GIS Odyssey Journal

2023 • Volume 3 • Number 2

https://doi.org/10.57599/gisoj.2023.3.2.107

Kamil Czaplicki[1]

# USE OF ARTIFICIAL INTELLIGENCE IN REMOTE BIOMETRIC IDENTIFICATION SYSTEMS

**Abstract:** Work is currently underway to regulate the use of artificial intelligence. The article presents the ideas and principles of creating remote biometric identification systems using AI technologies. Risks to privacy and possible scenarios for the use of such systems are presented.

**Keywords**: biometrics, artificial intelligence, remote biometric identification systems

Received: 27 November 2023; accepted: 22 December 2023

[1] Cardinal Stefan Wyszyński University, Faculty of Law and Administration, Department of Informatics Law, Warsaw, Poland, ORCID ID: https://orcid.org/0000-0002-3777-4339, email: k.czaplicki@uksw.edu.pl

## Introduction, material and methods

The article uses the method of analyzing legal texts and scientific publications. The historical method was also used to illustrate technological changes. The materials used in the article are legal acts created at the European Union level and English-language scientific articles.

**The idea of artificial intelligence.** Artificial intelligence is a topic that has been widely discussed in recent times. Although the idea itself emerged in the 1950s, when John Mc Carthy first used the phrase at the Dartmount Conference, it is only in recent years that the development of digital transformation has made a wide audience aware of the possibilities of using this tool. The literature indicates that artificial intelligence (AI) is the science of how to produce machines equipped with some of the characteristics of the human mind (Sheikb et al., 2023), such as the ability to understand language, recognize images, solve problems and learn. Jerzy Cytowski, in the Great Encyclopedia of Law (Wielka Encyklopedia Prawa, 2021), pointed out the synergy of artificial intelligence with the environment in which it operates, stressing that artificial intelligence is a device or computer system capable of analyzing the environment in which it operates and learning and acting in response to stimuli acquired from the environment (Szpor et al., 2021). Artificial intelligence broke through into the general public consciousness in the second half of 2022, when the so-called GPT chat appeared (Oguz et al., 2023). Because it is a text generator designed to converse with the user, for many people it has become the epitome of a viable conversation partner, a helper who writes papers for us, translates text, or solves problems such as climate problems at a very fast pace (Biswas, 2023). The GPT chat, despite the fact that it has contributed to the popularization of artificial intelligence, is not an example of its strict application. More and more research and scientific centers are conducting research on the use of artificial intelligence, more and more complex models and algorithms are being created, and new applications and implementations are emerging. Global companies, seeing its potential, are commercializing many of its applications in their own operations. Artificial intelligence algorithms are used in banking, information technology, communications, medicine, law, customer service, architecture, logistics, spatial information systems or the military, among others (Bramer, 2004). Recently, there has also been a growing role for artificial intelligence algorithms used in the process of identifying identities, including those carried out in real time without the consent or awareness of the person being identified. More and more applications of artificial intelligence, raise legitimate concerns about their security and violation of, for example, our privacy. Unfortunately, this is a new technology, largely ahead of current regulations. The European Commission, in an effort to maintain the technological superiority of the European Union countries, while at the same time ensuring the harmonious development of artificial intelligence technology while protecting the fundamental rights of European residents, has taken the initiative to create a separate piece of legislation regulating the most important issues of artificial intelligence.

**Legal regulation of artificial intelligence systems.** On April 21, 2021. The European Commission submitted a proposal to adopt a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence and amending certain legislative acts of the union (Com 2021) 206 final 2021/0106 (COD) (https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52021PC0206). As indicated in the preamble to the regulation, "The purpose of the regulation is to improve the functioning of the internal market by establishing a single legal framework, in particular for the development, marketing and use of artificial intelligence in accordance with the values of the Union". The draft regulation seeks to regulate a number of issues related to the use of artificial intelligence in the European Union area. Importantly, it was stressed that technological development necessitates rational legislation that supports the development of technology while guaranteeing respect for fundamental rights.

The draft regulation envisages basing the regulation of artificial intelligence on risk analysis, imposing a number of restrictions on high-risk systems. The originators of the project considered the use of a risk-based legal framework to be a better solution than general regulation of all artificial intelligence systems. The types of risks and threats should be determined on a case-by-case and sector-by-sector basis. Risks are also to be calculated, taking into account the impact on rights and security. The draft explicitly prohibits some particularly harmful practices using artificial intelligence, which are contrary to EU values (e.g. social categorization). In the case of high-risk systems, the use of which may be a threat to health and safety or fundamental rights, a number of specific restrictions and safeguards have been proposed, which the originators assume should contribute to the sound protection of citizens' interests. Before such systems can begin to be used, they will have to meet a number of horizontal mandatory requirements and will have to undergo procedures for assessing their compliance. In the draft regulation, a number of definitions have been introduced, including, among others, the definition of artificial intelligence, user and provider, purpose of training data validation data, biometric data, effective operation of the artificial intelligence system, post-market monitoring, test data, emotion recognition system or national supervisory authority.

**Biometric data – concept and types.** The draft regulation includes remote biometric identification systems in the catalog of high-risk artificial intelligence systems. Biometrics is a technique for measuring living beings, aimed at methods of automatically recognizing people based on their physical characteristics (Vacca, 2007). Biometric systems use so-called biometric data in the process of identifying (or verifying ) identity. Recital 7 of the preamble to the draft Regulation indicates that the concept of biometric data used in this Regulation is consistent with the concept of biometric data as defined in Article 4(14) of Regulation (EU) 2016/679 of the European Parliament and of the Council, Article 3(18) of Regulation (EU) 2018/1725 of the European Parliament and of the Council, and Article 3(13) of Directive (EU) 2016/680 of the European Parliament and of the Council, and should be interpreted in a manner consistent with this concept. Despite this, the legislator decided to reinsert the definition of biometric data into the draft regulation. Article 3(33) indicates that "biometric data" means personal data resulting from special technical processing that relates to physical, physiological or behavioral characteristics of a natural person and enables or confirms the unambiguous identification of that person, such as facial image or dactyloscopic data.

We divide biometric data into two categories: anatomical data called genotype and behavioral data called phenotype. Anatomical data is related to a person's physical characteristics and includes fingerprint, iris of the eye, vein pattern of the hand or wrist, voice color, odor, facial geometry, hand geometry, facial temperature distribution, retina, DNA identification, ear geometry, skin surface analysis. Behavioral data is related to our behavior and requires movement for verification. Behavioral traits include the movement of the mouth, eye movement, the way we type, including the way and speed of typing, voice characteristics or the way we walk (Nanavati et al., 2002). A biometric trait, in order to be used in an identity confirmation system, must be characterized by five factors: immutability, uniqueness, indestructibility, measurability and acceptability. In addition, the European Commission, in Biometrics at the Frontiers: Assessing the Impact on Society, indicated that a biometric trait must be characterized by universality, uniqueness, immutability, retrievability, efficiency , acceptability and resistance to fraud. (Biometrics AT the Frontiers: Assessing the Impact on Society, Technical report series EUR 21585 EN, p. 37).

Biometrics, despite being considered one of the top ten technologies that could revolutionize the world (Pugliese, 2010), is also considered a highly privacy-invasive technology that could infringe on citizens' fundamental rights. Much attention has been paid to biometric technology in the RODO Regulation, which has largely regulated the processing of biometric data. It is commonly used in identity documents, in securing sensitive areas requiring access control or in banking. In addition, biometrics is one of the three main methods of identity identification. The other two methods are: based on what we know (passwords, pin codes) and based on what we have (cell phone, access card) (Walte, 2014). Biometric identity identification is characterized by speed, non-invasiveness, simplicity and certainty of result.

As a rule, it proceeds in a flowchart, where the first block is the collection and recording of the master feature. In this process, it is necessary to acquire the best possible sample of the biometric trait, since any distortion of the trait will affect subsequent processes. In the second block of processes, the user's identity is declared (e.g. by entering an individual number or applying a card with stored data). In the next block of processes, the reader takes the biometric characteristic of the person who previously declared his identity, and in the fourth block of processes, a comparison of the collected characteristic with the stored pattern takes place, and a decision is made about the positive or negative result of identity identification (verification).

## Results and discussion

**Remote biometric identification systems.** Nowadays, one can increasingly observe the trend of creating remote identity identification systems. This is largely due to the need to carry out the process of identity identification efficiently and quickly, without having to take out documents, magnetic cards, stand in queues, or even touch devices that can carry viruses and bacteria. Also important in this is the process of fighting terrorism or even widely understood threats (including kidnapping and search for missing persons). Remote identification is used by both police authorities and private companies. In the latter context one can point to, among other things, the identification of employees and customers to improve customer service. Remote identity identification is also the basis of many smart city and smart house services. It serves as part of the fight against homelessness and theft (Tan, 2020).

Technological developments, including the creation of cameras with increasingly better quality parameters, have made it possible to take biometric patterns and distinguish them from a greater distance than before. Biometric features that can be collected from a distance are, in particular, photos (image) but also iris of the eye, or even the way of movement. Such systems, compared to systems based, for example, on RFID technology or device identification (e.g. phones), guarantee the identification of a person, not a device. The device can be carried by someone else and then the identification result will be falsified. It is worth noting at this point that biometric identification based on the image (photos of the face) has many technical limitations and, compared to other biometric features, is more susceptible to external influences (Bharadwaj et al., 2013). Systems based on the facial image, use the pursuit of a natural way in everyday interactions to identify people based on anatomical differences in the face, are non-invasive and do not require the cooperation of the person being identified. On the other hand, however, the face is characterized by variability, flowing from natural grimaces and facial expressions triggered by conversation, emotion or illness. The face is subject to aging processes, which can change it to a great extent over a lifetime. In addition, using simple ways, we can easily change its appearance, for example, by using a beard, mustache, glasses. The impact of social changes after the coronavirus pandemic, where covering one's face with a mask no longer surprises anyone and can be considered a natural way to shuffle around in public, is also not insignificant. An additional problem is the environment of the face under examination, the influence of lighting, the reflections created or its movement.

The creation of remote identity identification systems, mainly those based on biometric identification, raises many controversies. Such systems perform processing of personal data without the knowledge and, more importantly, without the consent of the person subjected to the identification process. It is worth noting here that one of the main ideas of the data protection law reform expressed in the RODO Regulation was data autonomy and informed decision-making of citizens about the processing of their personal data (Vold & Whittleston, 2019). Being subject to a continuous identification process modeled on China's Public Trust System (Social Scoring System) raises many concerns about citizens' privacy and the preservation of their fundamental rights. There is no doubt that the legal regulations in the European Union and China regarding the protection of personal data are quite different, but more importantly, the awareness of data protection and privacy among Europeans and Chinese is quite different. In China, the public attaches much more importance to the development of the state and overall prosperity than to the protection of their own privacy (Lucero, 2019).

Remote identity identification processes have been accelerated by the emergence of artificial intelligence algorithms, supporting work in large volumes of data. Able to quickly analyze uploaded photos and recordings and compare extracted biometric characteristics with stored patterns. This solution is revolutionary from the point of view of speed and non-invasiveness, while bringing a very high level of efficiency to identity identification processes. It is worth noting, however, that this solution can invade the privacy of people unaware of the identification process and their identity in a huge and uncontrollable way. Such tools allow tracking, recording the route of movement, analyzing the way and mode of operation. It is a tool of remote and widespread social surveillance. Such systems can create a sense of constant surveillance and indirectly discourage the exercise of freedom of assembly and other fundamental rights.

The European Commission has recognized this risk of using remote biometric identification for the rights set forth in the Charter of Fundamental Rights, among others (OJ EU. C. 2007 No. 303, p. 1 as amended). In the draft regulation of the act on artificial intelligence) (https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52021PC0206) introduced in Article 5 a general rule prohibiting the use of real-time remote biometric identification systems in public spaces. As defined in Article 3 para. 36 of the proposed regulation, "remote biometric identification system" means an artificial intelligence system for identifying individuals remotely by comparing a person's biometric data with biometric data contained in a reference database, without the user of the artificial intelligence system knowing in advance whether the person will appear in the system and can be identified; and according to Art. 3(37) of the proposed regulation, "remote biometric identification system in real time" means a remote biometric identification system in which biometric data collection, comparison and identification take place without significant delay. Such a system is considered to be one in which identification occurs immediately, but also with a slight delay. The term remote biometric identification system as used in the proposed regulation is functionally defined as an artificial intelligence system for identifying individuals remotely by comparing a person's biometric data with biometric data contained in a reference database, without prior knowledge of whether the person will be in the database and can therefore be identified, regardless of the specific technology and the specific processes or types of biometric data used. The service provider has distinguished between two systems: the "real-time" remote biometric identification system and the "post-factual" remote biometric identification system, taking into account their different characteristics and modes of operation, and most importantly the different risks associated with them. With "real-time" systems, biometric data collection, comparison and identification occur immediately or without significant delay. "Real-time" identification systems involve the use of "live" or "near real-time" recorded material, such as video generated by a camera or other device with similar functionality. In contrast, with "post-factual" identification systems, biometric data has been taken earlier, and comparison and identification occur with a significant delay. This applies to materials, such as photos or video generated by closed-circuit television cameras or private devices, which were recorded before the system was used on an individual.

The mentioned general rule prohibiting the use of real-time remote biometric identification systems in public spaces applies to systems used for law enforcement purposes. The legislator used the general formulation of law enforcement, which should be interpreted as the general task of ensuring that people behave in accordance with the regulations set forth in the law. In the absence of an indication by the legislator, it should be broadly assumed that it refers to both generally applicable laws and internal regulations.

The legislature has adopted three exceptions to the general rule prohibiting the use of real-time remote biometric identification systems in public spaces for law enforcement purposes:

1. targeted search for specific potential victims of crime, including missing children;
2. to prevent a specific, serious and imminent threat to the life or physical safety of individuals or a terrorist attack;
3. to detect, locate, identify or prosecute the perpetrator of a crime or suspected perpetrator of a crime referred to in Article 2(2) of Council Framework Decision 2002/584/JHA and punishable in the Member State concerned by a custodial sentence or a security measure involving deprivation of liberty for a maximum period of at least three years, in accordance with the law of the Member State concerned.

The legislator has indicated that these exceptions may be applied only if and to the extent that such use is absolutely necessary for the purposes indicated above. This exception, therefore, is defined very generally, and each use must be in accordance with Article 5 of the proposed regulation. Control of compliance with the purposefulness of the exception as well as its absolutely necessary nature is carried out in accordance with Article 5, para. 3. the competent judicial or administrative authority which shall issue each time a permit to perform remote real-time biometric identification. This authority shall issue permission before the biometric identification processes have even been initiated , unless there is an emergency and justified case of using the system without the approval of the judicial authority, in which case such approval shall be issued during or after the process. The competent judicial or administrative authority shall grant permission only if it is convinced, on the basis of objective evidence or clear grounds brought to its attention, that the use of the "real-time" remote biometric identification system in question is necessary and proportionate to achieve one of the objectives set forth in the Regulation. The judicial or administrative authority shall also take into account:

1. the nature of the situation necessitating the possible use of the system, in particular the severity, probability and scale of the damage caused if the system is not used;
2. the consequences of the use of the system on the rights and freedoms of all persons concerned, in particular the severity, likelihood and scale of such consequences.

It is worth noting here that the draft regulation only regulates the use of biometric systems for real-time remote identification of identity for law enforcement purposes.

Any other systems using remote processing of biometric data must still comply with all requirements under Article 9(1) of Regulation (EU) 2016/679, Article 10(1) of Regulation (EU) 2018/1725 and Article 10 of Directive (EU) 2016/680, as applicable. According to Annex III to the draft regulation, artificial intelligence systems intended to be used for remote biometric identification of individuals "in real time" and "post factum", qualified as high-risk systems.

June 14, 2023. The European Parliament passed the negotiating position on Artificial Intelligence Act by a large majority (499 votes in favor, 93 abstentions by 29 votes against). During the discussion, a great deal of space was devoted to the issue of using artificial intelligence systems in biometric identity identification processes. Despite a number of amendments (https://www.europarl.europa.eu/doceo/document/A-9-2023-0188_PL.html) by MEPs and appeals from organizations defending fundamental rights and privacy, MEPs and decided not to completely ban the use of biometric identity identification systems in real time, and decided to deepen judicial review of applications for its use.

## Conclusions

Artificial intelligence is a technology that is becoming increasingly important. It can be used in many systems based on large data sets (including GIS systems). Attempts to regulate artificial intelligence are made both at the state level and at the level of international organizations. The remote biometric identification systems described in the article and the use of artificial intelligence algorithms in them may violate the privacy of people and therefore must be subject to strict legal control.

## References

Bharadwaj S., Vatsa M., Singh R. (2014). Biometric quality: a review of fingerprint, iris, and face. EURASIP Journal Image and Video Processing, no. 34. https://doi.org/10.1186/1687-5281-2014-34

Biometrics at the Frontiers: Assessing the Impact on Society (2005), Technical report series EUR 21585 EN, p. 37.

Biswas S.S. (2023). Potential Use of Chat GPT in Global Warming. Annals of Biomedical Engineering, vol. 51, pp. 1126–1127. https://doi.org/10.1007/s10439-023-03171-8

Bramer M., Devedzic V. (2004). Artificial Intelligence Applications and Innovations, IFIP 18th World Computer Congress TC12 First International Conference on Artificial Intelligence Applications and Innovations (AIAI-2004), 22–27 August 2004, Toulouse, France.

Lucero K. (2019). Artificial Intelligence Regulation and China's Future, Columbia Journal of Asian Law, vol. 33, no. 1, pp. 109–110.

Nanavati S., Thieme M., Nanovati R. (2002). Biometrics Identity Verification in a Networked World, p. 10.

Oğuz F.E., Ekersular M.N., Sunnetci K.M., Alkan A. (2023). Can Chat GPT be Utilized in Scientific and Undergraduate Studies? Annals of Biomedical Engineering. https://doi.org/10.1007/s10439-023-03333-8

Pugliese J. (2010). Biometrics, Bodies, Technologies, Biopolitics. New York, p. 1.

Sheikh H., Prins C., Schrijvers E. (2023). Artificial Intelligence: Definition and Background. In: Mission AI. Research for Policy. Springer, Cham.

Tan M., China: Facial recognition and its legal challenges, https://www.taylorwessing.com/en/insights-and-events/insights/2020/05/china--facial-recognition-and-its-legal-challenges [access: 25.11.2023].

Vacca J. (2007). Biometric Technologies and Verification System, Elsevier, p. 3.

Vold K., Whittleston J. (2019). Privacy, Autonomy and Personalised Targeting: rethinking how personal data is used. In: C. Veliz (ed.), Raport on Data, Privacy, and the individual in the Digital Age.

Walter W. (2014). Security for Service Oriented Architectures, CRC Press, p. 4.

Wielka Encyklopedia Prawa, tom XXII Prawo Informatyczne (*The Great Encyclopedia of Law, volume XXII Information Technology Law*). (2021). In: G. Szpor, L. Grochowski (ed.), Fundacja Ubi Sociatas, ibi ius, p. 435.