Image-Based Digital Face Identification Technologies: Criminal Law Aspect

Submitted: 23 August 2022
Reviewed: 18 October 2022
Revised: 26 October 2022
Accepted: 22 November 2022

Article submitted to blind peer review

Sofiia Ya. Lykhova[*]
https://orcid.org/0000-0003-2861-519X
Andrii V. Svintsytskyi[**]
https://orcid.org/0000-0002-0956-0341
Andrii M. Padalka[***]
https://orcid.org/0000-0003-3713-1007
Yuriy Yu. Nizovtsev[****]
https://orcid.org/0000-0002-7641-6403
Andrii Lyseiuk[*****]
https://orcid.org/0000-0002-9026-1188

DOI: https://doi.org/10.26512/lstr.v15i2.44744

Abstract

[Purpose] The purpose of this article is to analyze the theoretical and practical aspects of digital face identification technology in Ukraine and suggest the necessary corrections to the optimal legal regime for the use of such technology in criminal proceedings.

[Methodology/Approach/Design] The leading research method is the inductive method of the legal analysis that involves the problem formulation, analysis of the legal provisions regulating this question, practical study of the law enforcement, and formulation of conclusions.

[*]Sofiia Ya. Lykhova is Doctor of Law, Professor, Head of the Department of Criminal Law and Procedure of the he National Aviation University. Address: 03058, 1 Lubomyr Husar Ave., Kyiv, Ukraine. E-mail: lykhova8094@edu-knu.com.

[**]Andrii V. Svintsytskyi is PhD in Law, Professor at the Department of Criminal Procedure and Criminalistics of the Educational and Scientific Institute of Humanities of the National Academy of the Security Service of Ukraine. E-mail: svintsytskyi8143@acu-edu.cc.

[***]Andrii M. Padalka is Doctor of Law, Deputy Director of the Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine. Dr. Padalka is also Associate Professor at the Department of Financial Investigations of the University of the State Fiscal Service of Ukraine. E-mail: padalka8143@neu.com.de.

[****]Yuriy Yu. Nizovtsev is PhD in Law, Leading Researcher of the Research Laboratory of the Center for Forensic and Special Expertise of the Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine. E-mail: nizovtsev8218@sci-univ.com.

[*****]Andrii Lyseiuk is PhD in Law, Associate Professor at the Department of Investigative Activities of the National University of the State Fiscal Service of Ukraine. E-mail: lyseiuk8143@sci-univ.com.

[Findings] In this article, the authors present a complex analysis of the Ukrainian legislation, define the particularity of criminal responsibility for the violation of privacy under the Ukrainian law in the context of the use of digital face identification technology, and suggest a list of reasonable amendments to the legislation to improve the level of such protection.
[Practical Implications] The materials of this article have practical value for investigating crimes and protecting individuals against illegal use of their images by using digital face identification technology in the context of Ukrainian law.
[Originality/Value] The topicality of the study is due to the fact that over the past decade face recognition has become one of the most powerful biometric technologies capable of identifying and verifying people involved in crimes based on digital images or video frames, but the legal regime of said identification had not yet been sufficiently explored in Ukraine.

Keywords: Digital Identification. Biometric Technologies. Portrait Expertise. Privacy. Face Identification.

INTRODUCTION

A person's face is the central feature by which one can be identified. It changes relatively little over time and is a typical identification object. Somehow, the person's identification by his or her face has been used by investigators since very ancient times. Even before the invention of photography, law enforcement agencies employed artists to draw portraits of criminals based on the victim's description. The invention of photography made it possible to photograph criminals, create card indexes, and identify a person by photos and not only directly as it was. It has expanded the opportunities of investigators in detecting crimes. The next step of the person identification by appearance was the creation of a facial composite, which was a tool that allowed to make an approximate portrait of a suspect provided by an eye witness without the involvement of a forensic artist. However, only the invention of the technology that allows identifying a person by a photo or video directly, without human intervention, has been a real revolutionary development in this field. Moreover, modern identification technologies often determine who is in the photo more precisely than traditional direct recognition by photos in the criminal proceeding (Inshyn et al., 2021).

C. Poirson states face recognition has become one of the most powerful biometric technologies over the last decade, capable of identifying and verifying people based on a digital image or video frame (Poirson, 2021). The modern investigative practice makes the research of this subject especially relevant. In particular, the recent case of Victoria Kotlenets caused a great resonance in the Ukrainian mass media. According to investigators, she resembled a woman who

escorted the Ukrainian military prisoners in Donetsk in August 2014. As for the woman, the investigators applied the facial recognition approach at the Forensic Center of the Ministry of Internal Affairs using her photos from social networks. At the same time, the defense provided alternative data for comparing photos using a modern batch data identification system. The court has now sided with the defense and released Victoria Kotlenets from custody (Shramovich, 2021). This example is illustrative but not unique. In particular, in 2017, a victim reported it to the US police service on the following issue. After a date at a bowling club, she found herself missing $400 and asked the manager to view the security footage that showed her companion stealing the money from her bag. Despite the clear evidence, the search for the woman's companion was difficult: she only knew his name, and he deleted his profile from the dating site where they had met. His number, then disconnected, was tied to a hard-to-track phone. The security video spotted his car in the parking lot, but the number plate was not visible. After some time, the investigator provided a photo from the victim's mobile phone for digital face identification. It helped to identify the man, his personal data, and the address (Merchlinsky, 2019).

Antoaneta Roussi points out that there are a lot of claims in the USA right now that are aimed at forbidding (at least temporary) the use of face identification technologies by the police (Roussi, 2020). To date, a lot of cities in the USA forbid, at least temporarily, the use of face identification technology by government agencies to enact legislation that would make the procedure of face identification more transparent. Europe and the USA are now considering suggestions on how to regulate this technology. However, Thakur and other scientists say it is important to remember that the digital identification system has been recently directed on a person’s identification, approvals of payments, identification of criminals, etc. So, the identification of criminals is not the main way to utilize such systems (Thakur et al., 2020).

Given the above, the purpose of this article is to analyze the theoretical and practical aspects of the use of digital face identification technology in Ukraine and to propose an optimal legal regime for the use of such technology in criminal proceedings based on the study.

METHODOLOGICAL FRAMEWORK

At this stage of the development of legal science, most legal scholars do not pay enough attention to the methodology of legal research. Legal research involves the interpretation of the law through various methods, such as interpreting the content of the text itself, analyzing case law, using the history of the law to determine the intentions of the legislator and studying the views of other legal scholars or experts. Scientific and legal research involving the use of

primarily inductive methods by the researcher (analytical research) differ from the positivist research paradigms both in form and essence. In general, in science, the researcher must indicate methods, procedures, statistics, and information about the boundaries of a study for it to be reproducible. However, analytical legal research cannot be considered strictly reproducible in this case since the materials, taken for generalization (for example, the most famous cases), cannot be often selected at random like samples in biology or respondents in sociology. Examples from practice, the scientists' approaches for analysis are selected on the principle of reputation and authority. Choosing just random cases from the practice of different courts at different times will not demonstrate the appropriate scientific effect.

N. Semchuk points out that legal science is currently actively seeking new solutions to methodology issues (Semchuk et al., 2019). Sunstein notes that when applying the method of legal analogy in the analysis of specific issues, the following components should be taken into account: causation, focus on details, avoidance of purely theoretical statements, and principles operating at low and medium levels of abstraction (Sunstein, 1993). T.R. Tyler points out that the classical method of legal research is a normative analysis of law (doctrinal analysis) that involves an attempt to understand the optimal balance of rights and responsibilities within the framework defined by law (Tyler, 2017). Claire Nolasco claims that the most common method of classical legal research in Europe is the IRAC acronym, which means a method of legal analysis that consists of a problem statement, analysis of legal provisions governing this issue, study of law enforcement practice, and formulation of conclusions (Nolasco et al., 2010).

Given the above, this study has an analytical nature, aims to study the current state of legal regulation on the issue of theoretical and practical aspects of the use of digital face identification technology in Ukraine, and applies the primarily inductive scientific method. In this scientific work, the inductive method of legal analysis is used as the main one, which involves a problem statement, analysis of the provisions, rights governing this issue, the study of the law enforcement, and formulation of conclusions.

RESULTS

As Bah points out, from the technical point of view, face identification is a computer program that is able to find, track, identify, and check a person's face by a photo or video that is made with a digital camera (Bah e Ming, 2020). There are a number of factors that influence the program: different light conditions, noise in the pictures, scale, pose, etc. Variations of the Local Binary Pattern (LBP) are usually used as an algorithm. It is a type of a visual descriptor used to classify

in computer vision as a special case of the texture spectrum model proposed in 1990. OpenCV (Open-Source Computer Vision Library) is also an often-used method. It is a library of functions and algorithms of the computer vision, image processing and numerical algorithms of a general-purpose type with open source.

Thakur described advantages of the OpenCV – the library that was created by Intel in 1999. It is mainly built to work in real-time image processing systems that include state-of-the-art computer vision algorithms (Thakur et al., 2020). Ramnya stated that a face is the most important part of a human body that unambiguously confirms the identity. Using facial features as biometric, you can implement a face recognition system (Ramya et al., 2020). There was a project used in practice to check attendance of students. The project was grounded on the face identification technology system that is based on OpenCV and showed a good result. Herewith Intorna and Nissenbaum paid attention to the fact that it is important to have an extensive photo base to compare the images for the right functioning of the digital algorithms (Introna e Nissenbaum, 2020). J. Detsing also paid attention to the technical advantages and the high accuracy of the method, sometimes even more than 90% (Detsing e Ketcham, 2017).

It is also important to mention that now, the most popular programs for face recognition are Clarifai, DeepFace, DeepVision, FaceFirst, Face++, OpenFaceTracker, Paravision, Rohos Face Logon, Trueface etc. At the same time, Google (Google lance) and Facebook have powerful face recognition capabilities as well. That is, today, face recognition systems are a software product owned by its developers, private companies, and distributed primarily on a commercial basis. For instance, in criminal procedure, an attorney may possess a high-quality and functional face recognition system that he bought. Meanwhile, investigators may have no face recognition system, because the state has not purchased such a system for the police yet.

The next important aspect of the face recognition system is the fact that for its successful functioning there is a need for an extensive library of humans' images that will be taken for comparison. One of the top-priority questions for the legal science is processing the digital photos of an individual, unbeknownst to him or her, with the purpose to identify a person. As C. Poirson pointed, the technology of the face recognition system is not only being used during investigations but also in a lot of other fields (Poirson, 2021). At the same time, scientists are seriously concerned about the limits of the use of the technology, because face recognition can indeed have a very serious and irreversible impact on fundamental human rights and civil liberties. Meanwhile, it is worth noting that from the criminal point of view, such human identification based on the physical characteristics, on one hand, may be classified as the subspecies of forensic portrait examination, because it also has an aim to clench the matter whether one

or different people are depicted in the presented photographs or other objective images of the person's appearance. On the other hand, given the possibility of conducting such a study using simple software in real time (i.e., ease of use), it can be compared with the use of the police databases or forensic records.

From a legal point of view, there are reasons to consider the results of digital visual identification of an individual as operational measures (for preliminary identification and construction of versions that will be supported by other evidence or refuted by them during the investigation in the future) as well as appropriate evidence in the form of expertise that will be provided to the court (Britchenko & Saienko, 2017). In this case, despite the almost identical technical procedure of identification, from a legal point of view, there will be some differences. From the point of view of criminal law, in this context, there are such problematic aspects as the legal regime of photographs imported into the face recognition databases and photographs used for comparison with those available in databases, as well as the limits of such technology in Ukraine in terms of privacy in criminal law.

Firstly, let us look at the way of dealing with the said problem abroad. C. Poirson pointed on the main features of legal regulation of the face identification technology in different countries. He also stated that the Chinese Cybersecurity Law from November 7th, 2016 gave to the Chinese government a big range of authority to regulate and control Internet services. Article 24, of this law, obliges Internet providers to identify the user before entering into the agreement or delivering them any services. Under the pretext of protection of users' rights, providers, social networks, and websites of China require users to make their photos available for further digital identification. Such an approach that is not democratic nonetheless makes China a world leader in the development of digital face identification technology. In contrast to China, Japan provides high standards of personal data protection according to the 2003 Act on the Protection of Personal Information. The Act provides for the consent of the data subject, except in exceptional cases. In exceptional cases, the use of such technologies without the consent of the subject may be possible only if the Ministry of Justice gives a special permit (Poirson, 2021).

In Europe, the processing of photographs is generally not considered to be the processing of biometric data unless such data are processed by a technical system for the purpose of unambiguous identification or authentication of an individual. However, the General Data Protection Order No. 2016/679 of 27 April 2016 prohibits the processing of images for identification purposes without the consent of the data subject (Poirson, 2021). Claire Merchlinsky notes that in the United States, face recognition is usually decided at the state level. Many states, including Massachusetts, California, and others, are currently considering

banning such use because of the high risk of human rights abuses. The rest of the states treat this technology with caution (Merchlinsky, 2019).

The legislation of Ukraine regulates the legal regime of photographs in a rather outdated way, without taking into account the development of technology. The Civil Code of Ukraine (2003) in Art. 303 still classifies photographs of an individual as personal papers and considers them as personal property of the person. The Law of Ukraine "On Information" (1992) contains a definition of the term “document”. In this case, the document is a material medium that contains information, the main functions of which are its storage and transmission in time and space. At the same time, the information is any information and / or data that can be stored on physical media or displayed electronically. As it can be seen, different laws in virtually the same sense operate with the concepts of personal "papers" and "documents". In this regard, it would be important for the legislator to unify the terminology by amending the Civil Code of Ukraine by clarifying, for example, "personal papers (documents)". Nevertheless, it should be noted that the Law correctly states that the main function of documents is to store information.

On the other hand, in accordance with Art. 307 of the Civil Code of Ukraine, an individual may be photographed, filmed, televised or videotaped only with his or her consent. A person's consent to be photographed, filmed, televised, or videotaped is presumed if the filming is carried out openly on the street, at meetings, conferences, rallies and other public events. In this case, an individual who has agreed to be photographed, filmed, televised or videotaped may demand the cessation of his or her public showing in the part that concerns their personal life. Expenses related to the dismantling of the image or record are reimbursed by this individual. The norm formulated in Art. 308 of the Civil Code of Ukraine indicates that a photograph, other works of art depicting an individual may be publicly shown, reproduced, distributed only with the consent of this person, and in case of death - with the consent of their heirs (except for the cases of posing for a fee) (Lytvyn et al., 2022).

The above gives grounds to conclude that such legal regulation was quite justified in pre-digital times, when the photograph had no direct identification value and could be used only as part of a paper file. In the digital age, the direct provision that an individual may be photographed or videotaped without his or her consent in any public place (without specifying whether such an image may then be stored, distributed, or included in an appropriate identification database) may be considered as excessive interference in their personal life. By contrast, a total ban on filming in public places will make it impossible for, for example, car video recorders, traffic cameras, etc. to work. Therefore, at this stage, the structure available in the Civil Code of Ukraine calls for rethinking in terms of the balance of public interests and private life.

The Law of Ukraine "On Personal Data Protection" (2010) indicates that consent of the personal data subject is a voluntary expression of the individual's will (on the condition that the person was informed) to give a permission for the processing of their personal data according to the aim of such processing that was expressed in written form or in any other form that provides an opportunity to confirm that there was such permission. In the field of e-commerce, the consent of the personal data subject may be given during registration in the information and telecommunication system of the e-commerce subject by marking the permission to process their personal data in accordance with the stated purpose of their processing, provided that such system does not create opportunities for personal data processing up to the moment of marking.

Article 264 of the Criminal Procedure Code of Ukraine (2013) points out that the search, detection and recording of the information contained in the electronic information system or its parts, access to the electronic information system or its part, as well as obtaining such information without the knowledge of its owner, possessor or holder may be carried out by decision of the investigating judge, if there is any data on the availability of the information in the electronic information system or its part that is important for a certain pre-trial investigation. It does not require the permission of the investigating judge to obtain information from electronic information systems or parts thereof, access to which is not restricted by its owner, possessor or holder or is not related to overcoming the logical protection principles.

Herewith, the compression of Art. 245 and Art. 160 of the Criminal Procedure Code of Ukraine involves receiving of samples for examination in the form of things and documents by the decision of the investigating judge in the order of temporary access to things and documents. Art. 182 of the Criminal Code of Ukraine (2011) sets responsibility for illegal collection, storage, using, destruction, sharing of confidential information about an individual or illegal alteration of such information, except cases provided by other articles of the Criminal Code of Ukraine. At the same time, the Criminal Code of Ukraine has an explanatory norm, according to which public, including through the media, journalists, public associations, trade unions, notification about a criminal or other offenses committed in compliance with the law, are not actions provided for in this article, and does not entail criminal liability.

However, the question arises: has the face recognition system ever been used illegally in the world? For example, the Data Protection Authority in Sweden fined the local authority 200,000 SEK ($20,700) last year as it used face recognition technology to monitor student attendance at school. Data Protection Authority in France said such a technology violates the EU General Data Protection Regulation. Local authorities in Skelleftea have illegally processed

sensitive biometric data and did not perform a proper impact assessment provided for consulting with the regulatory body and obtaining prior approval. Although the school provided parental consent to monitor students, the regulatory body did not consider this an adequate legal reason for collecting such personal data.

The regulatory body notes that some parts of the school can be called public spaces. However, students shall have the right to privacy when they are in the classroom. The decision stated that it would have been possible to record attendance without surveillance cameras since other ways existed. Apart from this case, Big Brother Watch researched that face recognition technology has been secretly used in shopping malls, museums, and conference venues in Britain (Levchenko et al., 2021).

The research described a situation where a 14-year-old child, wearing a school uniform, was misidentified by the facial recognition system and subsequently surrounded by four plainclothes police officers. They dragged her out to a side street, held her hands, interrogated and asked for her phone number, and even took her fingerprints. When the officers realized that the "system" was wrong, they released the child within ten minutes. However, the child remained scared and said that she felt as if the police were following her.

As for the situation in Ukraine, there is little experience in regulating face fixation and recognition systems. So, the Constitution of Ukraine stipulates that the collection, storage, use, and dissemination of confidential information about a person without his consent shall not be permitted except for the cases determined by the law and only in the interests of national security, economic welfare, and human rights. The local authority is known to use surveillance cameras. For example, there are more than 6,200 CCTV cameras with a face recognition system in Kyiv, but the grounds of local authorities to use them still are unclear. Unfortunately, no law provides for the powers of local authorities to use a surveillance camera.

At the same time, the police can use the information received from video surveillance systems set up within the territory of someone else's possession. Article 25 of the Law of Ukraine "On the National Police" contains provisions that allow the police to use the databases of the Ministry of Internal Affairs and other public authorities. As known, local self-government bodies and utilities do not belong to public authorities. There is a need to fill in such gaps and develop documents regulating access to video surveillance systems and processing of personal data.

Let us analyze all this contradictory set of normative legal acts from the point of view of criminal law. Firstly, let us note that photos from the bases and photos of a person that are used for the identification have a status of documents (although due to defects in legal technique it is called "personal paper"). Herewith,

it is important to mention that the law points correctly that the main function of the document is to store information. That is, these photos are confidential information and belong to the object of the crime, the set of facts of which is provided in the Art. 182 of the Criminal Code of Ukraine. From an objective point of view, the actions that are provided in the Art. 182 of the Criminal Code of Ukraine, may be divided into two categories: the first is collection, storage, using, detention and sharing of confidential information about a person. The second is illegal alteration of such information.

From the practical side, illegal actions against the photos that are used during digital identification, usually fall into the first category: illegal collecting of someone's digital photos, preservation of such photos (including digital data base) and detention of such photos (including identification purposes) and destruction of such photos which is also possible. However, talking about the second category, illegal changes of such information, committing violation of this nature is more unlikely. Criminal offense, the set of facts of which is provided in Art. 182 of the Criminal Code of Ukraine, does not provide any specific consequences. That is why establishing a corresponding causal correlation does not seem appropriate.

The subject of criminal offense is an individual of sound mind who have attained the age of 16. In this regard, according to this legal norm, it means that even an unscrupulous investigator may be liable for breaking the image processing rules, as well as the owner of the paid database if some photos were included in there in an illegal way, and also users of such databases if there were violations that occurred during the processing. An interesting question, therefore, is what the form of the guilt is in this case - intent or imprudent. On one hand, there is a possibility of performing such acts intentionally (with direct or oblique intention). However, given the complicated procedure of obtaining consent for the photo processing, especially digital images, to perform such acts due to imprudence or negligence is theoretically possible, because a person may not consider his or her actions as illegal regarding someone's digital photos due to the difficult processing procedure from the legal point of view. Also, it is important to note that the majority of such face identification systems work online within several jurisdictions. In this case, according to Art. 6 of the Criminal Code of Ukraine, a crime that was started, continuing, and finished or stopped on the territory of Ukraine is considered as the one that was committed in Ukraine.

Theoretically, any digital face identification databases used by at least one individual or legal person on the territory of Ukraine in breach of law fall under the criminal jurisdiction of Ukraine. This means both the opportunity of investigating and convicting the perpetrators on the territory of Ukraine and blocking the relevant content on the territory of Ukraine in case it violates the law.

At the same time, many photo comparisons programs where it is possible to identify a person by a photo online (Google lance, etc.) artificially partially block such an opportunity in order to protect the privacy of individuals.

As mentioned above, there are some grounds to consider results of digital visual identification of an individual as operational measures (for preliminary identification and construction of versions that will be supported by other evidence or refuted by them during the investigation in the future) as well as independent evidence of expertise that will be submitted to the court. Herewith, there is again a question of the legal status of the photos that are used for the identification. During uploading the photos to the Internet on your own or while taking photos in the public places, the permission of the subject is necessary. In fact, uploading a photo to the Internet in its current form on your own may be interpreted by the owner of the facial recognition database in their favor - as consent to comprehensive processing of personal data, including the import of the photos to the facial recognition database and the use of these photos for identification purposes in the future. On the other hand, there is always the possibility of challenging such a presumption as well as the constant possibility of withdrawing consent, making the processing of such information still legally risky for the owners of such image identification programs.

When conducting a pre-trial investigation, first of all, it is difficult to obtain digital photos without the consent of the suspect or accused. There are two options possible – to freely receive photos from the electronic information systems or parts thereof, access to which is not limited to its owner, possessor or holder and not related to overcoming the logical protection principles (for example, excluding the official website of the employer, a personal page in social networks and etc.). The second option is to receive temporary access to things and documents with the subsequent appointment of the relevant examination. It should be noted that, in general, the legislation of Ukraine on the protection of the rights of the subject to his or her own image is developing alongside the European tradition. In particular, cases of the image use without the consent of the subject are extremely limited. That being said, the protection of personal data in Ukraine is at a fairly high level. By contrast, the legislation in this field is quite imperfect all over the world, so the Ukrainian example, taking into account the clarifications proposed by the authors of this article, can be a model for other countries.

DISCUSSION

As it can be seen from what was stated above, the use of digital face identification technologies based on the image provides opportunities for the qualified investigation of crimes. Some of the foreign scientists such as C. Poirson (2021), L. Introna and H. Nissenbaum (2020), J. Detsing and M. Ketcham (2017);

Ramya (Ramya et al., 2020), etc. noted a number of technical advantages of this method. We fully agree with named scientist on the effectiveness of such approach. Herewith other scientist, for example Antoaneta Roussi, paid attention to the necessity to take into account human rights while using the technology; to limit the fields where the technology can be implemented at the legislative level, and also to set strict rules of using such technology by investigators.

There is currently a direct contradiction between the continuity of technological progress in the field of digital technologies and the need to protect human rights. In this case, the almost total ban which is supported by a number of countries is as detrimental as the extremely broad powers granted by the state to companies and law enforcement agencies in this field. It should be noted that the procedure for obtaining the consent of the subject of identification and the processing of images without such consent in different countries has significant national characteristics. However, there are also common trends. On one hand, the example of China, where companies are actually obliged to process images of users, is illustrative. On the other hand, it is the example of the European Union, where cases of such processing without the consent of the identification subject are extremely limited.

In comparison with foreign legislation, Ukraine has a fairly broad and reasonable regulation of the protection of human rights by law (including criminal) in terms of digital identification. At the same time, the legislation provides sufficient opportunities for law enforcement officials to use modern technology to identify criminals. The study of foreign experience is sufficient because theoretically any digital face identification database used by at least one individual or legal person in Ukraine in breach of law falls under the criminal jurisdiction of Ukraine. This means both the opportunity of investigating and convicting the perpetrators on the territory of Ukraine and blocking the relevant content on the territory of Ukraine in case it violates the law.

Facial recognition can indeed have a very serious and irreversible impact on fundamental human rights and freedoms. At the same time, maximizing benefits and mitigating risks depends on sound regulation of this issue at the legislative level. After conducting the study, we can agree on that. It is important to protect the rights of an individual who was photographed in a public place without his or her direct consent and a person who uploaded their own images to the Internet, given the recent developments of the digital age. In the modern context, the direct provision that an individual may be photographed without his or her consent in any public place (without an indication of whether such an image may then be stored, distributed, or included in an appropriate identification database) may be considered excessive interference with individual's privacy. By contrast, a total ban on filming in public places will make it impossible for, for

example, car video recorders, traffic cameras, etc. to work. Moreover, peculiarities of the use of digital face identification technology in Ukraine, taking into account the Ukrainian legislation, were analyzed for the first time. Especially since this method is already being used in practice. The obtained results can be considered the latest, as previously this issue has not been actively explored due to the innovative nature of digital face identification technology.

It is forbidden to identify a person's face who is in a public place. The EU temporarily bans face recognition technology to use in public places for three to five years. The EU considers this as the only way to prevent the risks associated with the rapid and uncontrolled distribution of face recognition software. In the media space, reliable news has repeatedly spread about effective ways to mislead the algorithms of the recognition technology. In the media space, reliable news has repeatedly spread about effective ways to mislead the algorithms of the recognition technology.

The draft regulation refers to the right of EU citizens under the General Data Protection Regulation – "not to be subject to a decision based solely on automated processing, including profiling" (Article 22 of the General Data Protection Regulation). Under the document, a new regulatory framework for artificial intelligence is introduced, which may include a time-limited ban on face recognition technology used in public places. The use of face recognition technology in public places by public or private entities is prohibited under the document for a certain period (up to 5 years). This period is needed to develop a reliable methodology for impact assessment of face identification technology and possible measures for risk management. Not everyone shares the precautionary measures Brussels takes. Law enforcement officials in Great Britain are testing face recognition software as an "innovative" way to identify people suspected of a crime. Even though Great Britain has left the EU, the draft regulation on AI (artificial intelligence) also matters there. The common European rules will apply here at least until the end of 2020. However, everything can change in the future. Negotiations on the future relationship will determine how the rules of Great Britain comply with EU requirements, including data processing and collection.

The EU sees perspectives in face recognition technology, but it takes time to introduce it gradually. European politicians give a message that the identification of a person is prohibited and indicate, at the same time, that this is an exclusively temporary measure. The goal is to get enough time to develop and implement an adequate legal regulation. The German government plans to introduce face recognition technology at 134 train stations and 14 airports following a successful test in Berlin. France is set to become the first country in the EU, which allows its citizens to access secure government websites using face

recognition software. The French Parliament is preparing a new regulatory framework that will allow using technology in the future.

At the same time, non-governmental organizations are concerned that face recognition technology is being introduced so fast. The Information Commissioner's Office in the UK has been urged to be cautious with face recognition technology. Brussels currently considers several solutions to ethical and legal issues caused by using "artificial intelligence" and software with corresponding algorithms. The Commission plans to implement minimum standards for government departments and use legally binding instruments if the use of "artificial intelligence" is of high risk in such areas as transportation, healthcare, law enforcement, and justice.

A Commission spokesperson said: "To multiply the benefits and address the challenges in using artificial intelligence, Europe must act as a whole and define its own path. Technology should serve purpose and people. So, the EU strategy will focus on the trust, guarantees, and security of citizens." The benefits of using "artificial intelligence" and associated software algorithms are well understood. The prospect of using facial identification technology seems like a winning strategy in many areas. However, the potentially negative consequences and possible violations of the rights enshrined in the General Data Protection Regulation call for balanced and gradual steps.

CONCLUSIONS

From a forensic perspective, the identification of a person by his or her physical characteristics, on the one hand, can be considered a subspecies of portrait examination, because it also aims to identify one or different individuals depicted in photographs or other objective images of human appearance. On the other hand, given the opportunity of conducting such a study using simple real-time software (i.e., ease of use), it can be compared with the use of police databases or forensic records. Today, facial recognition systems are software products owned by its developer, private companies, and distributed primarily on a commercial basis, which limits the use of such systems during the investigation.

An important aspect of the facial recognition system is the fact that their successful functioning requires the largest possible library of images that are taken for comparison. Therefore, one of the priority issues to be addressed by legal science is the processing of personal digital photos without the knowledge of that person in order to establish the identity. These photos are confidential information and relate to the subject of the crime, the set of facts of which is provided in the disposition of Art. 182 of the Criminal Code of Ukraine. From an objective point of view, the actions provided for in Art. 182 of the Criminal Code of Ukraine can be divided into two categories. First - collection, storage, using, destruction,

dissemination of confidential personal information. Second - illegal alteration of such information. From a practical point of view, illegal actions against photographs used in the process of digital identification are most likely to fall into the first category: illegal collection of other people's digital photos, storage of such photos (including in digital databases), use of such photos including for identification purposes) and even the destruction of such photos is also possible. However, the second category, illegal alteration of such information, the commission of such an encroachment in digitally identifying photos, seems unlikely. The subject of a criminal offense is an individual of sound mind who has attained the age of 16.

In this regard, according to this legal norm, it means that even an unscrupulous investigator may be liable for breaking the image processing rules, as well as the owner of the paid database if some photos were included in there in an illegal way, and also users of such databases if there were violations that occurred during the processing. An interesting question, therefore, is what the form of the guilt is in this case - intent or imprudent. On one hand, of course there is a probability of performing such acts intentionally (with direct or oblique intention). However, given the complicated procedure of obtaining consent for photo processing, especially digital images, to perform such acts due to imprudence or negligence is theoretically possible, because a person may not consider their actions as illegal regarding someone's digital photos due to the difficult processing procedure from the legal point of view. Also it is important to note that the majority of such face identification systems work online within several jurisdictions via the Internet.

Theoretically, any digital face identification databases used by at least one individual or legal person on the territory of Ukraine in breach of law fall under the criminal jurisdiction of Ukraine. This means both the opportunity of investigating and convicting the perpetrators on the territory of Ukraine and blocking the relevant content on the territory of Ukraine in case it violates the law. At the same time, many photo comparisons programs where it is possible to identify a person by a photo online (Google lance, etc.) artificially partially block such a possibility in order to protect the privacy of individuals.

During the pre-trial investigation, first of all, it is difficult to receive digital photos without the consent of the suspect or accused. There are two options possible – to freely receive photos from the electronic information systems or parts thereof, access to which is not limited to its owner, possessor, or holder and not related to overcoming the logical protection system (for example, excluding the official website of the employer, a personal page in social networks and etc.). The second option is to receive temporary access to things and documents with the subsequent appointment of the relevant examination.

Thus, one must abide by the law when processing biometric data, including face recognition, and the latest documents of the EU have only confirmed this. The GDPR generally prohibits such processing. Similar to the provision of the Law of Ukraine "On the Protection of Personal Data," these data can be processed only in particular cases (a person provides clear consent in order to protect his life or the case is of significant public interest) and when appropriate guarantees, adapted to these risks, are provided. Under the Data Protection Directive, law enforcement activity follows the same logic, allowing such data to be processed only when unconditionally necessary. On June 20, 2018, ther4e were amendments to the French Data Protection Act to comply with European documents. Consequently, if there is no consent, the owner, public or private, can process biometric data only when its first permission by law.

RECOMMENDATIONS

At present, a number of amendments to the basic legislation that regulates issues related to the legal regime of digital face identification are necessary. Based on the analysis, we propose to make certain changes in the legislation of Ukraine. One of the proposed changes is the unification of terminology through amendments to Art. 303 of the Civil Code of Ukraine by specifying, for example, "personal papers (documents)".

It is also necessary to radically change the wording of Art. 307 of the Civil Code of Ukraine that requires the consent of the subject to be photographed, filmed, televised or videotaped. Such consent is presumed if the filming is carried out openly on the street, at meetings, conferences, rallies and other public events. At the time this article was adopted, it was only possible to visually identify a person in a photo by his or her personal acquaintances, and not to accurately identify a person based on a photo only. Therefore, the provision that an individual who has agreed to be photographed, filmed, televised, or videotaped may require the cessation of a public screening in the part relating to his or her personal life that needs to be clarified insofar as it has become relevant not only to ban on a person showing his or her photo in terms of personal life, but also a ban on such use for digital identification purposes.

REFERENCES

Bah, S. M. & Ming, F. (2020). An improved face recognition algorithm and its application in attendance management system. *Array, 5*.

Britchenko, I. & Saienko, V. (2017). The perception movement economy of Ukraine to business. *Ikonomicheski Izsledvania*, *26*(4), 163-181.

Civil Code of Ukraine. (2003). Available at: https://zakon.rada.gov.ua/laws/show/435-15.

Criminal Code. (2011). Available at: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

Criminal Procedure Code. (2013). Available at: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

Detsing, J. & Ketcham, M. (2017). Detection and facial recognition for investigation. *2017 International Conference on Digital Arts, Media and Technology (ICDAMT), 407-411*. (Chiang Mai, 1-4 March 2017) Chiang Mai: IEEE.

Inshyn, M., Vakhonieva, T., Korotkikh, A., Denysenko, A. & Dzhura, K. (2021). Transformation of labor legislation in the digital economy. *InterEULawEast, 8*(1), 39-56.

Introna, L. & Nissenbaum, H. (2020). *Facial recognition technology a survey of policy and implementation issues*. New York: Center for Catastrophe Preparedness & Response.

Law of Ukraine "On Information". (1992). Available at: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

Law of Ukraine "On Personal Data Protection". (2010). Available at: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

Levchenko, I., Dmytriieva, O., Shevchenko, I., Britchenko, I., Kruhlov, V., Avanesova, N., Kudriavtseva, O., & Solodovnik, O. (2021). Development of a method for selected financing of scientific and educational institutions through targeted capital investment in the development of innovative technologies. *Eastern-European Journal of Enterprise Technologies, 3*, 55-62.

Lytvyn, N. A., Berlach, A. I., Kovalko, N. M., Melnyk, A. A. & Berlach, H. V. (2022). Legal regulation of the state financial guarantees of medical services for the population: Domestic and international experience. *International Journal of Health Governance*, Article in Press.

Merchlinsky, C. (2019). How facial recognition became a routine policing tool in America. Available at: https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251.

Nolasco, C., Vaughn, M.S. & del Carmen, R.V. (2010). Toward a new methodology for legal research in criminal justice. *Journal of Criminal Justice Education, 21*(1), 1–23. DOI:10.1080/10511250903518944.

Poirson, C. (2021). The legal regulation of facial recognition. *The Fourth Industrial Revolution and Its Impact on Ethics. Sustainable Finance*, 283-302. Cham: Springer.

Ramya, N., Manasa, D., Ramya Sri, N. & Naveed, Sk. (2020). Testing of modules for facial recognition. *EPRA International Journal of Research and Development (IJRD), 5*(11), 132-136.

Roussi, A. (2020). Resisting the rise of facial recognition. *Nature, 587*, 350-353.

Semchuk, N., Lykhova, S. & Demianenko, U. (2019). Using English as a foreign language when teaching subject of the criminal law cycle. *The Asian International Journal of Life Science. Supplement, 21*(2), 517–534.

Shramovich, V. (2021). She or she is not: a veteran of the Right Sector is suspected of escorting Ukrainian prisoners in Donetsk. Available at: https://www.bbc.com/ukrainian/news-55752337.

Sunstein, C. (1993). On analogical reasoning. *Harvard Law Review, 106*, 741–791.

Thakur, A., Prakash, A., Mishra, A.K., Goldar, A., & Sonkar, A. (2020). Facial recognition with Open Cv. *Computational Vision and Bio-Inspired Computing*. *Advances in Intelligent Systems and Computing, 1108*, 213-218. Cham: Springer.

Tyler, T.R. (2017). Methodology in legal research. *Utrecht Law Review, 13*(3), 130–141.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET