Similarly, to the previous provision, no requirement to obtain a court order, as well as no subsequent judicial review is established. Thus, the FRT is nowadays regulated by the several lines in the

[341] Draft Law №6177 on the National Commission for Personal Data Protection and Access to Public Information (2021) <https://cutt.ly/jJ98pBX> accessed 10 June 2022.

[342] Draft Law №7147 on Amendments to the Laws of Ukraine "On the National Police" and "On the Disciplinary Statute of the National Police of Ukraine" in order to optimize the activities of the police, including during martial law (2022) <https://cutt.ly / 6J98YIL> accessed 10 June 2022, Part 1(7).

[343] Law of Ukraine on Information Protection in Information and Communication Systems (1994) <https://cutt.ly/6J98YIL> accessed 10 June 2022, Article 1.

[344] Law of Ukraine on National Police (2015) <https://cutt.ly/rJ952KB> accessed 10 June 2022, article 40.

Law on National Police instead of developing a comprehensive framework with appropriate safeguards against abuses. Existent regulation neither provides for a procedure of deployment of FRT nor for maintenance of adequate functioning.

Interestingly, the amendments to the Law on Security Service of Ukraine likewise propose to empower the Security Service with access to any database of the law enforcement authorities, municipal authorities and other State organs in a free and uncontrolled manner.[345] No review of the access operations is conducted by the court or other independent bodies, thus creating the risks of establishing a so-called "police State", where law enforcement can profile any individual, conducting permanent monitoring of citizens' activities.

The Code of Criminal Procedure of Ukraine has been recently amended with Article 245[1], enabling the investigators and prosecutors to collect information from the technical devices (including filming and video recording devices), which operate in publicly accessible places, including in automatic mode.[346] This novelty once again enables investigating authorities to access street surveillance without any court review, thus opening a space for abusive practices. Importantly, no special provisions ensuring the protection of journalistic sources or other types of confidential information have been incorporated. Neither have amendments included the special protection for activists and prohibition of the deployment of the FRT in course of the peaceful demonstrations. Hence, the fragmented regulation only grants powers to intervene, not the guarantees of human rights protection, creating a risky legal framework.

Basically, the framework regulation of surveillance measures had to be provided in the National Human Rights Strategy of 2015, under which the Action Plan 2021-2023 has been approved by the Cabinet of Ministers.[347] The Action Plan prescribes

---

[345] Draft Law №3196-d on Amendments to the Law of Ukraine "On the Security Service of Ukraine" on Improving the Organizational and Legal Basis of the Security Service of Ukraine (2020) <https://cutt.ly/oJ96kfn> accessed 10 June 2022, Article 13(6).

[346] Law of Ukraine on Amendments to the Criminal Procedure Code of Ukraine and the Law of Ukraine "On Electronic Communications" to Increase the Effectiveness of Pre-Trial Investigations "On Hot Tracks" and Counteraction to Cyberattacks (2022) <https://cutt.ly/3J96OGi> accessed 10 June 2022, Part 12.

[347] Order of the Cabinet of Ministers of Ukraine "On approval of the action plan for the implementation of the National Strategy for Human Rights for 2021-2023" (2021) <https://cutt.ly/ZJ3qGOb> accessed 10 June 2022.

operational and covert investigative measures, an exhaustive list of guarantees and recommendations on human rights compliance while applying video surveillance systems. However, none of the listed actions has been implemented. The previous Action Plans containing similar provisions found no practical manifestation either. Yet, despite the absence of legal regulation, the FRT surveillance is applied in practice.

Nowadays Ukrainian law enforcement have an access to approximately 19,000 surveillance cameras in 25 regions with more than 2,000 being equipped with FRT.[348] The "Safe City" program is actively implemented in Kyiv, Zaporizhzhia, Dnipro, Chernivtsi, Lviv and many other Ukrainian cities. For instance, in Uzhhorod, the library of the FRT cameras comprises more than 30,000 face samples, having an alarm function for critical situations, with access to the system being granted to the law enforcement authorities.[349] Similarly, in Vinnytsia, AI-driven video surveillance was operated by law enforcement authorities with only two individuals conducting the monitoring over the system,[350] neither of them having an independent oversight nature. Likewise, the data from Kyiv's underground FRT cameras is analysed by the police, municipal guards, the State emergency services, as well as is used for statistical purposes.[351] No unified approach is developed regarding the access to the FRT and their operation.

Most cameras are deployed and operated by the local authorities or the municipal enterprises, authorized by the municipal councils. The most detailed regulation is developed in Zaporizhzhia, where the city council adopted the Regulations for the use

---

[348] Ukraine Crisis Media Center, 'В Україні працює близько 19 тисяч камер відеоспостереження, але бракує законодавчого регулювання – експерти' (*Ukraine Crisis Media Center*, 2021) <https://cutt.ly/RJ3eD5f> accessed 10 June 2022.

[349] Телеканал Sirius, 'Смарт-камери по 50 тис. грн. закуплять в Ужгороді' (*Телеканал Sirius*, 19 March 2019) <https://cutt.ly/pJ3eJBI> accessed 10 June 2022.

[350] Марія Лєхова, 'Розпізнавання номерів і облич: що це за система Vezha, яка запрацює у Вінниці' (*20minut*, 22 February 2021) <https://cutt.ly/6J3rr6t> accessed 10 June 2022; Вінницька міська рада, 'У Вінниці функціонують вже 111 камер зі штучним інтелектом' (*Вінницька міська рада*, 27 April 2022) <https://cutt.ly/8J3roGf> accessed 10 June 2022.

[351] Українська правда, 'Київ закупив камери: розпізнавати обличчя і температуру, дані передаватимуть поліції' (*Українська правда*, 3 April 2020) <https://cutt.ly/UJ3rcLf> accessed 10 June 2022.

and operation of the video surveillance system of Zaporizhzhia,[352] dwelling upon the general principles of systems functioning and access to the biometrics contained therein. However, it still fails to address the attestation of the system, access to one's biometrics, rectification and removal of personal data and many other issues. And, most importantly, the Regulations were adopted based on the Law on Municipal Authorities in Ukraine,[353] which does not empower local councils with the capacity to deploy the FRT or authorize any installation of surveillance mechanisms.

Nevertheless, despite the lack of legal grounds, AI-driven surveillance is used in different public places, including roads and public transport stations, schools and State authorities' premises. The tenders are regularly announced,[354] yet without any unified technical requirements for the systems, which might frequently lead to the preference for cheaper rather than qualitative technologies. Moreover, no standard on the storage and access to biometrics is provided, as well as the mechanism for removal of personal data. Especially, it is relevant for the cases, where the system is composed of the children's biometrics[355] and individuals cannot avoid the surveillance effect (being put before the choice of either accessing public spaces or having one's privacy safeguarded). Therefore, the FRT remain in the legal "grey zone", while their use often amounts to an unfettered discretion, seriously violating human rights standards.

Lack of regulation raises two main problems: the absence of technical standards for deployment of the FRT and individuals deprived of effective remedies in case of violations. On the one hand, the research shows a 95% success rate, when the FRT are applied in the search for missed children.[356] Yet, a more large-scale application provides only 18 positive results in 450 cases of the FRT application in Lviv

---

[352] Zaporizhzhia City Council, Regulations on the video surveillance system of the city of Zaporizhzhia (2019) №23; Zaporizhzhya City Council, Regulations for the use and operation of the video surveillance system of the city of Zaporizhzhia (2019).

[353] Law of Ukraine on Local Self-Government in Ukraine (1997) <https://cutt.ly/WJ3kY0s> accessed 10 June 2022.

[354] Ольга Татаренко, 'У Рівному будуватимуть систему відеоспостереження. Де будуть камери і що вони зможуть' (Suspilne Media, 1 December 2021) <https://cutt.ly/xJ3kakj> accessed 10 June 2022.

[355] Prozorro, 'Нове будівництво комплексної системи відеоспостереження та відеоаналітики у Рівненській міській територіальній громаді' (*Prozorro*, 2021) <https://cutt.ly/wJ3jK9x> accessed 10 June 2022.

[356] LB.ua, 'У Києві тестують програму розпізнавання облич за допомогою камер відеоспостереження' (*LB.ua*, 8 February 2019) <https://cutt.ly/mJ3jFTo> accessed 10 June 2022.

(effectiveness around 3,5%),[357] which can be reasoned by the low quality of technical equipment in absence of the legally fixed standard. A mistake rate will be even higher, where individuals targetedly act to overcome the systems' effect. For instance, Israeli research has shown that the presence of makeup over one's face decreases the efficiency of the FRT 30 times, making its accuracy around 1,22% compared to 47,57% in ordinary circumstances.[358] Since the deployment of the FRT with effectiveness of less than 1% would simply amount to a waste of the State or municipal budget, at least the threshold for efficiency of the system shall be provided on the legislative level.

As regards the effective remedies issue, the absence of the legal definition of the FRT and technical standards for their organisation might lead to massive data leakages, non-consensual use of biometrics, and various other misuses. Simultaneously, individuals will be deprived of the complaints mechanism given non-defined responsible individuals, standards to be appealed and the list of applicable remedies. For example, the hackers' attack on 13-14 January 2022 on application "Diya", databases of Ministry of Foreign Affairs, Ministry of Healthcare and other State services with a subsequent leak of large amounts of personal data caused no meaningful investigation, ending up with no remedy procedure.[359] One of the reasons behind the absence of the remedy procedure is the under-regulation of this issue at the State level. Respectively, the FRT shall be introduced as a legal phenomenon with the instances of its use being specifically regulated on the level of law. Although nowadays such acts do not exist despite the application of the FRT in practice, several proposals for legal framing of this technology were already made public by the competent authorities.

[357] Твоє Місто, 'Камери, що бачать знаки та обличчя або що міська рада знає про вас' (*Твоє Місто*, 2019) <https://cutt.ly/GJ3hNJT> accessed 10 June 2022.

[358] Toi Staff, 'Israeli researchers bypass facial recognition using AI-generated makeup patterns' (*The Times of Israel*, 1 October 2021) <https://cutt.ly/7J3hKax> accessed 10 June 2022.

[359] Всеволод Некрасов, 'Чергова масована кібератака на Україну: як це стало можливим та які наслідки' (*Економічна правда*, 14 January 2022) <https://cutt.ly/QJ3hvy4> accessed 10 June 2022.

3.2. Proposals for the legal regulation of the facial recognition technologies in Ukraine

3.2.1. Review of existing initiatives for the facial recognition regulation

The Kyiv police have communicated the decrease in the crime rate following the installation of the FRT surveillance with 34% of crimes being investigated via video cameras (124 wanted individuals successfully apprehended).[360] Moreover, the FRT surveillance is deployed not only for the search of wanted or missed individuals. Nowadays installation of such systems pursues the goals of maintaining security in educational institutions,[361] and even controlling the mask regime, social distance and conducting the temperature screening during the COVID times.[362] Additional COVID-oriented functions have already been criticised in Europe given their excessive intrusiveness and violation of the principle of data minimisation.[363] Albeit, in Ukraine the COVID epoch has faded against the backdrop of the full-scale Russian invasion.

Video surveillance and the FRT became useful tools in detecting the occupants, recording the perpetrators and various threats to the public order and security. For example, in the Kyiv region, the video surveillance enabled the identification of the looters,[364] who tried to break into the local gas station. Apart from that, Ukraine started deploying the FRT produced by the highly criticised Clearview AI for identification of the dead occupants, Russian soldiers and saboteurs,[365] reuniting refugees with their families,[366] assisting Ukrainian authorities in uncovering false messages on war-related

---

[360] Євгенія Підгайна, 'Керівник "розумного" Києва: "Цього року хочемо на 100% "закрити" камерами всі виїзди та в'їзди до міста"' (*Mind.ua*, 30 November 2021) <https://cutt.ly/FJ3gDl4> accessed 10 June 2022.

[361] Портал МВС, 'МВС працює над цифровим проєктом "Безпечна країна", відбулося громадське обговорення - Ігор Бондаренко' (*Портал МВС*, 10 December 2021) <https://cutt.ly/GJ3gcj1> accessed 10 June 2022.

[362] Наталія Пристанська, 'В Україні з'являться камери, які фіксуватимуть порушників карантину: коли й в яких містах' (24 Харків, 12 October 2021) <https://cutt.ly/lJ3f6f3> accessed 10 June 2022.

[363] Max Opray and Angela Skujins, 'Eyes on facial recognition in home quarantine app' (*InDaily*, 3 December 2021) <https://cutt.ly/eJ3fJbk> accessed 10 June 2022.

[364] Володимир Хлєбников, 'На Київщині мародери-колаборанти погоріли через несподівано увімкнені відеокамери' (*Big Kyiv*, 23 April 2022) <https://cutt.ly/CJ3fSa8> accessed 10 June 2022.

[365] Геннадій Лубенець, 'Дозволить опізнати вбитих окупантів та розвіяти кремлівські фейки: Україна отримає потужний інструмент' (*Telegraf*, 14 March 2022) <https://cutt.ly/YJ3faRG> accessed 10 June 2022.

[366] Вадим Карпусь, 'Україна почала використовувати технологію розпізнавання облич Clearview AI' (*ITC.ua*, 14 March 2022) <https://cutt.ly/vJ3fvVn> accessed 10 June 2022.

topics on social media.[367] Although Ukraine is not the first country to use the FRT to identify combatants,[368] the scale of applying such technologies is significant, which has raised a wave of criticism. For instance, the experts notice that the FRT of Clearview AI is far from perfect,[369] which is risky at the checkpoints and on the battlefield and can lead to civilian causalities, unlawful apprehensions and prosecutions. Furthermore, it is almost impossible to meaningfully control the use of technology and prevent abuses in the area of armed conflict. Moreover, the biggest area for criticism still implies the way Clearview AI collects personal data, *i.e.* searching the social media and other available images in the public domain, and downloading them without a person's consent. Since this company primarily uses unlawfully obtained biometrics, its use even in the exceptional circumstances of the armed conflict *de facto* legitimizes such procedures of data collection. Given the fact that approval of such techniques for composing the AI systems never serves the purposes of human rights protection, the State had to search for the less intrusive options for detecting dangerous individuals.

In response to criticism of Clearview AI, Ukrainian companies YouControl and Artellence with the support of the Security Service of Ukraine developed an application "TyHto".[370] Instead of deploying the FRT, this application uses identifying numbers of personal IDs and names to find the matches with the database of dangerous individuals, such as "Myrotvorets". However, as was further established, the effectiveness of the system is relatively low. Accordingly, its use in the course of armed conflict might also lead to misapprehensions and even mistaken shooting, seriously endangering the integrity of civilians. Nevertheless, according to the Ukrainian authorities, similar

[367] Олексій Морозов, 'Україна почала використовувати систему розпізнавання облич Clearview AI. Як вона допоможе' (*The Village*, 14 March 2022) <https://cutt.ly/5J3fwaZ> accessed 10 June 2022.

[368] Джеймс Клейтон, 'Як штучний інтелект допомагає ідентифікувати загиблих в Україні' (*BBC News Україна*, 14 April 2022) <https://cutt.ly/9J3dNUT> accessed 10 June 2022.

[369] Фокус, 'Міноборони України використовуватиме технологію розпізнавання осіб Clearview AI' (*Фокус*, 14 March 2022) <https://cutt.ly/iJ3aaMa> accessed 10 June 2022.

[370] Asya Harbuzova, 'В Україні створили програму для миттєвої перевірки осіб. Розробники просять пришвидшити розгляд застосунку в Play Store' (*DOU*, 9 April 2022) <https://cutt.ly/XJ3pQVU> accessed 10 June 2022.

technologies have already detected more than 200 combatants and deserters,[371] although the detailed reports on the mistake rate were not published. Only a couple of examples of the misidentification were outlined in the media,[372] stressing the unreliable nature of the FRT for the apprehension of individuals and the impossibility of the AI-driven surveillance use as a source of evidence for the prosecution of perpetrators.

On the one hand, the AI-driven surveillance showed its relative effectiveness, speeding up the investigative processes and decreasing the crime rate, making identification processes easier, and, generally, possible. On the other, underregulated and sometimes uncontrolled application of the FRT has already led to several challenging situations. To exemplify, a Kyrgyzstan citizen tried to set an explosive device on the car of an employee of the Chief Intelligence Directorate of the Ministry of Defence, the location of which he discovered from the "Smart city" database.[373] Another case relates to the tracking of the first deputy director of the State Bureau of Investigation based on data disclosed by the FRT operator.[374] Finally, in the aftermath of Sternenko's support protests near the Office of the President of Ukraine, the ex-deputy Minister of Internal Affairs of Ukraine has stated that allegedly violent activists will be identified through the cameras with the FRT.[375] Although subsequently no investigation results have been announced, it might be ascribed to the low quality of the deployed technology, not the absence of desire to identify activists via the AI-driven surveillance.

These three situations are only a few examples of misuses and potential abuses, done for the sake of blackmailing, threatening the life and security of individuals,

---

[371] Катерина Тищенко, 'Завдяки штучному інтелекту на блокпостах затримали 200 бойовиків і дезертирів – МВС' (*Українська правда*, 25 April 2022) <https://cutt.ly/bJ3o4iL> accessed 10 June 2022.

[372] Вікторія Андрєєва, 'Ймовірно, штучний інтелект помилився: розслідувачі встановили іншу особу мародера з Ірпеня' (*Українська правда*, 28 May 2022) <https://cutt.ly/iJ3i4xM> accessed 10 June 2022.

[373] Самуїл Проскуряков та Юліана Скібіцька, 'Камери спостереження використовують у боротьбі з коронавірусом. Ми вивчили, як ця система працює в Києві й чому це небезпечно' (*Заборона*, 25 April 2021) <https://cutt.ly/wJ3izBx> accessed 10 June 2022.

[374] Ukraine Crisis Media Center, 'В Україні працює близько 19 тисяч камер відеоспостереження, але бракує законодавчого регулювання – експерти' (*Ukraine Crisis Media Center*, 2021) <https://cutt.ly/RJ3eD5f> accessed 10 June 2022.

[375] 24 канал, 'Хочуть крові, – у МВС відреагували на протести через Стерненка' (*24 канал*, 20 March 2021) <https://cutt.ly/UJ3rcLf> accessed 10 June 2022.

coercing them to inappropriately use their powers or simply persecuting someone due to one's political position. Similar situations signalize the threat of using non-certified and non-standardized systems without effective independent oversight, review and authorisation of the instances, where the FRT might be applicable. Since the danger during the armed conflict only exacerbates, the threshold for the deployment of these technologies from both legal and technical perspectives is higher, requiring more guarantees of effective functioning and safeguards against arbitrary use.

Although no regulatory proposals have been developed in respect of technologies deployed for military purposes, the Ministry of Internal Affairs has announced the "Safe Country" project,[376] which is expected to amend the existing legislation expanding the law enforcement powers. According to the presentation of the Ministry, the purpose of the system will be to ensure the security of the citizens, centralized collection and storage of data, decreasing the threats of terrorist attacks, and monitoring of the city infrastructure's effective functioning.[377] As regards the substance of the proposal, certain risks have to be outlined. For example, the document provides for empowering the municipal authorities with the function of ensuring the monitoring of security. However, no safeguards for human rights, requirements towards such systems, or restrictions over the cases of its use are developed. *De facto*, the proposed regulation lifts the problem with the unfettered discretion of the municipal councils, but does not guarantee technically and legally compliant FRT functioning. Moreover, the Draft Law proposes to empower the National Police with the function to get real-time access to the State electronic information resources, automated information and reference systems, registers and databases, integrated security monitoring systems without any judicial oversight. This, in turn, contravenes the international standards in the surveillance area. Apart from that, the idea of granting the law enforcement direct operational, real-time access to automated information systems, registers and databases provides the National Police with unlimited powers in conducting surveillance and

[376] Проєкт Закону України "Про внесення змін до деяких законів України щодо моніторингу стану безпеки" (*Національна поліція України*, 8 November 2021) <https://cutt.ly/mJ3uv2c> accessed 10 June 2022.

[377] Міністерство внутрішніх справ, Концепція створення та впровадження програмно-апаратного комплексу "Безпечна країна" (*МВС*, 2019) <https://cutt.ly/XJ3yLLH> accessed 10 June 2022.

collecting biometrics. Lastly, not only access but the right to create one's AI-driven surveillance systems amounts to overly intrusive practice, undermining the very essence of privacy. Neither safeguards against the discriminatory nature of algorithms, nor guarantees of security for vulnerable groups are enshrined in the draft law, while the technical side of it is left for the discretion of deployers. Respectively, the proposed legal regulation is weak and overly broad, enabling excessive interference of public authorities into citizens' privacy.

A relatively similar legislative proposal has been drafted in 2019,[378] elaborating on the systems of monitoring the state of security. However, this project was highly criticised by the Chief Scientific and Expert Department of the Parliament due to overly broad discretion granted to the State and municipal authorities.[379] Among the critical remarks, the reviewers have also mentioned the necessity of authorizing such measures by the relevant judicial or oversight bodies. Moreover, the expenses for the installation and maintenance of monitoring systems were considered a potential obstacle to their effective implementation. Accordingly, the experts criticised the very essence of the general monitoring measures (which likewise cover the notion of the FRT), arguing their incompatibility with the human rights standards.

Lastly, the Draft Law №7267-1 on counterintelligence activities in Ukraine proposes to empower the Security Service of Ukraine with the capacity to access any video surveillance system without a court order during martial and emergency law periods.[380] Yet, in peaceful times the access to such systems is restricted for security services or being limited to the authorisation by the court. Accordingly, the relevant safeguards are incorporated into the draft law, however, cumulatively with the proposal on the "Safe Country" project, it also might create significant risks for human rights. It can be reasoned by the intention to establish a unified information-communication

[378] Draft Law №10120 on Amendments to Certain Legislative Acts of Ukraine on Security Monitoring Systems (2019) <https://cutt.ly/fJ3yb6K> accessed 10 June 2022.

[379] Conclusion of the Main Scientific and Expert Department to the draft Law of Ukraine "On Amendments to Certain Legislative Acts of Ukraine on Security Monitoring Systems" (2019) <https://cutt.ly/4J3ypuf> accessed 10 June 2022.

[380] Draft Law №7267-1 on Amendments to Certain Legislative Acts of Ukraine on Improving the Legal Framework for the Organization and Implementation of Counterintelligence Activities in Ukraine (2022) <https://cutt.ly/1J3tJsq> accessed 10 June 2022.

system, which will create network access for all law enforcement and security services. Even though the idea of enhancing safety is particularly relevant, especially against the backdrop of armed aggression, safeguards shall be provided to ensure the human rights compliance of the deployed systems. The critical assessment of the proposed or practically applied initiatives, on the contrary, shows the enhanced risks for human rights stemming from the uncontrolled deployment of the FRT. This finding only supports the idea of the disproportionately intrusive nature of AI-driven surveillance regardless of the State's human rights record or the circumstances of the systems' installation.

3.2.2. Recommendations for regulation of the facial recognition in Ukraine

Safety policies imply a complex mechanism of ensuring a secure environment within the State, diligent investigation of the violations, and effective remedies, where the breaches occur on the side of the law enforcement authorities. Security measures shall be balanced with the interests of the citizens to remain anonymous, confidential in communications, professional and public activities, safe from potential tracking and persecution. To achieve this end goal, the legislative authorities shall consider strengthening the human rights protection framework in the area of the FRT surveillance. In particular, the recommendations for amending the national law and policy regulations involve:

- Development of the complex safety policies, where the FRT would be the supplementary tool for safeguarding public order rather than a central element of the security system. The State shall pay significant attention to the development of the street lighting system (having the effect of decreasing the crime rate),[381] creating comfortable and accessible public spaces, opening the temporary shelters for the homeless people and victims of violence.
- Ensure the availability of alternative sources of information on the security rate, including the victimological surveys, NGO reports, international fact-finding

[381] Анастасія Боброва та інші, 'Дані про безпеку в Україні: обмеження відомчих показників і наявних підходів' (*Cedos*, 27 May 2021) <https://cutt.ly/fJ9GUd5> accessed 10 June 2022.

missions, police reports, the Ombudsperson reports *etc*. Development of the Security Strategy shall be based on the comprehensive analysis of all available data, which enables the detection of the main threats to public safety and their combating via the narrowly tailored restrictive measures. Hence, the FRT and other AI-driven tools shall not be viewed as the only options for maintaining public security and order.

- Deployment of any FRT surveillance system should be prohibited until a comprehensive legal framework, governing the development, testing and application of such technologies are established. Use of any deployed FRT surveillance should be suspended, *i.e.* AI-driven functions shall be turned off, until the introduction of the technical and legal standards in this area. Importantly, this provision shall not preclude any development of new systems by the industry and academic circles subject to their testing exclusively in laboratory conditions.
- When drafting the legal framework for the FRT surveillance, the legislator shall bear in mind that the real-time FRT surveillance application shall only be allowed in exceptional circumstances, including and limited to the targeted search for the victims of a crime, prevention of imminent and substantial threats to life or property of individuals, detection and prosecution of perpetrators or suspects of criminal offences. This requirement shall be equally applicable to the State authorities and private parties deciding to deploy the real-time FRT surveillance systems, which extend their effect beyond the private property (*e.g.* cover the area nearby supermarkets, banks or households, which falls within the notion of public space).
- Technical requirements for the FRT surveillance systems shall be developed, including the minimal requirements on cybersecurity, balanced composition of the algorithm excluding the discriminatory components, the threshold for admissible false positives and false negatives rate, clear and transparent explanatory mechanism for AI decisions. Given the high-risk nature of the FRT surveillance, a certification procedure shall be developed with the responsible

institution, experienced in legal and technical AI regulation, empowered to provide certificates and audit the FRT surveillance systems.

- The State shall provide the developers with the testing facilities with the real, where possible anonymized datasets either in the "sandbox" or in any other acceptable format. The legal framework for the exchange of personal data between domestic authorities and private actors shall be established to enable an effective testing procedure. Developers shall have an opportunity to resort to the testing platforms at any stage of the development process, verifying the human rights compliance of the FRT surveillance systems throughout their entire lifecycle. No penalties for failure to comply with the relevant international or domestic law standards shall be applicable during the testing stage.
- The National Regulator on personal data protection shall be empowered with the function to conduct independent oversight over the AI-driven surveillance systems, including being notified about the used software, characteristics of the device applied, presence or absence of the machine learning capacity, algorithm of its work and testing details (average false positives and false negatives rates). In case machine learning capacities are employed, the National Regulator shall periodically audit the FRT surveillance systems, ensuring their human rights compliance. Deployment of real-time AI-driven surveillance for the search of victims of the crimes and detection of perpetrators and suspects shall be authorized by the National Regulator in each particular case.
- The mechanism for rectification and removal of biometrics, incorporated into the system following the application of the FRT surveillance shall be developed. It shall include the right to access one's data, object to its processing, require rectification of outdated or irrelevant information, erasing of odd data (based on the principle of data minimisation), and requirement not to be subjected to the FRT surveillance, where such denial is practically feasible.
- The requirement of notifying regarding the FRT surveillance application shall be legislatively prescribed. The warning sign shall necessarily involve not only the notice of video surveillance operation in the relevant area but also the

fact that an individual will be subjected to AI-driven technology. Likewise, the warning sign shall briefly explain the algorithm of the FRT surveillance functioning (if possible, providing a brief description of the system via infographics of QR-code located in a visible and accessible place).

- Development of safeguards against uncontrolled access to the biometrics databases, especially to prevent the unfettered discretion of the law enforcement authorities. Providing the State organs with a possibility to access the databases of private actors exclusively based on the permission of the independent regulatory authority or the court order. Prohibit the uncontrolled profiling of individuals, who are not accused of or suspected in crime commission, as well as sharing their biometrics with law enforcement authorities without legitimate permission.
- Legislatively establish the maximum data retention periods for biometrics collected via the FRT surveillance. Ensure the removal of personal data from the database of the AI-driven system following the expiry of the period of data storage. Meanwhile, the databases operated by the law enforcement authorities shall be revised and made compliant with the legislative requirements.
- Prohibit the use of the FRT surveillance to target activists, human rights defenders, journalists or protesters. Ensure that AI-driven surveillance cannot be deliberately used to discriminate, persecute or otherwise negatively affect vulnerable and marginalized groups. Development and deployment of FRT shall necessarily exclude unacceptable institutional discrimination patterns, outlawing them on the system's level and ensuring their absence throughout the whole AI lifecycle (including during the machine learning process).
- An effective remedial framework shall be developed to meaningfully address the issues of human rights violations following the deployment of the FRT surveillance. Any structural gaps have to be diligently and expeditiously addressed on both legal and technical levels.

Akin to the general recommendations, the legislators shall understand the context-specific application of the FRT surveillance from the perspective of various legal

regimes to be applicable (such as martial or emergency law), as well as the necessity to consider the peculiarities of each AI-driven system. Respectively, the State regulation shall remain flexible in a technical aspect, whereas providing the solid “red lines” for impermissible practices. Finally, Ukraine shall be ready to reflect the international regulation to be developed in the sphere of AI-driven surveillance, considering the possibility of its absolute prohibition.

***

Ukrainian legal framework fails to address the peculiarities of AI-driven systems, resorting to the unification of such technologies with ordinary video surveillance. The legislation on the protection of personal data, as well as proposed regulations in the given area, still lack the incorporation of international standards on automated decision-making and biometric surveillance. Also, Ukrainian legislation lacks the legal grounds, enabling authorities to deploy the FRT surveillance, thus qualifying the acts of local councils as unfettered discretion and excess of powers. Notwithstanding the absence of legal basis underneath, the FRT surveillance is actively deployed in practice, leading to several disputable legal cases.

The proposed regulatory framework, empowering law enforcement to obtain access to the information-communication systems might create the space for various abuses, leading to excessive intrusions with privacy. Moreover, the absence of technical requirements for the FRT and legal safeguards for those, subjected to such surveillance make the proposed regulation State rather than human-centred. Moreover, the practices of FRT application during the full-scale armed conflict with particular neglect towards the background of the companies, whose technology is deployed, serves as additional proof of danger stemming from the unregulated FRT use.

Respectively, a solid legal framework shall be developed, considering all relevant international standards, ensuring technical and legal sustainability of the FRT, their capacity to meaningfully react to changing surroundings and reflect the best practices in this area. And, notwithstanding the perfectness of such systems, human oversight shall remain the necessary component of the legal framework for the FRT regulation.

CONCLUSION

Active deployment of the FRT surveillance for security purposes has raised certain questions in the human rights dimension, creating numerous obstacles for the domestic policy-making bodies. The AI-driven monitoring tools have already been employed by various democratic and authoritarian governments, whereas no regulation has yet been developed either on the international or the domestic level in any State. Accordingly, these technologies are mostly guided by the by-law documents produced by the municipal authorities, which usually lack expertise in the FRT, surveillance techniques and the data protection.

This thesis was dedicated to conducting the human rights compliance of the FRT surveillance deployed by the State authorities for security purposes. Particularly, it is important to bear in mind that the processing of biometric data by autonomous devices shall be separately addressed in the domestic laws, considering all the peculiarities of such systems. The citizens shall be notified about the FRT surveillance application, the manner and methods employed for identification of individuals, the spaces covered by the video cameras, and the procedure for removal of biometrics. While composing the systems, developers shall abstain from incorporating societal biases and institutional discrimination, thus equally representing various ethnic, gender, national and social groups. Moreover, the States shall abstain from malicious application of the AI-driven surveillance, including from programming the systems to discriminately target certain individuals, strengthening the existent inequality.

Apart from the protection of biometric data and prevention of discrimination, the States shall also consider the mitigation of the chilling effect emerging from the application of the FRT. Specifically, they shall abstain from the deployment of AI-driven surveillance against vulnerable and marginalized groups, political opposition, minorities, journalists and human rights defenders. The FRT surveillance also shall not be used to identify protesters during and after the public gatherings to avoid discouraging them from the meaningful participation in social life. Furthermore, the necessary safeguards against abuses must be present, including the establishment of the supervisory bodies, which can verify the purposes, conditions and manner of the

FRT deployment. The independent oversight shall be qualitative and effective with the experts being able to both legally and technically check the human rights compliance of the surveillance systems.

Since most FRT cannot fully comply with the mentioned requirements, while the necessary safeguards are not provided on the domestic level, the application of such technologies shall be limited until the development of a solid legislative framework and ensuring the technical feasibility of each system intended for deployment. The best solutions for the States, which already resort to application of the FRT video surveillance is to turn off the real-time biometric identification function. This solution implies the possibility to proceed with monitoring of public places without the violation of human rights, while the States would not bear unnecessary economic losses due to re-installation of technologies.

Another important aspect is the transfer of technologies to the States with a low human rights record, which shall be subjected to the strictest control and supervision to avoid oppression and human rights abuses. As this thesis shows, even the countries with a high index of human rights protection are not always able to effectively prevent mal- and misapplication of the FRT, while further distribution of technically imperfect systems only exacerbates the risks. Although the threats to democratic values are minimized in the States with efficient and developed judicial oversight, the guarantees do not suffice for the purposes of preventing human rights breaches (as happened with persecution of the Black Lives Matter activists in the US, or gender misidentification in the UK). Respectively, even the most democratic regimes cannot grant the extensive protection, thus making mass and uncontrolled application of the FRT surveillance unjustifiable and dangerous.

Lastly, mass application of the FRT surveillance in the Ukrainian underground, schools and other public spaces shall likewise be compatible with the human rights standards, being subjected to independent supervision and authorisation. The existent legal framework does not fully address the peculiarities of the AI-driven system, thus failing to grant the relevant degree of protection to Ukrainian citizens. For example, the FRT application lacks a proper basis in domestic law, being slightly defined only

in the secondary legislation. Moreover, the technical feasibility of the systems intended for installation is not verified by a competent authority, while no general technical standards are provided on the tender stages. In this manner, Ukraine actively deploys Chinese technologies, which are recognized as having a threat to the national security in the US and some other States. Accordingly, the existent regulatory framework is unsuitable for the FRT in both technical and legal aspects.

Until the development of the solid legal regulation, Ukraine shall refrain from the application of the high-risk biometric identification systems regardless of martial law period or peaceful times. The already deployed technologies must be suspended in the FRT function with a simultaneous initiation of the process of drafting the legal regulation. The best option will imply following of the EU approach embodied in the Proposal for the AI Act and related documents, which tend to become the most comprehensive regulatory documents for AI-driven surveillance. Furthermore, it will become the next step for harmonisation of Ukrainian domestic legislation with the EU standards. Otherwise, Ukraine risks facing numerous applications in the international courts for violations of its obligations under the respective human rights treaties, while Ukrainian citizens are placed in the risky legal environment with a few, if any, safeguards against the FRT malfunctioning, abuses and data leakage.

LIST OF SOURCES

1. '13 Principles for a Human Rights Respecting State Surveillance Framework' (*EFF*, 10 September 2020) <https://cutt.ly/aJ0vDqj> accessed 10 June 2022.

2. 'Beyond face value: public attitudes to facial recognition technology' (*Ada Lovelace Institute*, 2 September 2019) <https://cutt.ly/4J9aOwD> accessed 10 June 2022.

3. 'Civil Rights Concerns Regarding Law Enforcement Use of Face Recognition Technology' (*New America*, 3 June 2021) <https://cutt.ly/TJ0DBGY> accessed 10 June 2022.

4. 'Necessary and Proportionate Coalition, Necessary & Proportionate Global Legal Analysis' (*EFF*, Article 19, May 2014) <https://cutt.ly/2JHw0hy> accessed 10 June 2022.

5. 'Use of spyware to surveil journalists and human rights defenders. Statement by UN High Commissioner for Human Rights Michelle Bachelet' (*UN*, 19 July 2021) <https://cutt.ly/eJ1Xhs9> accessed 10 June 2022.

6. 'Кампания против распознавания лиц' (*Bancam.ru*) <https://cutt.ly/rJ2MLrK> accessed 10 June 2022.

7. 'У Південній Кореї протестують технологію розпізнавання облич, щоб відстежувати хворих на Covid' (*Українська правда*, 13 December 2021) <https://cutt.ly/5J0R85X> accessed 10 June 2022.

8. *1 BvR 2835/17* (Judgment of the First Senate of 19 May 2020).

9. 24 канал, 'Хочуть крові, – у МВС відреагували на протести через Стерненка' (*24 канал*, 20 March 2021) <https://cutt.ly/UJ3rcLf> accessed 10 June 2022.

10. Access Now, 'Open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance' (*Access Now*, 21 December 2021) <https://cutt.ly/dJ0zX1Q> accessed 10 June 2022.

11. ACLU, 'Coalition letter calling for a federal moratorium on face recognition' (*ACLU*, 3 June 2019) <https://cutt.ly/KJ0nbsR> accessed 10 June 2022.

12. ACLU, 'End Mass Surveillance under the Patriot Act' (*ACLU*, 2015) <https://cutt.ly/VJVttvH> accessed 10 June 2022.

13. Ad hoc Committee an Artificial Intelligence (CAHAI), Deputies' 1353rd meeting (CM/Del/Dec(2019)1353/1.5) (11 September 2019 - 31 December 2021).

14. Adi Robertson, 'Facebook is shutting down its Face Recognition tagging program' (*The Verge*, 2 November 2021) <https://cutt.ly/mJG47Jn> accessed 10 June 2022.

15. Agathe Balayn and Seda Gürses, 'Beyond Debiasing: Regulating AI and its inequalities' (*EDRi*, 21 September 2021) <https://cutt.ly/2J1xfw1> accessed 10 June 2022.

16. Aidan Wills, 'Democratic and effective oversight of national security services' (*Council of Europe Commissioner for Human Rights*, 2015).

17. Al-Haq, 'Spyware Surveillance of Palestinian Human Rights Defenders' (*Al-Haq*, 8 November 2021) <https://cutt.ly/TJ1Ck66> accessed 10 June 2022.

18. Alexander Martin, 'Police force to roll out '81% inaccurate' live facial recognition' (*SkyNews*, 24 January 2020) <https://cutt.ly/oJ9wsOi> accessed 10 June 2022.

19. Alfred Ng, 'How China uses facial recognition to control human behavior' (*CNET*, 11 August 2020) <https://cutt.ly/1J0C4Vq> accessed 10 June 2022.

20. Amanda Lentino, 'This Chinese facial recognition start-up can identify a person in seconds' (*CNBC*, 16 May 2019) <https://cutt.ly/yJ0GG7X> accessed 10 June 2022.

21. Amnesty International Report 45/002/2014 'Amnesty International submission to the intelligence and security committee's privacy and security inquiry' (Amnesty International, 7 February 2014).

22. Amnesty International, 'Ban dangerous facial recognition technology that amplifies racist policing' (*Amnesty International*, 26 January 2021) <https://cutt.ly/WJ0zAbF> accessed 10 June 2022.

23. Amnesty International, 'EU companies selling surveillance tools to China's human rights abusers' (*Amnesty International*, 21 September 2020) <https://cutt.ly/JJ2RkDt> accessed 10 June 2022.

24. Amnesty International, 'Joint Open Letter: States Must Implement Moratorium on Surveillance Technology' (*Pen America*, 27 July 2021) <https://cutt.ly/0J1Ro0u> accessed 10 June 2022.

25. Amnesty International, 'Surveillance city: NYPD can use more than 15,000 cameras to track people using facial recognition in Manhattan, Bronx and Brooklyn' (*Amnesty International*, 3 June 2021) <https://cutt.ly/PJ1CIu9> accessed 10 June 2022.

26. Amnesty International, 'The World is Watching: Mass Violations by US Police of Black Lives Matter Protesters' Rights' (*Amnesty International*) <https://cutt.ly/AJ0StxN> accessed 10 June 2022.

27. Amnesty International, 'Two Years after Snowden: Protecting Human Rights in an Age of Mass Surveillance' (*Amnesty International*, 4 June 2015).

28. Anastasiia Kruope, 'Moscow's Use of Facial Recognition Technology Challenged' (*HRW*, 8 July 2020) <https://cutt.ly/gJ21ekt> accessed 10 June 2022.

29. Andrew Kenney, 'Colorado Will Use ID.me Tech Platform to Verify Unemployment Applications, Review Fraud Flags' (*CPR News*, 13 January 2021) <https://cutt.ly/8J0PeWL> accessed 10 June 2022.

30. *Antović and Mirković v Montenegro* App no 70838/13 (ECtHR, 28 November 2017).

31. Article 19, 'ARTICLE 19 tells Strasbourg Court that mass surveillance is incompatible with the Convention' (*Article 19*, 24 April 2019) <https://cutt.ly/hJ1WWJE> accessed 10 June 2022.

32. Article 19, 'Emotion Recognition Technology Report' (*Article 19*, 2021) <https://cutt.ly/tJ0Vdrg> accessed 10 June 2022.

33. Associated Press, 'Worcester bans city use of facial recognition technology' (*New York Post*, 15 December 2021) <https://cutt.ly/mJ0AGkX> accessed 10 June 2022.

34. Asya Harbuzova, 'В Україні створили програму для миттєвої перевірки осіб. Розробники просять пришвидшити розгляд застосунку в Play Store' (*DOU*, 9 April 2022) <https://cutt.ly/XJ3pQVU> accessed 10 June 2022.

35. Bethan Davies, *Martin Innes and Andrew Dawson, An evaluation of South Wales police's use of automated facial recognition* (Cardiff Universities' Police Science Institute, Crime and Security Research Institute, 2018).

36. *Big Brother Watch and Others v the UK* Apps no 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021).

37. Big Brother Watch Team, 'UK Mass Surveillance Found Unlawful by Europe's Highest Human Rights Court' (*BBW*, 25 May 2021) <https://cutt.ly/xJHLCnP> accessed 10 June 2022.

38. Bill Goodwin, 'UK spies face landmark challenge over mass surveillance in human rights court' (*Computer Weekly*, 7 November 2017) <https://cutt.ly/bJ9dmfi> accessed 10 June 2022.

39. C-188/15 *Asma Bougnaoui and Association de défense des droits de l'homme (ADDH) v Micropole SA* [2017] ECR I-204.

40. C-207/16 *Ministerio Fiscal* [2018] ECR I-788.

41. C-291/12 *Michael Schwarz v Stadt Bochum* [2013] ECR I-670.

42. C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Othe*rs [2020] ECR I-790.

43. C-708/18 *TK v Asociaţia de Proprietari bloc M5A-ScaraA* [2019] ECR I-1064

44. C-83/14 *CHEZ Razpredelenie Bulgaria AD v Komisia za zashtita ot diskriminatsia* [2015] ECR I-480.

45. CAHAI, 'Analysis of the Multi-Stakeholder Consultation' (CAHAI, 23 June 2021)

46. Carolina Goncalves Berenger, Laura O'Brien and Peter Micek, 'OSCE Mission to Skopje supports face recognition on-site training for border police officers' (*Access Now*, 10 September 2020) <https://cutt.ly/iJ0voTg> accessed 10 June 2022.

47. *Case 12.440, Report No 26/09 Wallace de Almeida (Brazil)* (IAComHR, 20 March 2009).

48. *Case Concerning Rights of Nationals of the US in Morocco (France v the US)*, Judgment, ICJ Reports 1952, 176.

49. *Centrum För Rättvisa v Sweden* App no 35252/08 (ECtHR, 25 May 2021).

50. Charles Doyle, *Extraterritorial Application of American Criminal Law* (Congressional Research Service, 2016).

51. Charlie Campbell, "The Entire System Is Designed to Suppress Us.' What the Chinese Surveillance State Means for the Rest of the World' (*Time*, 21 November 2019) <https://cutt.ly/3J0GTEy> accessed 10 June 2022.

52. Clare Garvie, Alvaro Bedoya and Jonathan Frankle, 'The Perpetual Line-Up: Unregulated Police Face Recognition in America' (*Georgetown Law Centre on Privacy and Technology*, 18 October 2016) <https://cutt.ly/AJ0ORhf> accessed 10 June 2022.

53. CoE, 'Facial recognition: strict regulation is needed to prevent human rights violations' (*CoE*, 28 January 2021) <https://cutt.ly/vJ1MVWO> accessed 10 June 2022.

54. CoE, 'Новий законопроєкт про захист персональних даних – експертні консультації за підтримки спільного проєкту ЄС та Ради Європи' (*CoE*, 20 November 2020) <https://cutt.ly/2J90DUN> accessed 10 June 2022.

55. Conclusion of the Main Scientific and Expert Department to the draft Law of Ukraine "On Amendments to Certain Legislative Acts of Ukraine on Security Monitoring Systems" (2019) <https://cutt.ly/4J3ypuf> accessed 10 June 2022.

56. Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108), 'Guidelines on facial recognition (2021)' (CoE, 2021).

57. Council Implementing Regulation (EU) 2020/2129 of 17 December 2020 implementing Article 8a(1) of Regulation (EC) No 765/2006 concerning restrictive measures in respect of Belarus (2020) OJ L 426 I.

58. Council of Europe Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies (2013).

59. Council of Europe Explanatory Report to the Convention for the protection of individuals with regard to the processing of personal data (2018) CM(2018)2-addfinal.

60. Council of Europe Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems (2020).

61. Council of Europe Report on Mass surveillance (2015) Doc 13734.

62. Council of Europe Resolution 2045 on Mass surveillance (2015).

63. Cynthia O'Murchu, 'Facial recognition cameras arrive in UK school canteens' (The Irish Times, 21 October 2021) <https://cutt.ly/vJ9oA0N> accessed 10 June 2022.

64. *D.H. and Others v the Czech Republic* App no 57325/00 (ECtHR, 13 November 2007).

65. Dave Gershgorn, 'China's 'Sharp Eyes' Program Aims to Surveil 100% of Public Space' (*CSET*, 2 March 2021) <https://cutt.ly/yJ0HbV4> accessed 10 June 2022.

66. David Leslie, 'Understanding bias in facial recognition technologies' (The Alan Turing Institute, 2020).

67. David Meyer, 'Privacy, bias and safety: On facial recognition, Berlin and London choose different paths' (*Euractiv*, 2 February 2020) <https://cutt.ly/CJ9myCQ> accessed 10 June 2022.

68. Draft Law №10120 on Amendments to Certain Legislative Acts of Ukraine on Security Monitoring Systems (2019) <https://cutt.ly/fJ3yb6K> accessed 10 June 2022.

69. Draft Law №3196-d on Amendments to the Law of Ukraine "On the Security Service of Ukraine" on Improving the Organizational and Legal Basis of the Security Service of Ukraine (2020) <https://cutt.ly/oJ96kfn> accessed 10 June 2022.

70. Draft Law №6177 on the National Commission for Personal Data Protection and Access to Public Information (2021) <https://cutt.ly/jJ98pBX> accessed 10 June 2022.

71. Draft Law №7147 on Amendments to the Laws of Ukraine "On the National Police" and "On the Disciplinary Statute of the National Police of Ukraine" in order to optimize the activities of the police, including during martial law (2022) <https://cutt.ly/6J98YIL> accessed 10 June 2022.

72. Draft Law №7267-1 on Amendments to Certain Legislative Acts of Ukraine on Improving the Legal Framework for the Organization and Implementation of Counterintelligence Activities in Ukraine (2022) <https://cutt.ly/1J3tJsq> accessed 10 June 2022.

73. Drew Harwell and Craig Timberg, 'How America's surveillance networks helped the FBI catch the Capitol mob' (*The Washington Post*, 2 April 2021) <https://www.washingtonpost.com/technology/2021/04/02/capitol-siege-arrests-technology-fbi-privacy/> accessed 10 June 2022.

74. ECtHR, Guide on Article 10 of the European Convention on Human Rights (CoE/ECtHR, 30 April 2021).

75. EDPB Guidelines 3/2019 on processing of personal data through video devices (2020).

76. EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (AI Act) (18 June 2021).

77. EDRi, 'Civil society calls for AI red lines in the European Union's Artificial Intelligence proposal' (*EDRi*, 12 January 2021) <https://cutt.ly/UJ1nlR4> accessed 10 June 2022.

78. EDRi, 'New German government calls for European ban on biometric mass surveillance' (*EDRi*, 1 December 2021) <https://cutt.ly/tJ9Sf43> accessed 10 June 2022.

79. Elvin Ong, "Online Repression and Self-Censorship: Evidence from Southeast Asia" (2019) 56(1) Government and Opposition 1.

80. *Escher and Others v Brazil* (IACtHR, 6 July 2009).

81. European Commission Explanatory Memorandum to AI Act (2021) COM/2021/206final.

82. European Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (AI Act) and Amending Certain Union Legislative Acts (2021) COM/2021/206final.

83. European Commission White Paper on Artificial Intelligence - a European approach to excellence and trust (2020) COM(2020)65final.

84. European Parliament and of the Council Regulation 2016/679 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.

85. European Parliament Resolution 2013/2188(INI) of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs [2013] OJ C 353 E.

86. European Union Agency for Fundamental Rights, Facial recognition technology: fundamental rights considerations in the context of law enforcement (FRA, 2020).

87. Eva Dou, 'China built the world's largest facial recognition system. Now, it's getting camera-shy' (*The Washington Post*, 30 July 2021) <https://www.washingtonpost.com/world/facial-recognition-china-tech-data/2021/07/30/404c2e96-f049-11eb-81b2-9b7061a582d8_story.html> accessed 10 June 2022.

88. Frank Hersey, 'UK can join EU biometric surveillance without Parliamentary scrutiny: Statewatch' (*Biometric Update.Com*, 20 January 2022) <https://cutt.ly/7J9wRdm> accessed 10 June 2022.

89. Fred H Cate and James X Dempsey, *Bulk Collection: Systematic Government Access to Private-Sector Data* (OUP, 2017).

90. *Friedl v Austria* App no 15225/89 (EComHR, 7 December 1992).

91. *Gaughran v the UK* App no 45245/15 (ECtHR, 13 February 2020).

92. Genia Kostka, Léa Steinacker and Miriam Meckel, "Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States" (2021) 30(6) Public Understanding of Science 671.

93. German Law to improve cooperation in the field of constitutional protection came into force (2015) <https://cutt.ly/3J9Qe4H> accessed 10 June 2022.

94. Germany, "Biometrische Gesichtserkennung" des Bundespolizeipräsidiums im Rahmen der Erprobung von Systemen zur intelligenten Videoanalyse durch das Bundesministerium des Innern, für Bau und Heimat, das Bundespolizeipräsidium, das

Bundeskriminalamt und die Deutsche Bahn AG am Bahnhof Berlin Südkreuz (Bundespolizeipräsidium Potsdam, 18 September 2018).

95. Germany, Datenschutzrechtliche Prüfung des Einsatzes einer Gesichtserkennungssoftware zur Aufklärung von Straftaten im Zusammenhang mit dem G20-Gipfel durch die Polizei Hamburg (Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, 2018).

96. Hamburg Data Protection Authority, Consultation prior to an order pursuant to Article 58(2)(g) GDPR (2020).

97. *Horváth and Kiss v Hungary* App no 11146/11 (ECtHR, 23 January 2013).

98. HRW, 'Russia Expands Facial Recognition Despite Privacy Concerns' (*HRW*, 2 October 2020) <https://cutt.ly/VJ2R1Sl> accessed 10 June 2022.

99. HRW, 'Russia: Broad Facial Recognition Use Undermines Rights' (*HRW*, 15 September 2021) <https://cutt.ly/HJ2Irxz> accessed 10 June 2022.

100. Huimin Li, *Human Rights in the Age of Surveillance: China's Expansion of Technological and Normative Power* (New York University, May 2020).

101. Hunton Andrews Kurth, 'China Publishes Draft Security Standard on Facial Recognition' (*National Law Review*, 29 April 2020) <https://cutt.ly/7J0H13A> accessed 10 June 2022.

102. Hussain Syed, 'How Human Rights is Facing up to Mass Surveillance' (*The British Institute of Human Rights*, 2019) <https://cutt.ly/LJ1RaRZ> accessed 10 June 2022.

103. Ian Carlos Campbell, 'Moscow adds facial recognition payment system to more than 240 metro stations' (*The Verge*, 15 October 2021) <https://cutt.ly/GJ2T5SM> accessed 10 June 2022.

104. Jacques Follorou, 'France's tepid intelligence reform' (*AboutIntel*, 7 June 2021) <https://cutt.ly/cJVqMsO> accessed 10 June 2022.

105. Jane Wakefield, 'AI emotion-detection software tested on Uyghurs' (*BBC News*, 26 May 2021) <https://cutt.ly/tJ0VqON> accessed 10 June 2022.

106. Jawahitha Sarabdeen, "Protection of the rights of the individual when using facial recognition technology" (2022) 8(3) Helyon 1.

107. Jeremy Hainsworth, 'US ‘mass surveillance’ company challenges B.C. privacy watchdog order' (*Pique*, 24 January 2022) <https://cutt.ly/hJ0Sluy> accessed 10 June 2022.

108. Joined Cases C-511/18, C-512/18 and C-520/18 *French Data Network, Fédération des fournisseurs d’accès à Internet associatifs, and Igwan.net v Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l’Intérieur, and Ministre des Armées* [2018] ECR I-791.

109. Joined cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* [2016] ECR I-970.

110. Joint Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014] ECR I-238.

111. Jordan Valinsky and CNN Business, 'Opinion: Facial-recognition technology is one of the biggest threats to our privacy' (*CNN Business*, 26 February 2020) <https://cutt.ly/uJVrLfW> accessed 10 June 2022.

112. José Sánchez del Río and Cristina Conde, "Face-based recognition systems in the ABC e-gates" (2015) 340-346 9th Annual IEEE International Systems Conference 340.

113. Joy Boulamwini, 'How well do IBM, Microsoft, and Face++ AI services guess the gender of a face?' (*Gender Shades*, 2018) <https://cutt.ly/KJMagRB> accessed 10 June 2022.

114. Joy Buolamwini and others, *Facial Recognition Technologies: A Primer* (Algorithmic Justice League, 2020).

115. Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification" (2018) Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81 77-91.

116. Joy Buolamwini, 'We Must Fight Face Surveillance to Protect Black Lives' (*OneZero*, 3 June 2020) <https://cutt.ly/FJ0nuvt> accessed 10 June 2022.

117. Jurica Dujmovic, 'Opinion: Facial-recognition technology is one of the biggest threats to our privacy' (*MarketWatch*, 27 December 2021) <https://cutt.ly/OJVrHq8> accessed 10 June 2022.

118. Karen Haoarchive and Patrick Howell O'Neill, 'The hack that could make face recognition think someone else is you' (*MIT Technology Review*, 5 August 2020) <https://cutt.ly/VJVttvH> accessed 10 June 2022.

119. Kashmir Hill, 'Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match' (*The New York Times*, 29 December 2020) <https://cutt.ly/jJ0A5hx> accessed 10 June 2022.

120. Katitza Rodriguez, Cindy Cohn, and Karen Gullo, 'European Court on Human Rights Bought Spy Agencies' Spin on Mass Surveillance' (*EFF*, 26 May 2021) <https://cutt.ly/oJHC0VA> accessed 10 June 2022.

121. Kelly Hine and Robert Fleet, 'Information is key to public support for police use of facial recognition technology' (*The Conversation*, 15 December 2021) <https://cutt.ly/wJ9qpgK> accessed 10 June 2022.

122. *Kennedy v the UK* App no 26839/05 (ECtHR, 18 May 2010).

123. Kenneth Roth and Maya Wang, 'Data Leviathan: China's Burgeoning Surveillance State' (*HRW*, 16 August 2019) <https://cutt.ly/tJ0VqON> accessed 10 June 2022.

124. *Klass and Others v Germany* App no 5029/71 (ECtHR, 6 September 1978).

125. *Klayman v Obama* 957 F Supp 2d. 1 (2013).

126. Kristyna Foltynova, 'We See You! How Russia Has Expanded Its' (*Radio Free Europe*, 19 January 2021) <https://cutt.ly/9J2RITv> accessed 10 June 2022.

127. Krisztina Huszti-Orbán and Fionnuala Ní Aoláin, *Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?* (Human Rights Center, University of Minnesota, 2020).

128. Laurent Pech, *The Concept of Chilling Effect: Its Untapped Potential to Better Protect Democracy, the Rule of Law, and Fundamental Rights in the EU* (Open Society Foundation, 2021).

129. Law of Ukraine on Amendments to the Criminal Procedure Code of Ukraine and the Law of Ukraine "On Electronic Communications" to Increase the Effectiveness of Pre-Trial Investigations "On Hot Tracks" and Counteraction to Cyberattacks (2022) <https://cutt.ly/3J96OGi> accessed 10 June 2022.

130. Law of Ukraine on Information Protection in Information and Communication Systems (1994) <https://cutt.ly/6J98YIL> accessed 10 June 2022.

131. Law of Ukraine on Local Self-Government in Ukraine (1997) <https://cutt.ly/WJ3kY0s> accessed 10 June 2022.

132. Law of Ukraine on National Police (2015) <https://cutt.ly/rJ952KB> accessed 10 June 2022.

133. Law of Ukraine on Personal Data Protection (2014) <https://cutt.ly/YJ9JCM5> accessed 10 June 2022.

134. Law of Ukraine on Principles of Preventing and Combating Discrimination in Ukraine (2013) <https://cutt.ly/SJ9Kjre> accessed 10 June 2022.

135. LB.ua, 'У Києві тестують програму розпізнавання облич за допомогою камер відеоспостереження' (*LB.ua*, 8 February 2019) <https://cutt.ly/mJ3jFTo> accessed 10 June 2022.

136. Liam Gibson, 'Japan bans facial recognition tech exports due to China's human rights abuses' (*Taiwan News*, 3 January 2022) <https://cutt.ly/HJ0VO8A> accessed 10 June 2022.

137. *Liberty and Others v the UK* App no 58243/00 (ECtHR, 1 July 2008).

138. *Lingens v Austria* App no 9815/82 (ECtHR, 8 July 1986).

139. *López Ribalda and Others v Spain* Apps no 1874/13 and 8567/13 (ECtHR, 17 October 2019).

140. Loprespub, 'Taming State Surveillance: Reconciling Camera Surveillance Technology with Human Rights Obligations' (*Hillnotes*, 16 March 2020) <https://cutt.ly/IJH2TfW> accessed 10 June 2022.

141. Lord Lester of Herne Hill and Sarah Joseph, *Obligations of Non-discrimination* (OUP, 1995).

142. Lucas Introna and Helen Nissenbaum, 'Facial Recognition Technology: A Survey of Policy and Implementation Issues' (Lancaster University Management School Working Paper, 2009).

143. Luke Harding, 'Mass surveillance is fundamental threat to human rights, says European report' (*The Guardian*, 26 January 2015) <https://cutt.ly/MJHrlD5> accessed 10 June 2022.

144. *Lupker and Others v the Netherlands* App no 18395/92 (EComHR, 7 December 1992).

145. Lynsey Chutel, 'China is exporting facial recognition software to Africa, expanding its vast database' (*Quartz Africa*, 25 May 2018) <https://cutt.ly/TJ0VLgg> accessed 10 June 2022.

146. Martin Pollard, 'Even mask-wearers can be ID'd, China facial recognition firm says' (*Reuters*, 9 March 2020) <https://cutt.ly/ZJ1PySg> accessed 10 June 2022.

147. Max Opray and Angela Skujins, 'Eyes on facial recognition in home quarantine app' (*InDaily*, 3 December 2021) <https://cutt.ly/eJ3fJbk> accessed 10 June 2022.

148. Melissa Heikkilä, 'German coalition backs ban on facial recognition in public places' (*Politico*, 24 November 2021) <https://cutt.ly/PJ9IrDB> accessed 10 June 2022.

149. Moussa Sangare, 'Mass Surveillance in the Post-Covid-19 World: A Test for the United Nations' (*Global Policy*, 18 May 2020) <https://cutt.ly/qJ0RTR0> accessed 10 June 2022.

150. Naseem Tarawnah, 'Mass surveillance, press crackdowns, and punishing prisoners of conscience – impunity reigns in MENA' (*IFEX*, 8 September 2021) <https://cutt.ly/wJMaOH2> accessed 10 June 2022.

151. *Navalnyy v Russia* Apps no 29580/12, 36847/12, 11252/13, 12317/13 and 43746/14 (ECtHR, 15 November 2018).

152. Nick Statt, 'ACLU sues facial recognition firm Clearview AI, calling it a 'nightmare scenario' for privacy' (*The Verge*, 28 May 2020) <https://cutt.ly/bJ0DRcK> accessed 10 June 2022.

153. OECD Principles on AI <https://cutt.ly/VJ16vPp> accessed 10 June 2022.

154. Omar Shakir and Maya Wang, 'Mass surveillance fuels oppression of Uighurs and Palestinians' (*Aljazeera*, 24 November 2021) <https://cutt.ly/RJ1zek4> accessed 10 June 2022.

155. Order of the Cabinet of Ministers of Ukraine "On approval of the action plan for the implementation of the National Strategy for Human Rights for 2021-2023" (2021) <https://cutt.ly/ZJ3qGOb> accessed 10 June 2022.

156. OSCE ODIHR, 'Border Management and Human Rights' (OSCE, 2021).

157. OSCE, 'OSCE Mission to Skopje supports face recognition on-site training for border police officers' (*OSCE*, 30 November 2016) <https://cutt.ly/oJ0c2RY> accessed 10 June 2022.

158. OSCE, 'Summary Report: A Human Rights-Centred Approach to Technology and Security' (OSCE, 8 November 2019).

159. OVD Info, 'How Authorities Use Cameras and Facial Recognition against Protesters' (*OVD Info*, 2022) <https://cutt.ly/uJ2PrhK> accessed 10 June 2022.

160. OVD Info, 'Позиция ОВД-Инфо по массовым преследованиям в связи с акциями 23 января' (*OVD Info*, 29 January 2021) <https://cutt.ly/lJ208H8> accessed 10 June 2022.

161. Patrick Grother, Mei Ngan and Kayee Hanaoka, *Face Recognition Vendor Test (FRVT). Part 3: Demographic Effects* (Internal Report 8280, National Institute of Standards and Technology Interagency, 2019).

162. Patrick Grother, Mei Ngan, and Kayee Hanaokai, "Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification" (2018) 8238 NIST Pubs.

163. Paul Mozur, 'China’s Internet Controls Will Get Stricter, to Dismay of Foreign Business' (*The New York Times*, 7 November 2016) <https://cutt.ly/3J0JfoF> accessed 10 June 2022.

164. Paul Mozur, 'Inside China’s Dystopian Dreams: A.I., Shame and Lots of Cameras' (*The New York Times*, 8 July 2018) <https://cutt.ly/gJ2EkPk> accessed 10 June 2022.

165. Paul Mozur, Jonah M Kessel and Melissa Chan, 'Made in China, Exported to the World: The Surveillance State' (*The New York Times*, 24 April 2019) <https://cutt.ly/sJ0HtHL> accessed 10 June 2022.

166. *Peck v the UK* App no 44647/98 (ECtHR, 28 January 2003).

167. *Perry v the UK* App no 63737/00 (ECtHR, 17 July 2003).

168. Philipp Grüll, 'Germany's plans for automatic facial recognition meet fierce criticism' (*Euractiv*, 10 January 2020) <https://cutt.ly/iJ9nJVq> accessed 10 June 2022.

169. Philipp Hacker, "Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination Under EU Law" (2018) 55 Common Market Law Review 1143.

170. Pjotr Sauer, 'Privacy fears as Moscow metro rolls out facial recognition pay system' (*The Guardian*, 15 October 2020) <https://cutt.ly/uJ2TiKX> accessed 10 June 2022.

171. Privacy International, 'Biometrics collection under the pretext of counter-terrorism' (*Privacy International*, 28 May 2021) <https://cutt.ly/1JMrPw8> accessed 10 June 2022.

172. Privacy International, 'PI's submission to the UN Human Rights Committee regarding France's compliance with ICCPR' (*Privacy International*, 20 July 2021) <https://cutt.ly/TJ0b4i4> accessed 10 June 2022.

173. Privacy International, 'UK mass interception law violates human rights - but the fight against mass surveillance continues (from 2018)' (*Privacy International*, 24 May 2021) <https://cutt.ly/aJHZtR4> accessed 10 June 2022.

174. Prozorro, 'Нове будівництво комплексної системи відеоспостереження та відеоаналітики у Рівненській міській територіальній громаді' (*Prozorro*, 2021) <https://cutt.ly/wJ3jK9x> accessed 10 June 2022.

175. *R (Bridges) v CC South Wales Police and Others* [2020] EWCA Civ 1058.

176. Reclaim Your Face campaign <https://cutt.ly/xJ0xuFm> accessed 10 June 2022

177. Rob Davies, 'US facial recognition firm faces £17m UK fine for 'serious breaches'' (*The Guardian*, 29 November 2021) <https://cutt.ly/lJ9iQoZ> accessed 10 June 2022.

178. Robin Hopkins, 'Key points from the Bridges facial recognition appeal' (*Panopticon*, 3 September 2020) <https://cutt.ly/DJ9hNj5> accessed 10 June 2022.

179. Robyn Dixon, 'Russia's surveillance state still doesn't match China. But Putin is racing to catch up.' (*The Washington Post*, 17 April 2021) <https://www.washingtonpost.com/world/europe/russia-facial-recognition-surveillance-navalny/2021/04/16/4b97dc80-8c0a-11eb-a33e-da28941cb9ac_story.html> accessed 10 June 2022.

180. *Roman Zakharov v Russia* App no 47143/06 (ECtHR, 4 December 2015).

181. Ronja Kniep, 'Another layer of opacity: how spies use AI and why we should talk about it' (*AboutIntel*, 20 December 2019) <https://cutt.ly/MJC6Tl4> accessed 10 June 2022.

182. *Rupert Althammer v Austria*, Communication no 803/1998, UN Doc CCPR/C/74/D/803/1998 (2002).

183. Russell Brandom, 'French regulator tells Clearview AI to delete its facial recognition data' (*The Verge*, 16 December 2021) <https://cutt.ly/bJ0DRcK> accessed 10 June 2022.

184. Russell Brandom, 'Lawmakers call on feds to drop Clearview AI facial recognition contracts' (*The Verge*, 9 February 2022) <https://cutt.ly/2J0SmuU> accessed 10 June 2022.

185. Russell Brandom, 'Moscow's facial recognition system can be hijacked for just $200, report shows' (*The Verge*, 11 November 2020) <https://cutt.ly/3J2Yz6I> accessed 10 June 2022.

186. *S. and Marper v the UK* Apps no 30562/04 and 30566/04 (ECtHR, 4 December 2008).

187. Sally Weale, 'ICO to step in after schools use facial recognition to speed up lunch queue' (*The Guardian*, 18 October 2021) <https://cutt.ly/AJ9avBA> accessed 10 June 2022.

188. Sandra Wachter, Brent Mittelstadt, and Luciano Floridi, "Why a Right to Explanation of AutomatedDecision-Making Does Not Exist in the GeneralData Protection Regulation" (2017) 7(2) International Data Privacy Law 1.

189. Sarah Rainsford, 'Coronavirus: Russia uses facial recognition to tackle Covid-19' (*BBC News*, 4 April 2020) <https://cutt.ly/gJ2UNdN> accessed 10 June 2022.

190. *Sciacca v Italy* App no 50774/99 (ECtHR, 11 January 2005).

191. *Shimovolos v Russia* App no 30194/09 (ECtHR, 21 June 2011).

192. Steve Neavling, 'New legislation would ban facial recognition on federal level, withhold funds from cities like Detroit that use it' (*MetroTimes*, 15 June 2021) <https://cutt.ly/tJ0AO4W> accessed 10 June 2022.

193. Steven Feldstein, 'The Global Expansion of AI Surveillance' (Carnegie Endowment for International Peace, 2019).

194. *Szabó and Vissy v Hungary* App no 37138/14 (ECtHR, 12 January 2016).

195. Tambiama Madiega and Hendrik Mildebrath, Regulating facial recognition in the EU (EPRS, 2021).

196. Tatsiana Ziniakova, *Privacy, Mass Electronic Surveillance, and the Rule of Law in Times of COVID-19* (World Justice Project, 2020).

197. *Telegraaf Media Nederland Landelijke Media B.V. and Others v the Netherlands* App no 39315/06 (ECtHR, 22 November 2012).

198. The Conversation, 'A Generation Growing Under Surveillance: The Dangers of Facial Recognition In Schools' (*Interesting Engineering*, 14 November 2021) <https://cutt.ly/GJ9p4p6> accessed 10 June 2022.

199. The Jerusalem Post Staff, 'Ex-Mossad head: AI facial recognition tech superior to fingerprinting' (*The Jerusalem Post*, 21 December 2021) <https://cutt.ly/5J18aga> accessed 10 June 2022.

200. The Phuket, 'MorChana to have face recognition integrated, warn officials of foreigners outside designated Sandbox zones' (*The Phuket News*, 10 October 2021) <https://cutt.ly/5J2ED8P> accessed 10 June 2022.

201. The Russian Federation Federal Law on conducting an experiment to establish special regulation in order to create the necessary conditions for the development and implementation of AI technologies in the subject of the Russian Federation - the city of federal significance Moscow and amending Articles 6 and 10 of the Federal Law

"On Personal Data" of 2020 (№123-ФЗ) <https://cutt.ly/OJ2OmPV> accessed 10 June 2022.

202. The Russian Federation Federal Law on Personal Data of 2006 (№152-ФЗ) <https://cutt.ly/TJ2Imgx> accessed 10 June 2022.

203. Theodore Christakis and Mathias Becuywe, 'Pre-Market Requirements, Prior Authorisation and Lex Specialis: Novelties and Logic in the Facial Recognition-Related Provisions of the Draft AI Regulation' (*European Law Blog*, 4 May 2021) <https://cutt.ly/0J0Wdf1> accessed 10 June 2022.

204. *Timishev v Russia* Apps no 55762/00 and 55974/00 (ECtHR, 13 December 2005).

205. Toi Staff, 'Israeli researchers bypass facial recognition using AI-generated makeup patterns' (*The Times of Israel*, 1 October 2021) <https://cutt.ly/7J3hKax> accessed 10 June 2022.

206. Tom Simonite, 'Face Recognition Is Being Banned—but It's Still Everywhere' (*Wired*, 22 December 2021) <https://cutt.ly/nJ0O4X2> accessed 10 June 2022.

207. Tony Kingham, 'Cognitec Technologies to Capture Facial Images at German Borders' (*Border Security Report*, 25 August 2021) <https://cutt.ly/GJ9mnam> accessed 10 June 2022.

208. Tony Roberts and others, *Surveillance Law in Africa: a review of six countries* (Institute of Development Studies, 2021).

209. Tonya Riley, 'Momentum builds on federal oversight of facial recognition tech after reported abuses' (*CyberScoop*, 15 July 2021) <https://cutt.ly/LJMfIiZ> accessed 10 June 2022.

210. Tonya Riley, 'UN calls for human rights safeguards on artificial intelligence' (*CyberScoop*, 15 September 2021) <https://cutt.ly/TJMfzQY> accessed 10 June 2022.

211. Torkel Opsahl, *Equality in Human Rights Law* (Kehl am Rhein NP Engel Verlag, 1988).

212. UK Investigatory Powers Act of 2016 <https://cutt.ly/UJ9a95S> accessed 10 June 2022.

213. UK Protection of Freedoms Act of 2012 <https://cutt.ly/nJ9svLg> accessed 10 June 2022.

214. Ukraine Crisis Media Center, 'В Україні працює близько 19 тисяч камер відеоспостереження, але бракує законодавчого регулювання – експерти' (*Ukraine Crisis Media Center*, 2021) <https://cutt.ly/RJ3eD5f> accessed 10 June 2022.

215. Umberto Bacchi, 'Face for sale: Leaks and lawsuits blight Russia facial recognition' (*Reuters*, 9 November 2020) <https://cutt.ly/iJ21Wvk> accessed 10 June 2022.

216. UN Counter-Terrorism Committee Executive Directorate, 'Guidelines to facilitate the use and admissibility as evidence in national criminal courts of information collected, handled, preserved and shared by the military to prosecute terrorist offences' (UNCTED, 2019).

217. UN Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression and the Special Rapporteur for Freedom of Expression of the IAComHR, 'Joint Declaration on surveillance programs and their impact on freedom of expression' (2013).

218. UN Special Rapporteur on the right to privacy, Draft Legal Instrument on Government-led Surveillance and Privacy (Managing Alternatives for Privacy, Property and Internet Governance, 10 January 2018).

219. UNCHR 'Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance' (2017) UN Doc A/HRC/35/41.

220. UNCHR 'Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance on Combating racism, racial discrimination, xenophobia and related intolerance and the comprehensive implementation of and follow-up to the Durban Declaration and Programme of Action' (2017) UN Doc A/72/287.

221. UNCHR 'Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance' (2015) UN Doc A/HRC/29/46.

222. UNCHR 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism' (2014) UN Doc A/69/397.

223. UNCHR 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on surveillance and human rights' (2019) UN Doc A/HRC/41/35.

224. UNCHR 'Report of the Special Rapporteur on the right to privacy on Artificial intelligence and privacy, and children's privacy' (2021) UN Doc A/HRC/46/37.

225. UNCHR 'Report of the Special Rapporteur on the right to privacy on Right to privacy' (2019) UN Doc A/HRC/40/63.

226. UNCHR 'Report of the Special Rapporteur on the right to privacy' (2018) UN Doc A/HRC/37/62.

227. UNCHR 'Report of the Special Rapporteur on the right to privacy' (2017) UN Doc A/HRC/34/60.

228. UNCHR 'Report of the Special Rapporteur on the right to privacy' (2020) UN Doc A/HRC/43/52.

229. UNCHR 'Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association on exercise of the rights to freedom of peaceful assembly and of association as essential to advancing climate justice' (2021) UN Doc A/76/222.

230. UNCHR 'Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age' (2018) UN Doc A/HRC/39/29.

231. UNCHR 'Report of the United Nations High Commissioner for Human Rights on impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests' (2020) UN Doc A/HRC/44/24.

232. UNCHR 'Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age' (2021) UN Doc A/HRC/48/3.

233. UNCHR, General Comment №16 'Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation' (1988) UN Doc HRI/GEN/1/Rev.9 (Vol. I).

234. UNCHR, General Comment №37 'Article 21 (Right to Peaceful Assembly)' (2020) UN Doc CCPR/C/GC/37.

235. UNESCO, 'UNESCO member states adopt the first ever global agreement on the Ethics of Artificial Intelligence' (UNESCO, 25 November 2021) <https://cutt.ly/yJ1NKOt> accessed 10 June 2022.

236. UNESCO, Recommendation on the ethics of artificial intelligence (UNESCO, 2021).

237. UNGA 'Resolution 75/176 on the right to privacy in the digital age' (2020) UN Doc A/RES/75/176.

238. UNHR Council 'Joint report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association and the Special Rapporteur on extrajudicial, summary or arbitrary executions on the proper management of assemblies' (2016) UN Doc A/HRC/31/66.

239. UNHR Council 'The right to privacy in the digital ' (2017) UN Doc A/HRC/34/L.7/Re; Necessary and Proportionate, 'International Principles on the Application of Human Rights to Communications Surveillance' (Necessary and Proportionate, 2014).

240. UNHRC 'Concluding observations on the fifth periodic report of France' (2015) UN Doc CCPR/C/SR.3193.

241. UNSC Resolution 2396 (2017) UN Doc S/RES/2396(2017).

242. US Bill "To prohibit biometric surveillance by the Federal Government without explicit statutory authorization and to withhold certain Federal public safety grants from State and local governments that engage in biometric surveillance" (116th Congress, 2019-2020).

243. US Commercial Facial Recognition Privacy Act of 2019 (S.847) <https://cutt.ly/HJ0At7I> accessed 10 June 2022.

244. *Uzun v Germany* App no 35623/05 (ECtHR, 2 September 2010).

245. *Vajnai v Hungary* App no 33629/06 (ECtHR, 8 July 2008).

246. Venice Commission and OSCE/ODIHR Guidelines on Freedom of Peaceful Assembly (3rd Edition) (2019) CDL-AD(2019)017.

247. Venice Commission Opinion no 831/2015 'On articles 216, 299, 301 and 314 of the Penal Code of Turkey, adopted by the Venice Commission at its 106th plenary session' (2016) CDL-AD(2016)002.

248. VoaNews, 'Правозахисники у США закликали Байдена виступити проти використання технологій розпізнавання облич урядом' (*VoaNews*, 17 February 2021) <https://cutt.ly/hJ0DrBz> accessed 10 June 2022.

249. *Von Hannover v Germany (No 2)* Apps no 40660/08 and 60641/08 (ECtHR, 7 February 2012).

250. *Weber and Saravia v Germany* App no 54934/00 (ECtHR, 29 June 2006).

251. Wiebke Lamer, "From sleepwalking into surveillance societies to drifting into permanent securitisation: Mass surveillance, security and human rights in Europe" (2017) 1 Global Campus Human Rights Journal 393.

252. Will Schrepferman, 'Supervising Surveillance: Applying International Law to the Global Surveillance State' (*Harvard International Review*, 11 November 2020) <https://cutt.ly/BJNwJvV> accessed 10 June 2022.

253. William A Schabas, *The European Convention on Human Rights: The Commentary* (OUP, 2015).

254. Yuval Shany, 'On-Line Surveillance in the case-law of the UN Human Rights Committee' (*The Federmann Cyber Security Research Center – Cyber Law Program*, 13 July 2017) <https://cutt.ly/4J0PB4D> accessed 10 June 2022.

255. Zaporizhzhia City Council, Regulations on the video surveillance system of the city of Zaporizhzhia (2019) №23.

256. Zaporizhzhya City Council, Regulations for the use and operation of the video surveillance system of the city of Zaporizhzhia (2019).

257. Александр Бородихин, '"Скрыться невозможно". Как активиста "Другой России" задержали в метро по сигналу с видеокамеры, опознавшей его по ориентировке Центра "Э"' (*Медиазона*, 10 October 2018) <https://cutt.ly/dJ2NU0J> accessed 10 June 2022.

258. Анастасія Боброва та інші, 'Дані про безпеку в Україні: обмеження відомчих показників і наявних підходів' (*Cedos*, 27 May 2021) <https://cutt.ly/fJ9GUd5> accessed 10 June 2022.

259. Анна Кузнецова, 'Суд не увидел нарушения закона в неконтролируемой слежке за москвичами' (*РосКомСвобода*, 24 December 2020) <https://cutt.ly/eJ2Y2Iv> accessed 10 June 2022.

260. Вадим Карпусь, 'Україна почала використовувати технологію розпізнавання облич Clearview AI' (*ITC.ua*, 14 March 2022) <https://cutt.ly/vJ3fvVn> accessed 10 June 2022.

261. Вікторія Андрєєва, 'Ймовірно, штучний інтелект помилився: розслідувачі встановили іншу особу мародера з Ірпеня' (*Українська правда*, 28 May 2022) <https://cutt.ly/iJ3i4xM> accessed 10 June 2022.

262. Вінницька міська рада, 'У Вінниці функціонують вже 111 камер зі штучним інтелектом' (*Вінницька міська рада*, 27 April 2022) <https://cutt.ly/8J3roGf> accessed 10 June 2022.

263. Володимир Хлєбников, 'На Київщині мародери-колаборанти погоріли через несподівано увімкнені відеокамери' (*Big Kyiv*, 23 April 2022) <https://cutt.ly/CJ3fSa8> accessed 10 June 2022.

264. Всеволод Некрасов, 'Чергова масована кібератака на Україну: як це стало можливим та які наслідки' (*Економічна правда*, 14 January 2022) <https://cutt.ly/QJ3hvy4> accessed 10 June 2022.

265. Геннадій Лубенець, 'Дозволить опізнати вбитих окупантів та розвіяти кремлівські фейки: Україна отримає потужний інструмент' (*Telegraf*, 14 March 2022) <https://cutt.ly/YJ3faRG> accessed 10 June 2022.

266. Джеймс Клейтон, 'Як штучний інтелект допомагає ідентифікувати загиблих в Україні' (*BBC News Україна*, 14 April 2022) <https://cutt.ly/9J3dNUT> accessed 10 June 2022.

267. Євгенія Підгайна, 'Керівник “розумного” Києва: “Цього року хочемо на 100% “закрити” камерами всі виїзди та в'їзди до міста”' (*Mind.ua*, 30 November 2021) <https://cutt.ly/FJ3gDl4> accessed 10 June 2022.

268. Игорь Савкин, 'Система распознавания лиц в метро Москвы помогла найти преступников' (*Kod.ru*, 12 August 2021) <https://cutt.ly/JJ2YpuR> accessed 10 June 2022.

269. Катерина Тищенко, 'Завдяки штучному інтелекту на блокпостах затримали 200 бойовиків і дезертирів – МВС' (*Українська правда*, 25 April 2022) <https://cutt.ly/bJ3o4iL> accessed 10 June 2022.

270. Левада-центр, 'Видеонаблюдение в публичных местах' (*Левада-центр*, 20 August 2020) <https://cutt.ly/4J2Uu2z> accessed 10 June 2022.

271. Максим Дворовий та інші, *Цифрові права чи громадське здоров'я: цифрові права під час пандемії COVID-19 в Україні - з урахуванням кращих практик Євросоюзу* (Інститут інноваційного врядування, 2021).

272. Марія Лєхова, 'Розпізнавання номерів і облич: що це за система Vezha, яка запрацює у Вінниці' (*20minut*, 22 February 2021) <https://cutt.ly/6J3rr6t> accessed 10 June 2022.

273. Михайло Каменєв, 'Гостре око Старшого Брата' (*РПР*, 4 November 2017) <https://cutt.ly/hJ0ARc0> accessed 10 June 2022.

274. Міністерство внутрішніх справ, Концепція створення та впровадження програмно-апаратного комплексу "Безпечна країна" (*МВС*, 2019) <https://cutt.ly/XJ3yLLH> accessed 10 June 2022.

275. Наталія Пристанська, 'В Україні з'являться камери, які фіксуватимуть порушників карантину: коли й в яких містах' (*24 Харків*, 12 October 2021) <https://cutt.ly/lJ3f6f3> accessed 10 June 2022.

276. Никита Королев, 'Лицом к лицу лица не опознать' (*Коммерсантъ*, 25 September 2020) <https://cutt.ly/xJ2YPqc> accessed 10 June 2022.

277. Никита Королев, 'Регионы узнают в лицо' (*Коммерсантъ*, 25 September 2020) <https://cutt.ly/LJ2Ubxp> accessed 10 June 2022.

278. OVD News, 'Полиция всю неделю задерживает предполагаемых участников акций 21 апреля. Данные ОВД-Инфо' (*OVD News*, 24 April 2021) <https://cutt.ly/QJ22aYO> accessed 10 June 2022.

279. OVD News, 'Последствия акций протеста из-за заключения Навального. Хроника, часть 2' (*OVD News*, 22 April 2021) <https://cutt.ly/kJ24eos> accessed 10 June 2022.

280. Олександр Мельник, 'Китай став першою країною планети, де поліції видали смарт-окуляри' (*Na Chasi*, 8 February 2018) <https://cutt.ly/8J2ErrE> accessed 10 June 2022.

281. Олексій Морозов, 'Україна почала використовувати систему розпізнавання облич Clearview AI. Як вона допоможе' (*The Village*, 14 March 2022) <https://cutt.ly/5J3fwaZ> accessed 10 June 2022.

282. Ольга Кротовська, '"Великий брат спостерігає": в Китаї розробили систему, яка розпізнає обличчя навіть у масках' (*PG*, 10 March 2020) <https://cutt.ly/3J0HIOj> accessed 10 June 2022.

283. Ольга Татаренко, 'У Рівному будуватимуть систему відеоспостереження. Де будуть камери і що вони зможуть' (*Suspilne Media*, 1 December 2021) <https://cutt.ly/xJ3kakj> accessed 10 June 2022.

284. Портал МВС, 'МВС працює над цифровим проєктом "Безпечна країна", відбулося громадське обговорення - Ігор Бондаренко' (*Портал МВС*, 10 December 2021) <https://cutt.ly/GJ3gcj1> accessed 10 June 2022.

285. Проєкт Закону України "Про внесення змін до деяких законів України щодо моніторингу стану безпеки" (*Національна поліція України*, 8 November 2021) <https://cutt.ly/mJ3uv2c> accessed 10 June 2022.

286. Радіо Свобода, 'Human Rights Watch розкритикувала плани Росії розширити застосування системи розпізнавання облич' (*Радіо Свобода*, 2 October 2020) <https://cutt.ly/6J2MEUv> accessed 10 June 2022.

287. РБК-Україна, 'Правозахисники подали до суду на уряд США за масове стеження' (*РБК-Україна*, 12 June 2013) <https://cutt.ly/wJ0DSMf> accessed 10 June 2022.

288. РосКомСвобода, '"Думаете, если вы ведёте обычную жизнь, вас не могут нажатием одной кнопки подвести под статью?"' (*РосКомСвобода*, 16 December 2020) <https://cutt.ly/eJ2NlYo> accessed 10 June 2022.

289. РосКомСвобода, '“РосКомСвобода” обжаловала решение суда в деле о неконтролируемой видеослежке' (*РосКомСвобода*, 7 April 2021) <https://cutt.ly/eJ2Otfz> accessed 10 June 2022.

290. РосКомСвобода, 'История Сергея Межуева: первый кейс по ошибке системы распознавания лиц в метро' (*РосКомСвобода*, 19 November 2020) <https://cutt.ly/yJ2PxgH> accessed 10 June 2022.

291. РосКомСвобода, 'Разбор: можно ли деанонимизировать протестующих при помощи камер?' (*РосКомСвобода*, 18 February 2021) <https://cutt.ly/EJ2I81C> accessed 10 June 2022.

292. РосКомСвобода, 'Система распознавания лиц теперь ищет протестующих' (*РосКомСвобода*, 4 February 2021) <https://cutt.ly/qJ213SI> accessed 10 June 2022.

293. Самуїл Проскуряков та Юліана Скібіцька, 'Камери спостереження використовують у боротьбі з коронавірусом. Ми вивчили, як ця система працює в Києві й чому це небезпечно' (*Заборона*, 25 April 2021) <https://cutt.ly/wJ3izBx> accessed 10 June 2022.

294. Твоє Місто, 'Камери, що бачать знаки та обличчя або що міська рада знає про вас' (*Твоє Місто*, 2019) <https://cutt.ly/GJ3hNJT> accessed 10 June 2022.

295. Телеканал Sirius, 'Смарт-камери по 50 тис. грн. закуплять в Ужгороді' (*Телеканал Sirius*, 19 March 2019) <https://cutt.ly/pJ3eJBI> accessed 10 June 2022.

296. Тетяна Авдєєва, 'Чи легально встановлювати на міських вулицях камери із системою розпізнавання облич?' (*ЦЕДЕМ*, 30 June 2021) <https://cutt.ly/5J0HhBO> accessed 10 June 2022.

297. Українська правда, 'Київ закупив камери: розпізнавати обличчя і температуру, дані передаватимуть поліції' (*Українська правда*, 3 April 2020) <https://cutt.ly/UJ3rcLf> accessed 10 June 2022.

298. Фокус, 'Міноборони України використовуватиме технологію розпізнавання осіб Clearview AI' (*Фокус*, 14 March 2022) <https://cutt.ly/iJ3aaMa> accessed 10 June 2022.

299. ЦЕДЕМ, 'Захистити персональні дані: новий законопроєкт' (*ЦЕДЕМ*, 9 June 2021) <https://cutt.ly/cJ90bfL> accessed 10 June 2022.

300. Юлія Бруско, 'Законопроєкт про захист персональних даних подано до Верховної Ради України' (*Sayenko Kharenko*, 14 June 2021) <https://cutt.ly/7J92ra8> accessed 10 June 2022.