RAIS RESEARCH ASSOCIATION for INTERDISCIPLINARY STUDIES
April 6-7, 2023

DOI:10.5281/zenodo.7900818

Biometric Identification: Opportunities and Challenges in the Digital World

Nicoleta-Elena Hegheș

Researcher 2nd Degree at "Andrei Rădulescu" Legal Research Institute of Romanian Academy, Bucharest, Romania, nicoleta.heghes@icj.ro
Professor, PhD, "Dimitrie Cantemir" Christian University of Bucharest, Romania, nicoleta.heghes@ucdc.ro

ABSTRACT: Biometrics involves automatic methods of recognizing individuals based on physical or behavioral characteristics. These methods include fingerprints, retina and iris scanning, hand and finger geometry, voice feature recognition and facial recognition. Biometric technologies have become the preferred solutions for a wide range of applications. Biometrics is already incorporated in national security solutions, such as improving airport security, border control, verifying identification documents and visas, preventing identity fraud. Electronic identification systems have several advantages over well-known traditional identification methods, namely paper documents or personal verification. They are safer, much more efficient and very convenient. Consequently, biometric recognition systems are now being implemented in many government applications, including electronic identity cards, electronic passports, but also civil applications such as logging into a PC, laptop, mobile phone, internet access, smartcard etc. Identification elements cannot be lost, forgotten or stolen, as happens with passwords, identity cards or bank cards, as physiological characteristics have the advantage of being relatively stable over time.

KEYWORDS: identity, identification, authentification, biometrics, biometric identification

Introducere

The term *biometrics* comes from the Greek words' *bio* - life and *metreia* - to measure. Automated biometric systems have been available for several decades because of significant advances in computing power. Many of these new automated technologies are based on ideas born hundreds or even thousands of years ago.

The first modern biometric systems were introduced commercially in the 70s of the last centuries at the University of Georgia and later on Wall Street in the USA. They consist of simply scanning the hand to measure the length of the fingers. This system, called hand geometry, developed in the following years with a high implementation rate, especially in institutions where high security devices were required. In essence, biometric technology consists in the automatic identification or verification of a person using their anatomical and behavioral characteristics (Aron 2010, 12).

Biometrics is defined as the study and application of scientific and/or technological methods designed to measure, analyze and/or record the unique physiological or behavioral characteristics of humans. In fact, many of us already use biometrics in the form of our fingerprints and face (Goodner 2023).

Biometrics is a traditional method of identifying the individual with the help of modern technical and scientific means, based on his anatomical and behavioral characteristics. These characteristics must be universal, unique, permanent, collectable and measurable (Nechita 2009, 260). In other words, it refers to the use of identifiers and distinctive behavioral and anatomical features for the automatic recognition of a person. As biometric identification becomes more common and reliable it is increasingly used as the default authentication technology.

Biometrics implies the physical presence of the person at the identification point. Therefore, it is not enough for the individual to have an ID just as it is not enough to remember a code or a password. By replacing identity documents, keys or passwords, biometric techniques

help prevent fraudulent use of banking systems, cell phones, computers, automobiles, the Internet etc. The rapid evolution of biometric technology has allowed a wide application of them in the field of identifying criminals as well as in securing state institutions or those at risk including those of detention (Aron 2010, 12-13).

Identity, identification, authentication

When we are discussing about biometrics, the terms identity, identification and authentication are often confused with each other.

Identity constitutes one of the fundamental concepts of thought and, at the same time, an important means of researching the objects of the material world, with wide application to the most diverse fields of science: physics, chemistry, biology etc., including forensics. There is almost no thought process outside of the principle of identity. However, knowledge is not limited to identification, but includes it as a constituent element of a complex and multilateral process (Ionescu and Sandu 2011, 29). In the research stage of certain legal phenomena, the auxiliary sciences use scientific means specific to other sciences – physics, chemistry, medical sciences, mathematics, etc. (Boghirnea 2013, 13).

Identity is the character of what is identical (unique) or "the property of an object to be and remain at least for a certain time what it is, its quality to preserve for a certain time its fundamental characters" (Colectiv 1978, 341). Therefore, identity is a concept that many fields of knowledge cannot dispense with. In logic, it represents one of the basic forms of correct thinking. In other sciences, the notion is used as a means of research in accordance with the tasks of each.

From an etymological point of view, *to identify* a person refers to the activity of *ascertaining the person's identity,* that is, to individualize him in society, but also in the set of social relations.

The identification of a person is possible not only through technical methods, but also based on the statements of an eyewitness or the victim, within procedural activities, such as, for example, group recognition carried out in accordance with forensic tactical rules. This process is possible due to the perception of objective reality and awareness of the properties, characteristic features of a person or an object that is individualized within the broader category of similar beings or things. We are in the presence of the recognition of persons or objects, resulting from a thought process through which the characteristics of several objects or persons were compared in order to establish their identity or non-identity (Suciu1972, 16).

Electronic identity. One of the essential pillars of Romania's digitization is the electronic identity. Simplifying access to electronic public services requires a unique identification element, which is recognized by all institutions and authorities, so that access to several electronic public services does not involve repeating authentication procedures. Electronic identification will provide citizens with a valid, verified identity. In relations with public institutions, documents signed with the digital certificate in the virtual space will have the same value as documents signed holographically, on paper (Authority for the Digitalization of Romania 2023).

The identification of a natural person has the legal effect of individualizing him within the legal relations in which he participates. For the individualization process of the person, it is necessary to identify them according to criteria regulated by legal norms from different branches of law. In Romanian Civil Law, the identification data are only the name and surname and the domicile of the person (the classic identification attributes of the natural person are the name, domicile and marital status).

All other data are personal data protected by law that have a special regime, they are not disclosed in any situation, but only to institutions and companies authorized to manage them.

Biometric identification answers the question of *who you are* - the one-to-many matching process compares the data entry biometric data with all other entries in a database. For example, an unknown fingerprint found at a crime scene will be processed to identify who it belongs to.

Personal data is any information that relates to an identified or identifiable natural person. The various information collected can lead to the identification of a certain person also constitute personal data (European Commission 2023).

According to the definition in Art. 4, point 14 of the General Data Protection Regulation (Regulation no. 679 of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/ CE (General Data Protection Regulation), published in the Official Journal with number 119L of May 4, 2016), the notion of *biometric data* encompasses personal data "resulting from specific processing techniques related to physical, physiological characteristics or behavioral information of a natural person that allows or confirms the unique identification of that person, such as facial images or dactyloscopy data". These types of data are part of the category of sensitive data, the processing of which is, in principle, prohibited according to the provisions of Art. 9, par. (1) from RGDP (Goicovici 2021).

According to art. 3 point 1 of Regulation (EU) no. 910/2014 of the European Parliament and of the Council of 23 July 2014, on electronic identification and trust services for electronic transactions on the internal market and repealing Directive 1999/93/EC, published in OJ L 257, 28.8.2014, pp. 73 -114 *electronic identification* means *"the process of using personal identification data in electronic format, uniquely representing either a natural or legal person, or a natural person representing a legal person"* (For the repeal of the Directive see more details Vâlcu 2012, 40-42).

The most common types of biometric authentication are fingerprint recognition, facial recognition, and voice recognition. The aforementioned regulation defines in art. 3-point 5 *authentication* as *"an electronic process that allows to confirm the electronic identification of a natural or legal person or the origin and integrity of data in electronic format".*

Biometric authentication answers the question of whether *you are the person you say you are* - the one-to-one matching process compares biometric data entry with a single input (typically you that has been previously recorded for reference) in a database.

Biometric techniques

As biometric techniques (Nechita 2009, 266-267) we list:

- fingerprints;
- palm prints;
- hand dimensions;
- thermal image of the hand;
- digital image of the hand;
- eye photography (iris photography and retina scan);
- facial recognition;
- dynamic control techniques (keystrokes, signature traces, voice recognition);
- some techniques are based on visual characters (ear geometry, lip design, shape of pores on the skin, being also attached the analysis of biological traces – blood, saliva, DNA);
- and not in last line, voice recognition technology.

As an example, devices that use biometric security are telephones, computers with their accessories or specialized installations such as building access systems or USB sticks with fingerprint readers, tablets, peripherals etc.

The purpose of using electronic identification means is to gain access to certain online services, for example to bank accounts, health, fiscal, e-Administration and e-Government services.

RFC 6973 (Cooper et al. 2013) defines a *fingerprint* as *"a set of information elements that identify a device or application instance".* The Directive uses the term *lato sensu,* meaning it includes a set of information that can be used to identify a user, user agent or device over time.

According to Art. 3, point 10 of Regulation (EU) no. 910/2014 of the European Parliament and of the Council of 23 July 2014, *electronic signature* means "*data in electronic format, attached to or logically associated with other data in electronic format and used by the signatory to sign"; advanced electronic signature* means *"an electronic signature that meets the requirements set out in article 26 - art. 3, point 11";* and *qualified electronic signature* means "an advanced electronic signature that is created by a qualified electronic signature creation device and that is based on a qualified certificate for electronic signatures - Art. 3, point 12".

Conclusions

The health crisis caused by the SARS-Cov2 virus highlighted the strategic importance of the digitization of public services in Romania. If before the pandemic the digitization of public services could be considered a measure to make the public apparatus more efficient, during it, especially during the period of isolation of the population at home, it showed that digitization is a strategic priority and a national security objective.

Biometric recognition provides better security, greater efficiency and, in many instances, increased user convenience.

As no security system is impenetrable, the one that uses biometrics is not without some vulnerabilities, especially in a world where we are all interconnected.

The efficiency of biometric authentication systems can be strengthened if we use, in addition, a classic authentication method, such as a card or a password.

Data privacy is another issue raised in the debate on the level of security offered by biometric authentication systems, as data and identifiers can be stolen or misused.

From a technical point of view, the disadvantages are related to the fact that these technologies are quite expensive and to the fact that all biometric systems work on the fact that the scanning cannot have a degree of accuracy of 100%. For now, biometric security has proven more useful than passwords ever have been and has begun to be integrated into more and more major platforms and services.

References

Aron, I. 2010. *Biometria, metodă de identificare criminalistică a persoanelor (PhD thesis (abstract). Biometrics, method of forensic identification of persons).* Ministry of Administration and Interior, "Alexandru Ioan Cuza" Police Academy, Faculty of Law, Bucharest.

Authority for the Digitalization of Romania (ADR). 2023. *Electronic identity. Available at* https://www.adr.gov.ro/identitatea-electronica/, accessed on 30.01.2023.

Boghirnea, I. 2013. *Teoria generală a dreptului (General Theory of Law).* Craiova: SITECH Publishing House.

Colectiv. 1978. *Dicţionar de filosofie (Philosophy Dictionary).* Bucharest: Politică Publishing House.

Cooper, et al. 2013. *Privacy Considerations for Internet Protocols*. July 2013, https://www.rfc-editor.org/rfc/rfc6973, accessed on 30.01.2023.

EUR-Lex.europa.eu. 2019. "Information from member states." *Official Journal of the European Union* C 309/9. https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52019XC0913(02)&from=EN, accessed on 30.01.2023.

European Commission. 2023. What is personal data? https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_enhttps://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_ro, accessed on 30.01.2023.

Goicovici, J. 2021. *Noaptea, toate pisicile sunt negre: prelucrarea datelor biometrice ale consumatorilor (At night, all cats are black: the processing of consumers' biometric data).* 08.02.2021, available at

https://www.juridice.ro/716070/noaptea-toate-pisicile-sunt-negre-prelucrarea-datelor-biometrice-ale-consumatorilor.html.

Goodner, S. 2023. *Ce sunt biometria? (What are biometrics?),* https://ro.eyewated.com/ce-sunt-biometria/, accessed on 20.03.2023.

Ionescu, L., Sandu D. 2011. *Identificarea criminalistică (Forensic identification).* Bucharest: CH Beck Publishing House.

Nechita, E.-A. 2009. *Criminalistica. Tehnica și tactica criminalistică (Forensics. Forensic technique and tactics).* 2nd Edition. Bucharest: Prouniversitaria Publishing House.

Vâlcu, N.E. 2012. *Drept comunitar instituțional. Curs universitar (Institutional community law. University course).* Revised and Added 3rd Edition. Craiova: SITECH Publishing House.

Regulation (EU) no. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions on the internal market and repealing Directive 1999/93/EC, published in OJ L 257, 28.8.2014

Regulation no. 679 of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and on the repeal of Directive 95/46/EC (General Data Protection Regulation), published in the Official Journal with number 119L from May 4, 2016.