Ukrainian Journal of Ecology

Ukrainian Journal of Ecology, 2020, 10(5), 142-144, doi: 10.15421/2020_220

REVIEW ARTICLE

Ecological aspects of visual tracking technology and personal data protection

Remmikh E.A., Vasiliev A.A.

Altai State University, Barnaul, Russian Federation
**Corresponding author E-mail: anton_vasiliev@mail.ru*

Received: 08.09.2020. Accepted:22.10.2020

The article deals with the most important problems of protection of human rights in the field of personal data connected with information collection through the visual tracking. The possible risks of using CCTV (closed-circuit television) cameras and the consequences of their improper use are considered. In addition, the authors assessed the relationship between the public security interests and the need to protect the privacy of the individual citizen. This study is related to the widespread digitalization of society and the expansion of application scope regards the face recognition technology.

Keywords: Personal data; Environmental; Face recognition; Video surveillance cameras; Privacy

Introduction

Ensuring security has always been one of the priorities of the state. Moreover, the immanent need of a person for protection, which was ranked by a famous psychologist Abraham Maslow as one of the most important, in many respects determined and defines the necessity of the state itself. Even in XIX century, in the dictionary of F.A. Brockhaus and I.A. Efron it was stressed "personal and property security is the most important guarantee of human development"([The Brockhaus, 2019. Lack of security of personality and property is equivalent to the lack of any connection between human efforts and the achievement of the goals for which they are made. The citizens are willing to be partially restricted by specialized government agencies that, with a set of effective policing tools in their hands, will be able to provide security.

Of great interest in this context are the results of a large-scale sociological survey conducted by NORC, one of the largest independent social research organizations in the United States, together with the Associated Press. It showed that more than half of US citizens (54 percent) are willing to sacrifice their freedom if necessary for security and counter-terrorism purposes (AP-NORC, 2020). At the same time, it is most relevant to define the boundaries of such an intervention and to establish a clear procedure for its implementation. This topic becomes particularly important in the context of new digital technologies implementation. At present, Russia is actively implementing the "Safe City" project, which involves the use of a set of software and hardware and organizational measures to ensure video security and technical safety. Such systems are also being installed in some objects of transport infrastructure (airports, metro stations) to ensure transport security (Decree, 2016).

Methodology

According to some authors, the use of video cameras is not only an effective means of preventing offenses, but also an effective tool for their investigation (Gavrilin, 2019). In addition, the analysis of video streams in combination with the use of facial recognition technology in order to control the implementation of the ban on visiting the places of official sports competitions on the days of their conduct is also seen as promising. According to the researchers, the structural system should be designed in such a way that when a person subjected to this type of administrative punishment is recorded, he or she will be immediately detained (Shavaleyev, 2017). As far as the legislation is concerned, at present, there is no special legal regulation on the use of personal identification technologies and it is necessary to be guided by general rules, in particular by the legislation on personal data. According to the art. 3 of the Federal Law "On personal data", personal data are any information related to a directly or indirectly defined or identifiable natural person (Federal Law, 2006). The data on individuals, which are collected through video surveillance with a facial recognition system, are biometric personal data within the meaning of Article 11 of the said law, because they characterize the physiological and biological characteristics of the individual and are used to identify him.

T.A. Kuharenko, in the article-by-article commentary to the Federal Law N 152-FZ "On personal data", indicates that biometric data can be processed only with the consent of the personal data subject. Moreover, such consent should be necessarily executed in writing (Kukharenko, 2006). This is also established in the Clarifications of Roskomnadzor "On the Questions of Attribution of Photo- and Video Images, Dactyloscopic Data and Other Information to Biometric Personal Data and the Peculiarities of their Processing", which directly say: "Taking into account that the purpose of processing the above information in biometric identification systems is to determine the identity of a particular person, as well as the fact that this information contained in the template characterizes the physiological and biological characteristics of the person - the subject of personal data, then such strict requirements for the processing of biometric personal data are explained, first, by the nature of such data. Biometric data make it possible to identify at any moment the person concerned by the biological peculiarities inherent only in him/her. Therefore, their processing creates significant risks for the protection of citizens' rights and freedoms. The level of development of modern technologies makes it possible to falsify not only ordinary personal data, but also biometric data. Their leakage, for example, by changing their appearance, using special make-up that not only avoids identification, but also makes the system recognize as the face of another person, can have serious consequences for the person concerned: he or she will no longer be able to use compromised biometric data and subsequently identify himself or herself reliably (Brassolov et al., 2019).

At the same time, A.I. Saveliev in his comment to Federal Law No. 152-FZ notes that "a photo and video image of a face as such are not biometric data, but become it when the operator uses specialized facial recognition systems for various purposes, including security (Saveliev, 2017).

In view of this fact, the court dismissed the suit of a Moscow resident who demanded that the use of facial recognition systems in the work of surveillance cameras be recognized as illegal. He pointed to the fact that the obtained images can be identified only by comparing the image with those provided by the police. At the same time, the Unified Data Center (UDCD) itself, where the data from the cameras are flocked, lacks the necessary personal data (iris, height, weight and other biometrics) required for identification. In addition, Part 2, Article 11 of the FZ-152 establishes a number of exceptions in which consent to the processing of biometric personal data is not required at all. For example, data processing is provided by the Russian legislation on security (for example, the Federal Law "On security"); on detective-search activity (for example, the Federal Law "On detective-search activity"). On this basis, under the current legislation video surveillance with the recognition of persons in public places can be used without the written consent of visitors only if it is carried out for a public purpose and falls under the list of exceptions provided by Art. 11 of the Federal Law-152. These provisions are also correlated with Article 55 of the Constitution, which establishes that the rights and freedoms of a person and a citizen (including in the field of personal data) can be restricted by the federal law only to the extent necessary to protect the foundations of the constitutional order, the rights and legitimate interests of other persons, to ensure the defense of the country and security of the state.

The effectiveness of the system and the prospects of its application are confirmed by the data of the Ministry of Internal Affairs. Thus, according to a representative of the Main Directorate of the Ministry of Internal Affairs for Moscow, in two years of application of facial recognition technology it was possible to detain 90 wanted with the help of 1000 cameras installed outside the entrances of residential houses. In addition, every month, thanks to the subway cameras it is possible to detain from 5 to 10 criminals. At the same time, there was no need to increase the number of police officers (The Ministry, 2020). To identify the criminals in the above example were used technologies FaceT and FindFace - products of the Russian company NtechLab.

However, this is not the only company that develops facial recognition algorithm. For example, a number of other cities are using Securos Face Inspector based on Securos Premium 6.2 R3 software developed by the Russian company ISS as part of the Safe City project (Stepanov, 2012). It is not prohibited by law to use technologies of foreign companies, which raises reasonable concerns among researchers. Thus, E.N. Matyukhina points out in her article that the use of foreign software may pose a threat to national security (Matyukhina, 2019). In our opinion, in order to increase citizens' confidence in this technology, the possibility of using the algorithms of foreign companies should be excluded. When analyzing the pros and cons, the application of the system should also take into account the possibility of "false positive" recognition results. The developers themselves point out that it is impossible to create a system that would in 100% cases correctly identify a person. In a number of European countries, as well as in the United States, there have been many cases of incorrect recognition of faces. Thus, at the Champions League Final in Cardiff in 2017, the system mistakenly identified more than two thousand people as criminals, (Welsh police, 2018) and when testing software distributed by Amazon, it mistakenly identified 28 members of Congress as people who were arrested for crimes (Amazon face, 2018). Test results also revealed racial bias, a problem common to many facial recognition systems (Buolamwini, Gebru, 2018). All this has led, for example, to the complete ban on facial recognition technology in San Francisco. At the same time, human rights activists noted that even if facial recognition was 100% accurate, police could still abuse this technology against protesters or members of certain communities (San Francisco, 2019).

Discussion

In our opinion, such a measure is excessive, as it completely excludes the possibility of applying digitalization achievements to reduce crime rates. Nevertheless, in order to ensure a compromise between the desire of citizens to protect their privacy, to exclude the possibility of involuntary interference in it and the need to ensure security, it is necessary to clearly regulate the procedure for entering a person into a database of criminals and strictly define the range of those actors who may have access to such a database. The importance of detailed elaboration of these aspects is confirmed by the case of the detention in the metro of Mikhail Aksel, who was recognized by the system as a wanted person because his data were entered into it. After clarification of the circumstances, it turned out that there were no grounds for including Mikhail Aksel in the wanted person's database (Face recognition, 2020). Such cases, taking into account that the legal protection procedure in such a situation remains unregulated, significantly reduce the level of citizens' trust in the technology used. It is necessary to clearly define the circle of persons responsible for erroneous entry of persons into the search database and provide for the possibility, at the citizen's request, to delete his data from the register. In addition, it should be established that such data can be used only by court decision.

The procedure for accessing the resources of the Safe City system also deserves regulation that is more detailed. In accordance with the Order of the Government of the Russian Federation from 03.12.2014 N 2446-r such an order is determined in accordance with the access rights determined by regulatory legal documents and regulations of the relevant federal executive authorities. At the same time, specific goals and limits of the system usage are not defined. In our opinion, it is necessary to specify the conditions of access to the city video surveillance system in a single legislative act. In particular, to provide for liability for its illegal use for a purpose other than the protection of safety and well-being of citizens.

Conclusion

Summing up, the use of facial recognition technologies to reduce the crime and ensure the interests of citizens has a huge potential for development of technology. At the same time, the use of such software carries a certain risk associated with the interference of state authorities in the privacy of citizens and the possibility of data leakage (Polyakov, 2019). Thus, in order to implement the video surveillance programs in the most effective way, the procedure for working with the database, the subjective composition of persons having access to it and responsibility for violation of this procedure should be legally established. In addition, an effective method to increase the citizens' confidence in the system of recognition of persons will be the development of educational programs on personal data. Bringing to the public these data in accessible format ways will protect them in case of illegal interference with privacy (Vasiliev et al., 2019).

References

Amazon face recognition falsely matches 28 lawmakers with mugshots, ACLU says. Available from: https://www.theguardian.com/technology/2018/jul/26/amazon-facial-rekognition-congress-mugshots-aclu

AP-NORC Poll. (2020). Online surveillance is OK for the most. Available from: http://apnorc.org/news-media/Pages/News+Media/AP-NORC-Poll-Online-surveillance-is-OK-for-most.aspx

Brassolov, I.M., Chubukova, S.G., Mikurova, I.V. (2019). Biometrics in the context of personal data and genetic information: legal problems. Lex Russica, 1, 108-118.

Buolamwini, J., Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceed. I Conf. on Fairness, Accountability and Transparency. PMLR 81:77-91

Decree of the Government of the Russian Federation. (2016). 16.07.2016 No 678 "On requirements for transport security, including requirements for anti-terrorist security of objects (territories), taking into account the security levels for different categories of transport infrastructure objects and vehicles of sea and river transport". Collection of Legislation of the Russian Federation, 31, Art. 5012

Face recognition system. How it works on the example of Moscow and London. Available from: https://www.bbc.com/russian/features-48478959.

Federal Law. (2006). 27.07.2006 No 152-FZ "On Personal Data" (ed. from 31.12.2017) // Collection of Legislation of the Russian Federation, 31(1p.), Art. 3451.

Gavrilin, Yu.V. (2019). Technologies of the large data volumes processing in solving the problems of the criminalistic support of the law enforcement activity (in Russian). Russian Investigator, 7, 3-8.

Kukharenko, T.A. (2006). Commentary on the Federal Law of 27.07.2006 No 152-FZ "On personal data”. SPS ConsultantPlus.

Matyukhina, E.N. (2019). Russian and German legislation on personal data: a comparative analysis of approaches and practices. Lex Russica, 4, 170-178.

Polyakov, V. (2019). Criminalistics specifics of methods of committing computer crimes and peculiarities of their prevention. Religacion. Journal Of Social Sciences and Humanities, 4(19), 145-152. Available from: http://revista.religacion.com/index.php/about/article/view/518

San Francisco authorities have banned the use of facial recognition technologies. Available from: https://www.forbes.ru/tehnologii/376099-vlasti-san-francisko-zapretili-ispolzovanie-tehnologiy-raspoznavaniya-lic.

Savelievm, A.I. (2017). Scientific-practical article-by-article commentary on the Federal Law "On Personal Data". Statute, SPS ConsultantPlus

Shavaleyev, B.E. (2017). Execution of an administrative ban on visiting the places of official sports competitions in the days of their holding. Administrative law and process, 7, 80-82.

Stepanov, A.A. (2012). Introduction of Intelligent Facial Recognition Systems on the Objects of the Russian Ministry of Internal Affairs in the Omsk Region. Prospects and problems of realization. Information technologies, communication and information protection of the Ministry of Internal Affairs of Russia, 2, 151-152.

The Brockhaus and Efron Encyclopedic Dictionary. (2019). I.E. Andreevskij (Ed.). St. Petersburg: Tipo Lithography (I.A. Euphron).

The Ministry of Internal Affairs summed up the test work of facial recognition systems in Moscow. Available from: https://www.vedomosti.ru/technology/articles/2019/06/26/805163-mvd-podvelo?utm_source=yxnews&utm_medium=desktop.

Vasiliev, A., Zemlyukov, S., Ibragimov, Zh., Kulikov, E., Mankovsky, I. (2019). Ethical and legal aspects of the use of artificial intelligence in Russia, EU, and the USA: comparative legal analysis. Religacion. Journal of Social Sciences and Humanities, 4(19), 101-109. Available from: http://revista.religacion.com/index.php/about/article/view/511

Welsh police wrongly identify thousands as potential. Available from: https://www.theguardian.com/uk-news/2018/may/05/welsh-police-wrongly-identify-thousands-as-potential-criminals

Citation:

Remmikh, E.A., Vasiliev A.A. (2020). Ecological aspects of visual tracking technology and personal data protection. *Ukrainian Journal of Ecology, 10*(5), 142-144.