FACIAL RECOGNITION TECHNOLOGIES AND UKRAINE: HOW TO ENSURE BALANCE BETWEEN NATIONAL INTERESTS AND HUMAN RIGHTS DURING STATE OF EMERGENCY?

by Anna Liudva

LL.M Capstone Thesis
SUPERVISOR: Lorenzo Gasbarri
Central European University - Private University

June 2023

Table of Contents

ABSTRACT

Following the path of many European states, Ukraine actively retorts to the usage of facial recognition technologies, especially during the wartime. However, the absence of applicable provisions on usage of digital tools and legal safeguards for protection of personal data on Ukrainian level raises the issue of legitimacy and need for the human rights crush test. Current emergency situation in Ukraine only further complicates the issue. This work analyses the international regulation of facial recognition technologies under the paradigm of applicable standards as well as practice of Ukraine with digital technologies. This work proposes a set of recommendations to Ukrainian legislation according to which both national interests remain fulfilled and fundamental rights – protected.

INTRODUCTION

In times of constant digitalisation, mass surveillance has become a popular tool for authorities to preserve public order among individuals. One of the most often utilized surveillance tools constitutes facial recognition technology (hereinafter – FRT) – a biometric system, which uses automated methods to verify or identify a person. While performing functions, such system regularly processes all kinds of personal data, including biometric ones. Biometric data is obtained via particular technical processing and relates to the specific characteristics of the person's features that enable his/her unique identification.[1] Being equipped with artificial intelligence (hereinafter – AI) tools, FRTs can also identify emotions and expressions.

In this regard, Ukraine is one of the states which often resorts to the FRTs. Its need for biometric technologies became even more visible during the current wartime in 2022. In response to the emergent situation, the state turned to the use of Clearview AI system. Initially developed for law enforcement purposes, Clearview's technology matches the images against the database of publicly stored images scraped from websites, including social media platforms.[2] Noticeably, despite not having unified legislation on the usage of FRTs, Ukraine still retorts to digital measures without legal framework and safeguards for data subjects.[3] Taking into account the prolonged state of emergency caused by the war, arbitrary usage of FRTs by authorities may negatively influence citizen's privacy, by continuing to be applied even when the emergency ceases to exist. Therefore, the overall purpose of **written component** of the work constitutes the finding of an appropriate balance between Ukrainians' right to privacy and the state's national interests while the FRTs are applied in times of emergency.

[1] В. О. Гончаренко, ["Legal regulation of the use of facial recognition technologies"], *Journal of civil engineering: science and practical journal* 41 (2021): 56-60, p. 56.
[2] Pat Kelly, Chair, "Facial Recognition Technology and the Growing Power of Artificial Intelligence", *44th Parliament, 1st Session* (October 2022): 1-71, p. 19.
[3] Гончаренко, ["Legal regulation of the use of facial recognition technologies"], p. 58.

In terms of structure, this work will first focus on the functions of the FRTs as well as the standards of their usage proposed by the international human rights law with an additional focus on the lawful processing of biometric data. Sub-chapter will explain how the state of emergency affects the application of digital tools and provides different standard of human rights protection as well as how to avoid abuse of a person's privacy. The next chapter will be dedicated to Ukraine's experience with FRTs both through legal and policy analysis. It will also mention the war context Ukraine is currently in and the legal framework within it. Remarks will contain the findings of the analysis as well as the list of recommendations to Ukrainian law, which will be contained in the separate Annexes to this work.

Conducted analysis of Ukraine's legislation and international human rights standard will assist in subsequent advocacy campaigns toward amending Ukrainian legal framework. Moreover, as a result of the research, a recommendations list with legislative amendments will be proposed, which is the purpose of the **practical component** of this work. The amendments will be proposed on the basis of communication with the deputies from the Parliament's Committees, which will review them during the special reviewing sessions. After the recommendations are reviewed, the Committee will notify me whether they were accepted or rejected. Since Ukrainian law is still not completely developed in terms of FRT usage, the amendments submitted to the Parliament will assist Ukrainian deputies in creating a diligent legal framework that will ensure the state's interest and simultaneously protect individual rights. The advocacy campaign will also be useful for stakeholders engaged in media law who wish to develop the human rights framework. To achieve the objective of this capstone thesis, this work will use the formal legal method and documentary analysis as the main one since international conventions and law provisions will be assessed.

FACIAL RECOGNITION TECHNOLOGIES AND THEIR PURPOSE

Being part of the surveillance system, FRTs are biometric technologies used for purposes of detection, verification (one-to-one comparison, entailing comparison of the image to many images of a single person)[4], identification (one-to-many comparison, meaning comparison of the image to a database of different persons)[5] and categorisation of individuals.[6] By nature of the technology, FRTs are evidently processing biometric data, defined as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".[7] In other words, biometric data is the unique and individual information, which allows to identify the particular person.

Further, FRTs are often equipped with AI tools such as machine learning and computer algorithms,[8] which are usually called the "real-life FRTs".[9] They are able to define human expressions and emotions as well as behaviour. Said technological opportunities result in usage of FRTs for various purposes, including law enforcement, national security, and maintenance of public order.[10] They can be found in various circumstances: in the personal relationship between a user and a service (access to an application), to access certain place (physical filtering) or in a public space (live facial recognition).[11] The latter are extremely popularised since facial recognition provides much more benefits than usual procedure of identification (for

[4] Kelly, "Facial Recognition Technology and the Growing Power of Artificial Intelligence", p. 9.
[5] *Ibid*.
[6] Tambiama Madiega, Hendrik Mildebrath, "Regulating facial recognition in the EU", *European Parliamentary Research Service* (September 2021): 1-38, p. 1.
[7] Regulation (EU) 2016/679 of the European Parliament and of the Council 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), *L 119/1* (April 2016), Article 4(14).
[8] Madiega, Mildebrath, "Regulating facial recognition in the EU", p. 2.
[9] OECD, *Artificial Intelligence in Society* (Paris: OECD, 2019), p. 152.
[10] Sovantharith Seng, Mahdi Nasrullah Al-Ameen, Matthew Wright, "A First Look into Users' Perceptions of Facial Recognition in the Physical World", *Computers & Security* 105 no. 4 (February 2021): 1-22, p. 3.
[11] European Data Protection Board, "Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement", *Version 1.0* (May 2022): 1-49, p. 8.

example, fingerprints taking). In particular, FRTs are able to read information and gather data without the need of human interaction.[12]

Although FRTs overall are considered to be reliable tools,[13] they remain incredibly intrusive mechanisms within the person's right to privacy.[14] In particular, such technologies gather personal data and store it for an indefinite period of time since obtained data may be useful for the subsequent identification purposes. Moreover, FRTs constantly collect and process biometric data, which is heavily protected by the data protection rules unlike the ordinary kinds of personal data. In terms of technical application FRTs may face the "problem of error".[15] In this regard, the EU Fundamental Rights Agency underlined that "*determining the necessary level of accuracy of facial recognition software is challenging*".[16]

Since the application of the FRTs may lead to the abovementioned negative consequences, biometric technologies are subjected to numerous limitations and restrictions under the European framework.

[12] Abdulrhman M. Almansori, Mohamed Taha, Elsayed Badr, "A deep facial recognition system using computational intelligent algorithms", *PLOS ONE* 15 no. 12 (December 2020): 1-27, p. 2.
[13] A.S. Tolba, A.H. El-Baz, A.A. El-Harby, "Face Recognition: A Literature Review", *International Journal of Signal Processing* 2 no. 2 (2006): 88-103, p. 88.
[14] Philip Brey, "Ethical aspects of facial recognition systems in public places", *Journal of Information, Communication and Ethics in Society* 2 no. 2 (2004): 97-109, p. 104.
[15] *Ibid.*
[16] European Union Agency for Fundamental Rights, "Facial recognition technology: fundamental rights considerations in the context of law enforcement", *FRA Focus* (2019): 1-34, p. 9.

INTERNATIONAL REGULATION OF FACIAL RECOGNITION TECHNOLOGIES

This work will focus primarily on Ukraine, and the compatibility of its laws with the European Union framework, which embodies the legislation of the European Union (hereinafter – EU) as well as European courts' practice. Ukraine, even if it is not an EU member, regularly adopts or amends any legislation, the provisions of which are always adapted to the EU law.[17] In June 2022 European Council granted Ukraine the status of a candidate country to the EU,[18] which requires Ukraine to transpose the EU law and standards into its national legislation.[19]

Apart from the EU body of rules, Ukraine has ratified the European Convention on Human Rights (hereinafter – ECHR) recognising the jurisdiction of the European Court of Human Rights (hereinafter – ECtHR). The ECtHR's judgments will be assessed to analyse the current practice regarding the usage of FRTs. It is also essential to take into account the guidelines provided by the Committee of Ministers since Ukraine is also a member of the Council of Europe.

[17] European Commission, "Opinion on the EU membership application by Ukraine", *QANDA/22/3802* (June 2022): 1-2, p. 1.
[18] "Ukraine", *European Council, Council of the European Union*, accessed April 11, 2023, URL: https://www.consilium.europa.eu/en/policies/enlargement/ukraine/
[19] "Joining the EU", *European Union*, accessed May 23, 2023, URL: https://european-union.europa.eu/principles-countries-history/joining-eu_en

International Human Rights Law

EU Framework

Generally, on the EU level the usage of FRTs is governed by the General Data Protection Regulation (hereinafter – GDPR), binding legislation that specifies rules for the collection and processing of personal data.[20] According to GDPR, any processing of personal data should: (1) be lawful, fair, and transparent; (2) be conducted with prior consent of the data subject; (3) pursue a legitimate purpose; (4) be proportional; (5) be adequate, relevant and limited to what is necessary.[21] However, it should be reiterated that FRTs usually deal with processing biometric data. By virtue of GDPR, the latter constitute a special category of data, namely sensitive data. Herewith the processing of photographs (as will be shown later with Clearview AI) is covered by the biometric data only when such processing is done via specific technical means used to enable the unique identification or authentication of the person.[22] Article 9 of GDPR predominantly prohibits processing of such data, although still mentions an exhaustive list of exceptions to such rule,[23] which have to be interpreted restrictively.[24] Such exceptions include: (1) explicit consent of the data subject, (2) processing necessary in the field of employment and social security; (3) protection of the person's vital interests if one is incapable of giving consent; (4) processing with appropriate safeguards by a non-profit body; (5) data manifestly made public; (6) legal claims and judicial activities; (7) substantial public interest; (8) health care; and (9) public interest in public heath area.[25] Consequently, the data processing resulting from facial recognition is subjected to strict requirements. Such an approach is completely justified: facial recognition is a dangerous digital tool, which can also

[20] General Data Protection Regulation.
[21] *Ibid.*, Articles 5,6,7.
[22] *Ibid.*, Recital 51.
[23] *Ibid*., Article 9, Christopher Kuner (ed.), Lee A Bygrave (ed.), Christopher Docksey (ed.), Laura Drechsler (ed.), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford: Oxford University Press, 2020), p. 369.
[24] Kuner and others, *The EU General Data Protection Regulation (GDPR): A Commentary*, p. 375.
[25] General Data Protection Regulation, Article 9.

be used for illegal access, misuse of devices, and interference within the intimate sphere of a person's life.[26]

Nevertheless, national authorities often resort to FRTs for purposes of law enforcement, national defence, public order or public health. The most common place where FRTs in action can be found is the identification of a criminal suspected in an offence, where system checks and matches numerous photos in the database. In cases, where the data is processed by the competent authorities for the purposes of law enforcement, including investigation or prosecution of criminal offences, GDPR does not apply.[27] In turn, said activities are regulated by the Law Enforcement Directive 2016/680 (hereinafter – Directive),[28] which distinguishes from GDPR in terms of scope. As the EU Commission expert group noted, although the Directive was written in light of GDPR, the former covers activities of the law enforcement as well as criminal offences, thus establishing different grounds for data processing.[29] The Directive mirrors GDPR's fundamental principles in terms of personal data and establishes additional obligations on the law enforcement authorities who work with biometric data. In particular, the Directive also allows the processing of special categories of personal data in exceptional circumstances. Unlike GDPR, however, such processing is conducted only on the legal basis, when strictly necessary and subjected to appropriate safeguards.[30] Interestingly, while both GDPR and Directive refer to the existence of "appropriate safeguards", neither of the documents provide any explanation as to what they have to include. Thus, it is incumbent

[26] Committee of Ministers, "Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies" (June 2013), para. 6.
[27] Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, (Cham: Springer Publishing Company, 2017), p. 16.
[28] Directive (EU) 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive), *L 119/89* (April 2016).
[29] Minutes of the third meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680 (November 2016): p. 1-3, p. 1.
[30] Law Enforcement Directive, Article 10.

upon Member States to implement safeguards at the domestic level through their own resources, guided only by the fundamental tenets of GDPR.[31]

In terms of data protection, the Directive obliges states to provide appropriate and short time periods for the storage and review of personal data.[32] It is vital to follow requirements of necessity and proportionality which derive from the fact that data processing is prohibited for any other reasons other than defined purposes. Requirements of lawfulness, fairness and transparency of the data processing mainly echoes GDPR provisions.[33] Abovementioned provisions were also confirmed by the Guidelines 05/2022.[34] The document additionally emphasises the clarity of law, which has to regulate specific situations where the data is being processed, including the quantity of data, the nature of data and risks of its unlawful access.[35]

It is pertinent to mention that there is no regulation at the EU level that governs the FRTs' mechanism as the means of surveillance, except from the current laws governing data protection rules. In terms of current EU initiatives, however, the Proposal for an Artificial Intelligence Act (hereinafter – AI Act) covers some issues regarding FRTs.[36] As of now the AI Act is approved by the parliamentary committees and on the way to become new legislation for AI regulation.[37] In terms of provisions the AI Act especially emphasises on the so-called ""high-risk" AI systems", namely "*systems that pose significant risks to the health and safety or fundamental rights of persons*".[38] Noticeably, AI Act defines the FRTs as a ""high-risk" AI systems" and imposes on the latter specific requirements which include, *inter alia*, risk

[31] Kuner and others, *The EU General Data Protection Regulation (GDPR): A Commentary*, p. 381.
[32] Law Enforcement Directive, Article 5.
[33] FRA, "Facial recognition technology: fundamental rights considerations in the context of law enforcement", p. 13.
[34] EDPB, "Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement".
[35] *Ibid.*, p. 15.
[36] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, *2021/0106 (COD)* (April 2021).
[37] "AI Act: a step closer to the first rules on Artificial Intelligence", *News European Parliament*, accessed May 23, 2023, URL: https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence
[38] Artificial Intelligence Act, p. 3.

management system, data governance, technical documentation, record-keeping, transparency and provision of information to users, human oversight, accuracy, robustness and cybersecurity.[39] Therefore, while most EU provisions allow usage of FRTs by law enforcement authorities provided compliance with human rights standards, an AI Act condemns usage of "real-time" FRTs in publicly accessible spaces,[40] calling it "*particularly intrusive*" in persons' protected rights and freedoms.[41]

ECHR Framework

The usage of FRTs as well as subsequent data processing fall within the scope of person's right to privacy, protected under Article 8 of ECHR.[42] Although the concept of "privacy" is extremely broad, the right to private life remains non-absolute. Thus, for the interference within private sphere to be justified, such an interference has to comply with a restrictive three-part test, namely (a) be prescribed by law; (b) pursue a legitimate aim and (c) be necessary in the democratic society.[43] Turning to ECtHR's practice, the Court usually confirms the existence of the second criterion in actions of national authorities since the latter most of the time pursues the legitimate aim of national security or public order. For example, in the communicated case *Beghal v the United Kingdom*, which concerns the establishment of FRTs at the airports by the immigration officials, the Court agreed with domestic courts that such practice is compatible with the right to privacy since it protects national interests of the state.[44]

At the same time, ECtHR pays particular attention to the "provided by law" criterion. In this regard, the Court specifically emphasises on the existing legal regulation which allows the

[39] *Ibid.*, Chapter 3.
[40] Michael Veale, Frederik J. Zuiderveen Borgesius, "Demystifying the Draft EU Artificial Intelligence Act - Analysing the good, the bad, and the unclear elements of the proposed approach", *Computer Law Review International* 22 (2021): 97-112, p. 98.
[41] Artificial Intelligence Act, Recital 18.
[42] European Court of Human Rights, "Guide on Article 8 of the European Convention on Human Rights" (31 August 2022): 1-172, p. 56.
[43] William A Schabas, *The European Convention on Human Rights: A Commentary* (Oxford: Oxford University Press, 2017), pp. 402, 404, 406, ECtHR, *Peck v the United Kingdom*, app. no. 44647/98, paras. 67, 76.
[44] ECtHR, *Beghal v the United Kingdom*, app. no. 4755/16.

usage of surveillance systems,[45] including FRTs. Referring to the "quality of law", the Court posited that legal provisions must not be only accessible (mere existence of legal basis)[46] but also foreseeable (clearly defined circumstances and the conditions in which authorities may resort to intrusive measures).[47] However, the Court imposed additional requirements to the law governing secret surveillance (monitoring without person's awareness).[48] This is derived from the fact that persons under surveillance must have legislative guarantees and safeguards since such activity is correlated with collection of their biometric data. According to ECtHR's practice, the following minimum standards have to be met to prevent the abuse of authorities during surveillance operations:

- clear list of activities regarding which the surveillance can be used;
- indication of who may be subjected to surveillance;
- time limit of the surveillance;
- developed mechanism of storage and examination of the data obtained as a result of surveillance;
- mandatory rules on the erasure of the data.[49]

In addition to the abovementioned factors, applicable legislation should also offer a system of effective domestic remedies to safeguard people from the arbitrary use of surveillance. Since the remedies concern the surveillance measures, their effectiveness is heavily dependent on the context of the particular case.[50] For example, in case *Kennedy v the United Kingdom*, where the applicant was subjected to interception of his internal communications, the Court stressed that the remedial provisions may include person's request to delete the recorded material of

[45] ECtHR, *Ekimdzhiev and Others v Bulgaria*, app. no. 70078/12, para. 296.
[46] ECtHR, *Liberty and Others v the United Kingdom*, app. no. 58243/00, para. 59.
[47] ECtHR, *Big Brother Watch v the United Kingdom*, app. nos. 58170/13, 62322/14 and 24960/15, para. 333.
[48] ECtHR, *Roman Zakharov v Russia* [GC], app. no. 47143/06, para. 231, *Szabó and Vissy v Hungary*, app. no. 37138/14, para. 56.
[49] ECtHR, *Amann v Switzerland* [GC], app. no. 27798/95, paras. 56-58, *Valenzuela Contreras v Spain*, app no. 58/1997/842/1048, para. 46, *Prado Bugallo v Spain*, app. no. 58496/00, para. 30.
[50] Maria Helen Murphy, "Surveillance and the Right to Privacy: Is an 'Effective Remedy' Possible?", *Justiciability of Human Rights Law in Domestic Jurisdictions* (January 2016): 289-306, p. 291.

surveillance or to pay off the compensation for arbitrary abuse of powers by law enforcement authorities.[51]

Thus, the Court emphasises that any means of surveillance (including FRTs) remain prohibited unless appropriate legislative guarantees exist.[52] As the ECtHR rightfully mentions, "*existence of abusive surveillance practices … appear to be at least in part due to the inadequate legal safeguards*".[53] The human rights defenders, however, go even further, suggesting that FRTs are prohibited under any conditions if not regulated by appropriate legislation.[54]

Further, the Court particularly emphasises on the necessity criterion, which states that interference with person's right has to be proportionate to the aim pursued.[55] It should be underlined in this respect that assessment of the Court is individual and conducted on the case-by-case basis. For instance, in case *Gaughran v the United Kindom*, where applicant's custody photo was taken and held in the database by policy to apply FRTs, the Court found violation of Article 8 since there was no definite period of applicant's data retention.[56] On the contrary, in case *P.N. v Germany* concerning the retention of a photograph of the applicant who was an offender, the Court did not establish violation of Article 8 due to strict period of data retention (5 years).[57]

Overall the ECtHR practice demonstrates that in any case intrusive measures must remain necessary and proportionate. While assessing the legitimacy of the surveillance measures the Court takes into account the domestic legislation, which provides clear list of conditions and

[51] ECtHR, *Kennedy v the United Kingdom*, app. no. 26839/05, para. 167.
[52] *Ekimdzhiev and Others v Bulgaria*, para. 359, *Szabó and Vissy v Hungary*, para. 89.
[53] *Ekimdzhiev and Others v Bulgaria*, para. 357.
[54] "Is It Legal to Install Cameral with Facial Recognition Systems on City Streets?", *Center of Democracy and Rule of Law*, accessed April 11, 2023, URL: https://cedem.org.ua/analytics/kamery-rozpiznavannya-oblych/
[55] ECtHR, *Hájovský v Slovakia*, app. no. 7796/16, para. 32.
[56] ECtHR, *Gaughran v the United Kindom*, app. no. 45245/15, para. 94.
[57] ECtHR, *P.N. v Germany*, app. no. 74440/17, paras. 88, 90.

subjects of surveillance measures, timeframe of data retention and its subsequent erasure, as well as additional safeguards to people subjected to such activity.

It can be seen from the above that authorities have to ensure numerous safeguards so that collection of biometric data was lawful and justified. Apart from the aforementioned binding provisions, several recommendations were implemented by the Council of Europe to provide states with guidance in their policy towards regulation of FRTs. In this regard, Guidelines on Facial Recognition reiterate ECtHR practice and go somewhat further, encouraging states to adapt law with a clear indication of purpose of the surveillance, the accuracy of algorithm used and mechanism of monitoring of such systems.[58] Since facial recognition is an operation which requires the assistance of AI tools, it is also essential to mention Recommendation CM/Rec(2020)1.[59] The latter stresses the need for developed algorithms to be transparent and human-centric as most of them are connected with automatic decision-making process.[60] To avoid mistakes in identification it is recommended to establish the monitoring mechanism of the algorithmic systems as well as possibility of their auditing.[61] These measures will ensure protection of subject's rights during the usage of FRTs.

Therefore, the international standards regarding usage of FRTs are still developing both on the level of the EU and Council of Europe. Despite not having specific regulation, there already exist numerous safeguards and guidelines as to the proportionate usage of FRTs as surveillance means as well as protection of persons' personal data and privacy. It is essential for states to keep following the existing framework to avoid abusing fundamental human rights and develop its own standards for better legal protection.

[58] Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, "Guidelines on Facial Recogntion", *T-PD(2020)03rev4* (January 2021): 1-16, p. 4.
[59] Committee of Ministers, "Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems", *CM/Rec(2020)1* (April 2020).
[60] *Ibid*., paras. 4.3, 6.3.
[61] *Ibid*., para. 5.4.

Usage of Facial Recognition Technologies in Times of Emergency

It is essential to comply with human rights and obligations even in the exceptional circumstances, which allow certain deviations from rights to pursue national interests.[62] Such circumstances often refer to the state of emergency, namely situations "*threatening the life of the nation*".[63] Article 15 of ECHR states that in times of emergency, including war or any other public emergency, the state may derogate from its obligations under the Convention, thus restricting protected rights if necessary.[64]

The derogation sufficiently changes the stresses of non-absolute rights, such as the right to privacy: since limitation clauses under Article 8(2) of ECHR already provide justified interference of authorities, the derogation goes even further and allows wider state's discretion in actions.[65] Considering the latter, it is still unclear how far the authorities' discretion may extend, even if the derogation allows the suspension of certain rights' and regular procedures. As Harris, O'Boyle and Warbrick rightfully mention, "*once the necessity for derogation is conceded, it becomes difficult to control abusive recourse to the power of suspending rights that the provision permits*".[66] In this regard authorities may be authorised with more powers that they would not normally perform.[67] However, it is for the national courts to decide in the end whether such discretion is excessive. For example, in case *Lawless v Ireland (No. 3)*, concerning the introduction of special powers on detention, ECtHR justified such powers since the latter were used for the specific purpose of emergency and were subjected to a number of legal safeguards against abuse.[68]

[62] European Commission for Democracy through Law (Venice Commission), "Opinion on the Protection of Human Rights in Emergency Situations", no. 359/2005 (April 2006): 1-14, pp. 2-3.
[63] Council of Europe, "European Convention for the Protection of Human Rights and Fundamental Freedoms", *European Treaty Series* no. 5 (November 1950), Article 15(1).
[64] *Ibid*.
[65] Elliot Bulmer, "Emergency Powers", *International IDEA Constitution-Building Primer* 18 (2018): 1-45, p. 20.
[66] David Harris, Michael O'Boyle, Ed Bates, Carla Buckley, *Law of the European Convention on Human Rights 4th ed.* (Oxford: Oxford University Press, 2018), p. 824.
[67] Helen Fenwick, Daniel Fenwick, "The Role of Derogations from the ECHR in the Current "War on Terror"", *International Human Rights and Counter-Terrorism. International Human Rights* (2019): 259-290, pp. 269-270.
[68] ECtHR, *Lawless v Ireland (No. 3)*, app. no. 322/57, para. 38.

This work emphasises that the negative tendency of wider discretion in authorities' hands regarding FRTs is that the former may deploy even more intrusive digital technologies explaining them with the need to protect national interests. Here, however, the Court of Justice of European Union (hereinafter – CJEU) posited that in time of emergency derogations concerning personal data "*must apply only in so far as is strictly necessary*".[69] Thus, despite said restrictions indeed deem to be necessary when emergency occurs, states' margin of appreciation cannot be unlimited and still has to remain within the "necessity and proportionality" circle, which will exclude any case of arbitrary interference within human rights.[70] It is also confirmed by the Venice Commission, according to which state's "*discretion is not unfettered*".[71] It is crucial to keep in mind that human rights continue to exist even in times of emergency, and, therefore, respective obligations remain imposed on the states. Talking about war context, even if the state has a leeway regarding when to remove restrictions,[72] it must be guaranteed that excessive restrictions will be dropped as soon as conditions of emergency no longer apply.

It is noteworthy to mention that Ukraine has also derogated from its human rights obligations due to the war context. Considering Russian invasion to Ukraine on February 2022, the President of Ukraine introduced a state of emergency,[73] and later the martial law was established in Ukraine. Following the President's order, Ukrainian government notified the UN Secretary General on derogations under Article 4 of ICCPR as well as Article 15 of ECHR.[74]

[69] EDPB, "Guidelines 05/2022", p. 15.
[70] European Commission for Democracy through Law (Venice Commission), "Report. Respect for Democracy, Human Rights and the Rule of Law during States of Emergency: Reflections", no. 987/2020 (June 2020): 1-25, pp. 4-5.
[71] *Ibid.*
[72] Karen Reid, *A Practitioner's Guide to the European Convention on Human Rights 4th ed.* (London: Sweet & Maxwell, 2012), p. 356.
[73] Указ Президента України, ["On the introduction of a state of emergency in certain regions of Ukraine"], no. 63/2022 (February 2022).
[74] United Nations, "International Covenant on Civil and Political Rights. Ukraine: Notification under Article 4(3)", *C.N.65.2022.TREATIES-IV.4* (February 2022): 1-6, p. 2, Permanent Representation of Ukraine to the Council of Europe, "Note Verbale", no. 31011/32-017/3 (February 2022): 1-8, p. 3.

In this respect a state could deviate from its obligations thus imposing stricter limitations on human rights.[75] It is pertinent to mention that in both cases Ukraine derogated from the right to privacy thus allowing the wider margin of appreciation in its subsequent actions.[76] Analysing the derogation made by Ukraine, Lilian Apostol[77] focused on its overall necessity and legitimacy, while also highlighted the need for minimal safeguards during the trial process and effective remedies.[78]

With regard to state of emergency and derogations, it is essential thus to recognise the specific need for such tools but also remember that human rights obligations do not cease to exist and do not go beyond the legal protection provided for persons within their fundamental rights.

[75] Bulmer, "Emergency Powers", p. 20.
[76] Council of Europe, "Legal Analysis of the derogation made by Ukraine under Article 15 of the European Convention of Human Rights and Article 4 of the International Covenant on Civil and Political Rights" (November 2022): 1-42, pp. 20-21.
[77] International consultant of the Council of Europe.
[78] CoE, "Legal Analysis of the derogation made by Ukraine under Article 15 of the European Convention of Human Rights and Article 4 of the International Covenant on Civil and Political Rights", p. 35.

UKRAINE AND FACIAL RECOGNITION TECHNOLOGIES

Ukraine takes an active part in the development of modern technologies. As it was already indicated Ukraine also resorts to surveillance measures,[79] among which are FRTs. Its policy heavily relies on the digitalisation, which can be seen from the mobile app "Diya" created as a database of electronic documents[80] or programme "Safe.City" invented as an innovative way of ensuring local security.[81] The use of digital technologies in Ukraine, however, has only increased since the full-scale Russian invasion.[82] Thus, following sub-chapters will assess whether Ukrainian law grants sufficient safeguards to data subjects despite actively engaging with FRTs.

[79] Тетяна Соколан, ["Administrative and legal regulation of the use of video surveillance by law enforcement agencies of Ukraine"], *Dissertation for obtaining the scientific degree of candidate of legal sciences* (2016): 1-210, p. 38.
[80] URL: https://diia.gov.ua
[81] URL: https://www.datagroup.ua/pro-kompaniyu/socialna-vidpovidalnist/bezpechne-misto
[82] Simon Hogue, "Civilian Surveillance in the War in Ukraine: Mobilizing the Agency of the Observers of War", *Surveillance & Society* 21 no. 1 (2023): 108-112, p. 109.

Existing Law and Policy

In principle, Ukraine does not have a unified legal framework related to mass surveillance measures.[83] Specific provisions on the digital technologies can be found in the separate legal provisions or internal orders.[84] Thus, notwithstanding absence of regulation, certain laws can be analysed.

Data Protection Laws

Although Ukraine is regarded as a "digital state", surprisingly, its legislation on privacy and data protection remains extremely outdated.[85] The applicable Law of Ukraine "On the Protection of Personal Data" (hereinafter – Law) was introduced in 2010.[86] Following GDPR enforcement, the Law was amended many times, albeit it still does not address the specificities of the data protection mechanism.[87] Moreover, the current Law cannot keep up with all of advanced digital technology, which refutes the statement that legal provisions must be up-to-date.[88] In particular, the Law does not address the non-compliance with timeframe of data processing, remedy mechanism, unauthorised data collection etc.[89] While several new draft laws continue to be under consideration in the Ukrainian Parliament, little has been accomplished in terms of their examination and implementation.

Nevertheless, despite being generally formulated, the Law provides appropriate safeguards in terms of protecting the right to privacy.[90] Overall the Law outlines an exhaustive

[83] Гончаренко, ["Legal regulation of the use of facial recognition technologies"], p. 58.
[84] Тетяна Тарасевич, ["Legal regulation of biometric personal identification: national trends and foreign experience"], *Journal of the Kyiv University of Law* 2 (August 2021): 281-286, pp. 283-284.
[85] [How did personal data become a bargaining chip of political forces in elections? (part 2)"], *Internet freedom*, accessed June 1, 2023, URL: https://netfreedom.org.ua/article/yak-personalni-dani-stali-rozminnoyu-monetoyu-politichnih-sil-na-viborah-chastina-2
[86] [Law of Ukraine "On the Protection of Personal Data"], no. 2297-VI (2010).
[87] Марина Беланюк, ["Human rights on the Internet"], *Materials of the second scientific and practical conference* (May 2020): 116-122, p. 118.
[88] Наталія Уханова, ["Foreign and domestic experience of legal regulation of information security in the field of personal data protection"], *Materials of the second scientific and practical conference* (May 2020): 253-258, p. 256.
[89] *Ibid.*
[90] *Ibid.*, p. 255.

list of grounds for data collection and grants the data subjects essential rights to be protected from any illegal conduct or arbitrary data gathering. Apart from this, the Law obliges authorities to process data only when it is absolutely necessary, granting the individual a range of rights, including access to information as well as the right to data erasure.[91]

Following GDPR, the Law prohibits processing of biometric data since the latter constitute special categories of data.[92] At the same time, the Law highlights exceptions when such processing deems to be lawful, among which are given prior consent and data made publicly available by the individual.[93] The latter case creates a leeway for authorities to collect information,[94] including involvement with the Clearview AI technology (which collects public photos from social media).[95] In this regard, no permission from the data subject is required since the Law de-facto allows data collection from the public resources.

In terms of supervision powers, the Law of Ukraine № 383-VII authorised the Ombudsman of Ukraine to monitor compliance with the legislation on personal data protection.[96] However, since there is no relevant mechanism for protection of biometric data, it is unknown how the Ombudsman can diligently perform its functions in this sphere.

With respect to the new initiatives, the Draft Law "On the Protection of Personal Data" № 8153 of 2022 aims to adapt the legislation to the EU standards and fill the existing legislative gaps.[97] Draft Law significantly details existing procedures, enhancing mechanisms of protection in case of biometric data processing and the automatic decision-making process. However, even the proposed version of law does not contain any regulation towards

[91] Law of Ukraine "On the Protection of Personal Data", Article 8.
[92] *Ibid*., Article 7(1).
[93] *Ibid*., Article 7(2)(1,8).
[94] Михайло Брайчевський, ["The problem of personal data protection in Internet of systems in the conditions of regime measures"], *Materials of the second scientific and practical conference* (May 2020): 245-250, p. 248.
[95] Camilla Dul, "Facial Recognition Technology vs Privacy: The Case of Clearview AI", *Queen Mary Law Journal* 3 (2022): 1-24, p. 4.
[96] ["On Amendments to Some Legislative Acts of Ukraine regarding the Improvement of the Personal Data Protection System"], no. 383-VII (June 2013), para. 2.
[97] [Draft Law "On the Protection of Personal Data"], no. 8153 (October 2022), "Data Protection Laws of the World: Ukraine", *DLA PIPER* (May 2023): 1-8, p. 2.

surveillance. Particularly, unlike the EU AI Act which delineates three different systems, the Draft Law does not distinguish between ordinary surveillance and FRTs, which is more intrusive. Since the Draft Law does not provide any restrictions, it basically gives authorities the "green light" in usage any kind of FRTs without precautions. Unfortunately, said law is unlikely to be adopted very soon, given the Parliament's silence of half a year from the moment of its registration.

Law Enforcement Laws

The Law of Ukraine "On National Police" is another law which should be mentioned in context of surveillance. Article 40 of the Law authorises police to use "*photo and video equipment, including equipment that works in automatic mode*" as well as "*specialized software for analytical processing of photo and video information*".[98] No limitations whatsoever imposed on law enforcement authorities in this respect apart from the obligation to use the surveillance for strictly defined purposes.[99]

In March 2022 Ukrainian legislators amended the abovementioned Law, authorising the police to manage the register and databases which contain data about suspected criminals, accused persons, absconding defendants etc.[100] Noticeably, such database also possesses biometric data of individuals (including a digitalised image of a person's face) which police is obligated to collect from individuals.[101] Concerning introduced amendments two important points should be raised. Firstly, the new amendments state that storage period of biometric data and other material of video-surveillance is established by the Ministry on the Internal Affairs of Ukraine.[102] The latter authority is empowered to issue solely internal orders which do not

[98] [Law of Ukraine "On National Police"], no. 580-VIII (2015), Article 40.
[99] О.І. Безпалова, К.Ю. Мельник, О. О. Юхно та ін., [The Law of Ukraine "On the National Police": a scientific and practical commentary] (Kharkiv: Kharkiv, National University of Internal Affairs, 2016), p. 161.
[100] [Law of Ukraine "On amendments to the Laws of Ukraine "On National Police" and "On Disciplinary Statute of the National Police of Ukraine" in order to optimize police activities, including during martial law"], no. 2123-IX (2022).
[101] *Ibid*., Article 26(2).
[102] [Law of Ukraine "On National Police"], Articles 26(2), 40.

usually have a binding nature. This, in turn, may create a potential abuse of law enforcement authorities towards the biometric data which can be stored for the indefinite period of time. Secondly, the amendments were introduced during martial law, where wider discretion is allowed. However, the law gives no indication as to whether authority will have the same powers in peaceful times. In this regard, there is a danger that police will be left with an excessive authority even once martial law ceases to apply.[103]

Ukraine and Clearview AI

In terms of practical applications of FRTs, on March 2022 Ukrainian government announced its cooperation with the US company Clearview AI.[104] This system identifies persons by using images, which were previously scraped online from the social media platforms (such as Google, Facebook, Twitter etc.).[105] In other words, to identify the person, his/her photo has to be uploaded in database, and the algorithm will make a match. The company's biometric database has approximately 10 billion images in its possession and often sells the data to authorities, mostly police and agencies.[106] Being common in the US public sector, Clearview AI is now expanding towards Europe and being used in more than 26 countries (most of them being Member-States of the EU) assisting the latter in the law enforcement.[107] In Ukraine, Clearview AI is used to monitor potential infiltrators from Russia, combat disinformation and reunite refugees with their families separated because of war.[108] It mostly identifies dead

[103] Ольга Безпалова, ["Priority areas of activity of police authorities in ensuring the rights of citizens in the conditions of the legal regime of martial law in Ukraine"], *Law and security* 3 no. 86 (2022): 13-25, p. 16.
[104] "The Clearview/Ukraine partnership - How surveillance companies exploit war", *Privacy International*, accessed April 11, 2023, URL: https://privacyinternational.org/news-analysis/4806/clearviewukraine-partnership-how-surveillance-companies-exploit-war
[105] Dul, "Facial Recognition Technology vs Privacy: The Case of Clearview AI", pp. 3-4.
[106] *Ibid*., p. 2.
[107] "Facial recognition tech developed by Clearview AI could be illegal in Europe, privacy group says", *CNBC*, accessed April 11, 2023, URL: https://www.cnbc.com/2020/06/11/clearview-ai-facial-recognition-europe.html#:~:text=Hoan%20Ton-That%2C%20Clearview%20AI's%20CEO%2C%20said%3A%20"%EF%BB%BFClearview's%20image-search,public%20internet%20just%20like%20any%20other%20search%20engine
[108] Г.К. Авдєєва, ["Digital evidence in criminal proceedings concerning war crimes"], *A collection of abstracts of scientific and practical conference reports* (April 2023): 28-31, p. 29.

Russian soldiers (to notify their families about it) as well as the casualties of war (both among Russians and Ukrainians).[109]

It is critical to note that Clearview AI gets particularly negative treatment on the international arena. Both human right organisations and academic scholars found the Clearview system to be an extremely intrusive technology, and not in compliance with GDPR. With regard to the former, Privacy International emphasised that usage of Clearview AI "*is a considerable expansion of the realm of surveillance, with very real potential for abuse*".[110] In this regard, Privacy International along with other regional organisations (including Digital Human Rights, Homo Digitalis) filed several legal complaints against the Clearview AI company in France, Austria, Italy, Greece and the United Kingdom.[111] Complainants argued that Clearview AI violated numerous of GDPR provisions, namely the processing of sensitive data, lack of transparency and absence of lawful grounds for data processing. As a result of commenced domestic investigation, French regulator imposed on Clearview the fine of 20 million EUR, ordering to stop collecting and processing data as well as delete the already gathered one.[112] Similarly, Italy came up with an analogical decision, banning the web scraping technique and obliging the Clearview to delete all the data.[113]

Such a response from the international community is more than understandable. The use of Clearview AI bears lots of risks for data subjects and its further applications.

[109] Людмила Требик, Михайло Зубко, ["Use of artificial intelligence in the public sphere: foreign experience"], *1st International scientific and practical conference 'Current issues of science and integrated technologies'* (January 2023): 550-552, p. 552.
[110] "The Clearview/Ukraine partnership - How surveillance companies exploit war", *Privacy International*, accessed April 11, 2023, URL: https://privacyinternational.org/news-analysis/4806/clearviewukraine-partnership-how-surveillance-companies-exploit-war
[111] Privacy International, "Submission to the Information Commissioner – Request for Assessment of Processing Operators by Clearview AI, Inc." (May 2021): 1-42.
[112] CNIL, "Restricted Committee Deliberation No. SAN-2022-019 of 17 October 2022 concerning CLEARVIEW AI", 1-16, p. 15.
[113] GPDP, "Ordinanza ingiunzione nei confronti di Clearview AI" ["Injunction order against Clearview AI"], no. 9751362 (February 2022).

Firstly, while using the Clearview, there is always a danger of complete reliance on the algorithm of the system that replaces human decision-making. While the Facial Recognition Vendor Test[114] demonstrated the accuracy rate of 99,85% towards the Clearview algorithm,[115] the same accuracy can never be guaranteed during future matches. Automatic decision-making remains the mere machine, thus creating the constant issue of misrecognition. In the context of Ukrainian war this entails the constant danger that the Clearview system may produce fatal errors, such as mistaking civilians for soldiers, heavily wounded combatants for dead, or even confuse Ukrainians for Russian infiltrators.[116]

Secondly, the Clearview technology raises the issues of the person's privacy. Privacy is the concept that includes "*both a right to control whether one's information is shared and if so, with whom*".[117] Thus, there is a risk that people's expectations of privacy may have a chilling effect if they are aware that their photos might be collected and stored.[118] Further, Clearview violates rules of GDPR, especially regarding special categories of data.[119] To reiterate, the database consists of the publicly available pictures from social media. However, the Clearview scrapes the photos even from private accounts (where the person does not wish to make the information public) thus presuming that there is no need for a person's consent in the first place.[120] Nevertheless, the database contains even those images "*that are no longer, but once were, publicly available*",[121] which allows the technology to scrape even once deleted pictures.

[114] A series of tests carried out by the National Institute of Standards and Technology (NIST) to assess the performance of face recognition algorithms.
[115] "Consecutive NIST Tests Confirm Superiority of Clearview AI's Facial Recognition Platform", *Businesswire*, accessed April 11, 2023, URL: https://www.businesswire.com/news/home/20211124005505/en/Consecutive-NIST-Tests-Confirm-Superiority-of-Clearview-AIs-Facial-Recognition-Platform
[116] "Does facial recognition tech in Ukraine's war bring killer robots nearer?", *openDemocracy*, accessed April 11, 2023, URL: https://www.opendemocracy.net/en/technology-and-democracy/facial-recognition-ukraine-clearview-military-ai/
[117] Dul, "Facial Recognition Technology vs Privacy: The Case of Clearview AI", p. 9.
[118] *Ibid*., p. 11.
[119] Isadora Neroni Rezende, "Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective", *New Journal of European Criminal Law* 11 no. 3 (2020): 375-389, p. 380.
[120] *Ibid*., pp. 380-381.
[121] "The world's scariest facial recognition company, explained", *VOX*, accessed April 11, 2023, URL: https://www.vox.com/recode/2020/2/11/21131991/clearview-ai-facial-recognition-database-law-enforcement

Lastly, FRTs create serious risks while being used in the Ukrainian military context.[122] Since Clearview company decides on its own whom to offer its services, there is no guarantee the opposing party of the armed conflict will not obtain the technology at some point of time. Moreover, any private company may use the searchable database by Clearview provided it pays for its access. This may create the negative effect on Ukrainian information field. In the context of Ukrainian war, it may lead to dangerous repercussions: since Clearview AI also uses the images from the Russian social media "VKontakte", Russia may enhance its online manipulation of web-page[123] thus distorting results for Clearview.

All of the abovementioned concerns create an extremely serious risk with further usage of Clearview AI. Despite the fact that company's CEO encouraging the usage only by the "*trained investigator*",[124] the latter is unreasonable if no legal grounds are provided for regulation of biometric technology. This was the issue for the European states, and it remains the main problem for Ukraine giving the context of war. Thus, it is essential to advocate for the proper regulation of the surveillance, conducted both with military and civil purposes. It is also important to underline that any of the limitations imposed during war context have to be lifted immediately after the state of emergency cease to exist.[125]

[122] "Facial Recognition Goes to War", *The New York Times*, accessed June 1, 2023,
URL: https://www.nytimes.com/2022/04/07/technology/facial-recognition-ukraine-clearview.html
[123] Ulrik Franke, "War by non-military means: Understanding Russian information warfare", *Report* no. FOI-R-4065—SE (March 2015): 1-60, p. 45.
[124] "At war with facial recognition: Clearview AI in Ukraine", *The Record*, accessed April 11, 2023,
URL: https://therecord.media/at-war-with-facial-recognition-clearview-ai-in-ukraine
[125] Venice Commission, "Report. Respect for Democracy, Human Rights and the Rule of Law during States of Emergency: Reflections", p. 5.

RECOMMENDATIONS TO UKRAINIAN LEGISLATION

With the development of digital technologies and their deployment on the battlefield, it is essential to advocate for the amendment of Ukrainian legislation. If extraordinary means are deployed without appropriate safeguards, the former may very likely result in the grave consequences.[126] It is also important to pay special attention to the special categories of data since all the technologies Ukraine uses process data through a specific technical means allowing the unique identification or authentication of a natural person.[127]

In this regard, the main recommendation this work suggests for Ukrainian Parliament is the adoption of the unified law on surveillance, which will regulate the FRTs and other digital technologies, discretion of authorities, processing of biometric data and mechanism of protection for data subjects. However, given that at the moment such legislation does not exist, current legislation has to be amended at least with the minimum safeguards. Thus, to ensure the appropriate protection and human rights as well as lawful deployment of digital tool, this work recommends the Ukrainian legislators to amend specific laws suggesting the amendments in **Annex I** (Regulation in peaceful times). Since Ukraine is still acts in the wartime, this work also proposes the following recommendations in **Annex II** (Regulation in wartime). Proposed recommendations will be sent to respective Committees of Verkhovna Rada of Ukraine (Ukrainian Parliament). As amendments concern mainly data protection and law enforcement rules on the FRTs usage, I will engage with the Committee on Digital Transformation and Committee on Law Enforcement Activities. Since officially the amendments to the laws can be proposed only by the Ukrainian deputies, I will engage with the representatives of the relevant Committees via their e-mails and conduct following discussions about the recommendations

[126] European Center for Not-for-Profit Law, INCLO, Privacy International, "Under Surveillance: (Mis)Use of Technologies in Emergency Responses" (December 2022): 1-53, p. 12.
[127] General Data Protection Regulation.

proposed. Lastly, when amendments are proposed to the Committee, it is for the latter to decide whether to accept or reject them. I will be notified on either decision.

CONCLUSIONS

FRT is a huge digital tool of mass surveillance which must be regulated with an appropriate legal framework. The absence of legal provision enables authorities to act arbitrarily, which has extremely negative effect on human rights, considering that FRTs touch upon the issues of personal data and privacy. Taking into account the wartime in Ukraine, its derogation from the rights and wider state's discretion, the regulation becomes even more necessary. This work analysed the international regulation of the FRTs and the judicial approach to the issue, assessed the risks such technologies bear, evaluated its effectiveness in Ukraine and provided the set of recommendations to Ukrainian legislation. The recommendations aim at improving Ukrainian legislative framework which will shape the usage of intrusive technologies rather than undermine their impact on human rights. Thus, to ensure the balance between a person's right to privacy and state's national interests, it is essential not only having a legal provision but also provide appropriate safeguards, clear rules and comprehensive remedial mechanism. Only in such a case the authorities will perform their functions diligently, and people's fundamental rights will remain heavily protected.

BIBLIOGRAPHY

"AI Act: a step closer to the first rules on Artificial Intelligence". *News European Parliament*. Accessed May 23, 2023. URL: https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence

"At war with facial recognition: Clearview AI in Ukraine". *The Record*. Accessed April 11, 2023. URL: https://therecord.media/at-war-with-facial-recognition-clearview-ai-in-ukraine

"Consecutive NIST Tests Confirm Superiority of Clearview AI's Facial Recognition Platform". *Businesswire*. Accessed April 11, 2023. URL: https://www.businesswire.com/news/home/20211124005505/en/Consecutive-NIST-Tests-Confirm-Superiority-of-Clearview-AIs-Facial-Recognition-Platform

"Data Protection Laws of the World: Ukraine". *DLA PIPER* (May 2023): 1-8.

"Does facial recognition tech in Ukraine's war bring killer robots nearer?". *openDemocracy*. Accessed April 11, 2023. URL: https://www.opendemocracy.net/en/technology-and-democracy/facial-recognition-ukraine-clearview-military-ai/

"Facial Recognition Goes to War". *The New York Times*. Accessed June 1, 2023. URL: https://www.nytimes.com/2022/04/07/technology/facial-recognition-ukraine-clearview.html

"Facial recognition tech developed by Clearview AI could be illegal in Europe, privacy group says". *CNBC*. Accessed April 11, 2023. URL: https://www.cnbc.com/2020/06/11/clearview-ai-facial-recognition-europe.html#:~:text=Hoan%20%20Ton-That%2C%20%20Clearview%20AI's%20%20CEO%2C%20said%3A%20

"Is It Legal to Install Cameral with Facial Recognition Systems on City Streets?". *Center of Democracy and Rule of Law*. Accessed April 11, 2023. URL: https://cedem.org.ua/analytics/kamery-rozpiznavannya-oblych/

"Joining the EU". *European Union*. Accessed May 23, 2023. URL: https://european-union.europa.eu/principles-countries-history/joining-eu_en

"The Clearview/Ukraine partnership - How surveillance companies exploit war". *Privacy International*. Accessed April 11, 2023. URL: https://privacyinternational.org/news-analysis/4806/clearviewukraine-partnership-how-surveillance-companies-exploit-war

"The world's scariest facial recognition company, explained". *VOX*. Accessed April 11, 2023. URL: https://www.vox.com/recode/2020/2/11/21131991/clearview-ai-facial-recognition-database-law-enforcement

"Ukraine". *European Council, Council of the European Union*. Accessed April 11, 2023. URL: https://www.consilium.europa.eu/en/policies/enlargement/ukraine/

"Проект Закону про захист персональних даних" [Draft Law "On the Protection of Personal Data"], no. 8153 (October 2022).

"Як персональні дані стали розмінною монетою політичних сил на виборах? (частина 2)" [How did personal data become a bargaining chip of political forces in elections? (part 2)"]. *Internet freedom/Інтернет свобода*. Accessed June 1, 2023. URL: https://netfreedom.org.ua/article/yak-personalni-dani-stali-rozminnoyu-monetoyu-politichnih-sil-na-viborah-chastina-2

Almansori, Abdulrhman M., Taha, Mohamed, Badr, Elsayed. "A deep facial recognition system using computational intelligent algorithms". *PLOS ONE* 15 no. 12 (December 2020): 1-27.

Brey, Philip. "Ethical aspects of facial recognition systems in public places". *Journal of Information, Communication and Ethics in Society* 2 no. 2 (2004): 97-109.

Bulmer, Elliot. "Emergency Powers". *International IDEA Constitution-Building Primer* 18 (2018): 1-45.

CNIL. "Restricted Committee Deliberation No. SAN-2022-019 of 17 October 2022 concerning CLEARVIEW AI". 1-16.

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

Committee of Ministers. "Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems". *CM/Rec(2020)1* (April 2020).

Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. "Guidelines on Facial Recogntion". *T-PD(2020)03rev4* (January 2021): 1-16.

Council of Europe. "European Convention for the Protection of Human Rights and Fundamental Freedoms". *European Treaty Series* no. 5 (November 1950).

Council of Europe. "Legal Analysis of the derogation made by Ukraine under Article 15 of the European Convention of Human Rights and Article 4 of the International Covenant on Civil and Political Rights" (November 2022): 1-42.

Directive (EU) 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities

for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive). *L 119/89* (April 2016).

Dul, Camilla. "Facial Recognition Technology vs Privacy: The Case of Clearview AI". *Queen Mary Law Journal* 3 (2022): 1-24.

European Center for Not-for-Profit Law, INCLO, Privacy International. "Under Surveillance: (Mis)Use of Technologies in Emergency Responses" (December 2022): 1-53.

European Commission for Democracy through Law (Venice Commission). "Opinion on the Protection of Human Rights in Emergency Situations". no. 359/2005 (April 2006): 1-14.

European Commission for Democracy through Law (Venice Commission). "Report. Respect for Democracy, Human Rights and the Rule of Law during States of Emergency: Reflections". no. 987/2020 (June 2020): 1-25.

European Commission. "Opinion on the EU membership application by Ukraine". *QANDA/22/3802* (June 2022): 1-2.

European Court of Human Rights, *Amann v Switzerland* [GC], app. no. 27798/95.

European Court of Human Rights, *Beghal v the United Kingdom*, app. no. 4755/16.

European Court of Human Rights, *Big Brother Watch v the United Kingdom*, app. nos. 58170/13, 62322/14 and 24960/15.

European Court of Human Rights, *Ekimdzhiev and Others v Bulgaria*, app. no. 70078/12.

European Court of Human Rights, *Gaughran v the United Kindom*, app. no. 45245/15.

European Court of Human Rights, *Hájovský v Slovakia*, app. no. 7796/16.

European Court of Human Rights, *Kennedy v the United Kingdom*, app. no. 26839/05.

European Court of Human Rights, *Lawless v Ireland (No. 3)*, app. no. 322/57.

European Court of Human Rights, *Liberty and Others v the United Kingdom*, app. no. 58243/00.

European Court of Human Rights, *P.N. v Germany*, app. no. 74440/17.

European Court of Human Rights, *Peck v the United Kingdom*, app. no. 44647/98.

European Court of Human Rights, *Prado Bugallo v Spain*, app. no. 58496/00.

European Court of Human Rights, *Roman Zakharov v Russia* [GC], app. no. 47143/06.

European Court of Human Rights, *Szabó and Vissy v Hungary*, app. no. 37138/14.

European Court of Human Rights, *Valenzuela Contreras v Spain*, app no. 58/1997/842/1048.

European Court of Human Rights. "Guide on Article 8 of the European Convention on Human Rights" (31 August 2022): 1-172.

European Data Protection Board. "Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement". *Version 1.0* (May 2022): 1-49.

European Union Agency for Fundamental Rights. "Facial recognition technology: fundamental rights considerations in the context of law enforcement". *FRA Focus* (2019): 1-34.

Fenwick, Helen, Fenwick, Daniel. "The Role of Derogations from the ECHR in the Current "War on Terror"". *International Human Rights and Counter-Terrorism. International Human Rights* (2019): 259-290.

Franke, Ulrik. "War by non-military means: Understanding Russian information warfare". *Report* no. FOI-R-4065—SE (March 2015): 1-60.

GPDP. "Ordinanza ingiunzione nei confronti di Clearview AI" ["Injunction order against Clearview AI"]. no. 9751362 (February 2022).

Harris, David, O'Boyle, Michael, Bates, Ed, Buckley, Carla. *Law of the European Convention on Human Rights 4th ed.*. Oxford: Oxford University Press, 2018.

Hogue, Simon. "Civilian Surveillance in the War in Ukraine: Mobilizing the Agency of the Observers of War". *Surveillance & Society* 21 no. 1 (2023): 108-112.

Kelly, Pat, Chair. "Facial Recognition Technology and the Growing Power of Artificial Intelligence". *44th Parliament, 1st Session* (October 2022): 1-71.

Kuner, Christopher (ed.), Bygrave, Lee A (ed.), Docksey, Christopher (ed.), Drechsler, Laura (ed.). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford: Oxford University Press, 2020.

Madiega, Tambiama, Mildebrath, Hendrik. "Regulating facial recognition in the EU". *European Parliamentary Research Service* (September 2021): 1-38.

Minutes of the third meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680 (November 2016): p. 1-3.

Murphy, Maria Helen. "Surveillance and the Right to Privacy: Is an 'Effective Remedy' Possible?". *Justiciability of Human Rights Law in Domestic Jurisdictions* (January 2016): 289-306.

OECD. *Artificial Intelligence in Society*. Paris: OECD, 2019.

Permanent Representation of Ukraine to the Council of Europe. "Note Verbale". no. 31011/32-017/3 (February 2022): 1-8.

Privacy International. "Submission to the Information Commissioner – Request for Assessment of Processing Operators by Clearview AI, Inc." (May 2021): 1-42.

Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. *2021/0106 (COD)* (April 2021).

Regulation (EU) 2016/679 of the European Parliament and of the Council 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). *L 119/1* (April 2016).

Reid, Karen. *A Practitioner's Guide to the European Convention on Human Rights 4th ed.*. London: Sweet & Maxwell, 2012.

Rezende, Isadora Neroni. "Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective". *New Journal of European Criminal Law* 11 no. 3 (2020): 375-389.

Schabas, William A. *The European Convention on Human Rights: A Commentary*. Oxford: Oxford University Press, 2017.

Seng, Sovantharith, Nasrullah Al-Ameen, Mahdi, Wright, Matthew. "A First Look into Users' Perceptions of Facial Recognition in the Physical World". *Computers & Security* 105 no. 4 (February 2021): 1-22.

Tolba, A.S., El-Baz, A.H., El-Harby, A.A.. "Face Recognition: A Literature Review". *International Journal of Signal Processing* 2 no. 2 (2006): 88-103.

United Nations. "International Covenant on Civil and Political Rights. Ukraine: Notification under Article 4(3)". *C.N.65.2022.TREATIES-IV.4* (February 2022): 1-6.

URL: https://diia.gov.ua

URL: https://www.datagroup.ua/pro-kompaniyu/socialna-vidpovidalnist/bezpechne-misto

Veale, Michael, Borgesius, Frederik J. Zuiderveen. "Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach". *Computer Law Review International* 22 (2021): 97-112.

Voigt, Paul, Bussche, Axel von dem. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Cham: Springer Publishing Company, 2017.

Авдєєва, Г.К.. "Цифрові докази у кримінальному провадженні щодо воєнних злочинів" ["Digital evidence in criminal proceedings concerning war crimes"]. *A collection of abstracts of scientific and practical conference reports/Збірник тез доповідей науково-практичної конференції* (April 2023): 28-31.

Безпалова, О.І., Мельник, К.Ю., Юхно, О. О. та ін.. Закон України "Про Національну поліцію": науково-практичний коментар [The Law of Ukraine "On the National Police": a scientific and practical commentary]. Kharkiv: Kharkiv, National University of Internal Affairs, 2016.

Безпалова, Ольга. "Пріоритетні напрями діяльності органів поліції щодо забезпечення прав громадян в умовах правового режиму воєнного стану в Україні" ["Priority areas of activity of police authorities in ensuring the rights of citizens in the conditions of the legal regime of martial law in Ukraine"]. *Law and security/Право і безпека* 3 no. 86 (2022): 13-25.

Беланюк, Марина. "Права людини в Інтернет" ["Human rights on the Internet"]. *Materials of the second scientific and practical conference/Матеріали другої науково-практичної конференції* (May 2020): 116-122.

Брайчевський, Михайло. "Проблема захисту персональних даних в системах Інтернету речей в умовах режимних заходів" ["The problem of personal data protection in Internet of systems in the conditions of regime measures"]. *Materials of the second scientific and practical conference/Матеріали другої науково-практичної конференції* (May 2020): 245-250.

Гончаренко В. О.. "Правове регулювання використання технологій розпізнавання обличчя" ["Legal regulation of the use of facial recognition technologies"]. *Journal of civil engineering: science and practical journal/ Часопис цивілістики: науково-практичний журнал* 41 (2021): 56-60.

Закон України "Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних Law of Ukraine" ["On Amendments to Some Legislative Acts of Ukraine regarding the Improvement of the Personal Data Protection System"]. no. 383-VII (June 2013).

Закон України “Про внесення змін до законів України “Про Національну поліцію” та “Про Дисциплінарний статут Національної поліції України” з метою оптимізації діяльності поліції, у тому числі під час дії воєнного стану” [Law of Ukraine “On amendments to the Laws of Ukraine “On National Police” and “On Disciplinary Statute of the National Police of Ukraine” in order to optimize police activities, including during martial law”]. no. 2123-IX (2022).

Закон України “Про захист персональних даних” [Law of Ukraine “On the Protection of Personal Data”]. no. 2297-VI (2010).

Закон України “Про Національну Поліцію” [Law of Ukraine “On National Police”]. no. 580-VIII (2015).

Соколан, Тетяна. “Адміністративно-правове регулювання застосування відеоспостереження правоохоронними органами України” [“Administrative and legal regulation of the use of video surveillance by law enforcement agencies of Ukraine”], *Dissertation for obtaining the scientific degree of candidate of legal sciences/Дисертація на здобуття наукового ступеня кандидата юридичних наук* (2016): 1-210.

Тарасевич, Тетяна. “Правове регулювання біометричної ідентифікації особи: національні тенденції та зарубіжний досвід” [“Legal regulation of biometric personal identification: national trends and foreign experience”]. *Journal of the Kyiv University of Law/Часопис Київського університету права* 2 (August 2021): 281-286.

Требик, Людмила, Зубко, Михайло. “Використання штучного інтелекту в публічній сфері: зарубіжний досвід” [“Use of artificial intelligence in the public sphere: foreign experience”]. *1st International scientific and practical conference ‘Current issues of science and integrated technologies’/Перша міжнародна науково-практична конференція ‘Актуальні проблеми науки та цілісних технологій’* (January 2023): 550-552.

Указ Президента України. “Про введення надзвичайного стану в окремих регіонах України” [“On the introduction of a state of emergency in certain regions of Ukraine”]. no. 63/2022 (February 2022).

Уханова, Наталія. “Зарубіжний та вітчизняний досвід правового регулювання інформаційної безпеки у сфері захисту персональних даних” [“Foreign and domestic experience of legal regulation of information security in the field of personal data protection”]. *Materials of the second scientific and practical conference/Матеріали другої науково-практичної конференції* (May 2020): 253-258.

ANNEX I

Regulation in peaceful times		
The Law	**Amendment**	**Reasoning**
The Law of Ukraine "On the Protection of Personal Data"	Amendment of existing *Article 2* ("*Definitions*") by defining surveillance measures (including FRTs)	Inclusion within the framework of this digital tool provides the data subjects with possibility to rely on the legal provision in case the violation occurs. It also entails ensuring of the principle of legal certainty in terms of authorities' discretion.
	Amendment of existing *Article 7* ("*Special requirements for processing personal data*") by differentiating between "sensitive" and "ordinary" personal data	Since sensitive data is subjected to stricter requirements and also includes biometric data, it is essential to differentiate between both kinds of data for ensuring better protection of data subjects during data processing.
	Amendment of existing *Article 7* ("*Special requirements for processing personal data*") by introducing additional safeguards against the unlawful processing of special categories of data.	Since biometric data concerns more intimate data, the person has to be provided with more protection. The examples of safeguards are not provided neither by GDPR, nor by ECtHR. However, such safeguards may include specific time limits for storage of biometric data in the databases or the right to erase the data by the person's requirement. It is essential to engage human rights experts and representatives of NGOs on the regular basis to provide more safeguards for data subjects.
	New *Article 23-1* ("*Compliance with data protection*") on the establishment of the new supervisory body or independent agency which will ensure control and monitoring over compliance with rules.	Mere presence of Ombudsman is not enough to ensure compliance with rules, especially if the surveillance measures are at stake. It is vital to appoint a new person or establish a new body with the powers of oversight and review. Such body may also receive individual complaints from persons in case of violation of data protection rules.
	New *Article 24-1* ("*Ensuring data subjects' protection*") on	Person's right to privacy will not be ensured if no effective

	system of effective remedies which includes the complaint to the national court on the grounds of unauthorised collection, storage or processing of biometric data resulted from FRTs.	remedies exist to protect it. The mechanism of complaint to the supervisory body, judicial review of the order to use FRTs or possibility to obtain compensation in case of unauthorised use of FRTs are only few opportunities that can ensure the protection of human rights during surveillance.
Law of Ukraine "On National Police"	Amendment of existing *Article 24* ("*Additional police powers*") by adding provision on FRTs, which (1) provides the mechanism of their work, an exhaustive list of grounds for its usage; (2) differentiate between ordinary surveillance and FRTs, "high-risk" and "low-risk" systems	Separate set of rules ensures the limits of authorities' discretion when using FRTs as well as prevents the arbitrary interference within person's right to privacy. It is also vital to adopt the legislation to the EU standards, thus differentiating between ordinary technologies and measures which are more intrusive by their technical means.
	Amendment of existing *Article 40* ("*Application of technical devices, technical means and specialised software*") by limiting the usage of FRTs with the legitimate legal grounds for data processing as well as legitimate purposes for such processing	Clear list of the restrictions will prevent the arbitrary usage of FRTs and limit the discretion of law enforcement authorities.

ANNEX II

Regulation in war time		
The Law	**Amendment**	**Reasoning**
Law of Ukraine "On Protection of Personal Data"	Amendment of existing *Article 28* ("*Responsibility for violation of the legislation on the protection of personal data*") by establishing financial sanctions for violations in the field of data protection	As of now, violation of data protection rules results solely in administrative liability. During martial law it is vital to introduce stricter sanction policy on legal level to better enforce the rules and prevent the abuse of authority.
Law of Ukraine "On National Police"	Amendment of existing *clause 45 Article 23* ("*The main powers of the police*") by limiting the storage of biometric data to a reasonable period of time	Even if the derogation allows the authorities to store the biometric data for longer time periods, the latter cannot remain excessive. It is essential to establish a timeframe for data collection which cannot exceed at least 5 years (according to ECtHR practice).
	Amendment of existing *Article 26* ("*Formation of information resources by the police*") by stating about the engagement with other technologies and systems (such as Clearview AI) only for specific and legitimate purposes.	Even if the Clearview AI usage may be justified by the exigencies of the situation in Ukraine, such measures must be resorted to only for law enforcement purposes given their intrusive nature. Thus, any engagement with Clearview system must be compliant with human rights standards and GDPR rules.
	Amendment of existing *Article 40* ("*Application of technical devices, technical means and specialised software*") by permitting to use photo- and video-equipment for surveillance solely if the law enforcement purposes are at stake	The discretion of police has to be limited considering necessity and proportionality criteria. It is important to provide the list of purposes according to which surveillance measures can be used as well as to avoid the vague and non-specific language for clear understanding.
	Amendment of existing *Chapter 11* ("*Final and transitional provisions*") by stating that all of the	In Ukraine a lot of amendments are being made without considering future events. Thus, there is a

	restrictions will be lifted as soon as war circumstances cease to exist	danger that authorities will be left with a wide discretion even when the state will be back to "normal" regulation.
Criminal Code of Ukraine	New *Article 364* ("*Usage of surveillance measures*") (Chapter 16: Criminal offenses in the field of use of electronic computing machines (computers), systems and computer networks and electric communication networks)) by criminalising the unauthorised usage of surveillance measures (including AI-driven systems)	To improve enforcement mechanism of data protection provisions, it is essential to introduce sanction policy for violation of such rules.
	New *Article 365* ("*Collection, storage and processing of the biometric data*") by criminalising the abuse of biometric data or other illegal actions conducted with data.	As a special category of data, biometric data cannot be regulated solely by the internal orders. It is essential to establish responsibility on the level of the law for ensuring its legal force as well as more effective enforcement mechanism.