dr Magdalena Tomaszewska-Michalak
Faculty of Political Science and International Studies,
University of Warsaw
ORCID 0000-0001-5441-0396

HANDWRITING AS A BIOMETRIC TRAIT. PART II

Summary
The first part of the article deals with the legal aspects of biometric data processing with a special focus on the biometric signature identifier. In this regard, the author refers to the GDPR, indicating the rules for collecting and using personal data. The second part addresses technical problems that may arise in connection with the processing of biometric data, including errors, related to the operation of biometric systems.

Keywords: biometric technology, handwriting, signature, biometric processing

Introduction

This study is part two of a study entitled *Handwriting as a biometric trait*[1]. The first part addresses issues indicating that writing belongs to behavioral biometric traits and the possibility of using a signature as a biometric identifier. In this paper, however, the focus will be on the legal aspects of biometric data processing, as well as on the problems that may arise in connection with the automatic verification of a person's identity/ identification based on writing[2].

---

1 See "Current Problems of Forensic Science" 2022, vol. XXVI, pp. 423–433.

2 The publication developed under the project No. DOB-SZAFIR/06/A/042/01/2020 entitled "Intelligent System for Identification of Forgery of Biometric Features of Handwriting", financed from NCRD funds, carried out in the Program entitled. "Development of modern, cutting-edge technologies for national security and defense" pk. "SAAFIR" from Competition No. 1/SZAFIR/2020. The project is being implemented from 2021 to 2024 by a consortium consisting of: The Central Forensic Laboratory of the Police, the Institute of Forensic Science of the Polish Forensic Association Ltd. and JAS technologies Ltd.

Legal aspects of biometric data processing

The first issue to consider in the context of the legal feasibility of using biometrics, including signature-based verification/identification, is the general principles of biometric template processing. It is worth noting that the EU legislator has recognized in Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons concerning the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)[3] the distinctiveness of biometric identifiers, distinguishing biometric traits as an additional category of data. This is important because biometric data did not appear either under Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, on the protection of natural persons concerning the processing of personal data and on the free movement of such data[4] preceding GDPR, or under the now-repealed Polish Data Protection Act[5]. The GDPR defines biometric data as "personal data that results from special technical processing, relates to physical, physiological or behavioral characteristics of a natural person, and enables or confirms the unambiguous identification of that person, such as a facial image or fingerprint data" (Article 4(14) of the GDPR). At the same time, biometric data has been included in the catalog of special data, the collection and use of which is possible only in strictly defined situations (Article 9 of the GDPR)[6]. In addition, regarding the data indicated, the GDPR mandates a risk assessment of the processing of such data in terms of the effects of

---

3 Regulation (EU) 2016/679 of the European Parliament and of the Council 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/EC (General Data Protection Regulation), OJ. 2016, L119.

4 Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; OJ. 1995, L281.

5 Law of August 29, 1997 on the protection of personal data, OJ. 1997, no. 133, item 883.

6 Article 9 of the GDPR gives the possibility to process sensitive data only in the indicated situations, namely if:

a) "the data subject has given his or her explicit consent to the processing of such personal data for one or more specific purposes, unless Union or Member State law provides that the data subject may not waive the prohibition referred to in paragraph 1.

b) the processing is necessary for the fulfillment of obligations and the exercise of specific rights by the controller or the data subject in the fields of labor law, social security and social protection, insofar as authorized by Union or Member State law, or by a collective agreement under Member State law providing for adequate safeguards for the fundamental rights and interests of the data subject;

c) the processing is necessary to protect the vital interests of the data subject or another natural person, and the data subject is physically or legally incapable of giving consent;

such action on the rights or freedoms of natural persons (Article 35 GDPR). In a situation where biometric data processing is allowed, the database administrator should follow the principles of biometric template processing: reliability and transparency, purposefulness, and proportionality/adequacy. The principles of reliability and transparency are to process only data that is up-to-date. For some biometric identifiers, including, for example, a signature, it is important to remember that the template must be renewed after a certain time. The rule of fairness is also linked to the burden of maintaining data collection with an information obligation[7], as well as the determination of the time after which the data must be deleted. The principle of purposefulness is that data can be used only for the purposes for which it was collected. In the case of biometric data, this will mean that it cannot be transferred to others, such as for marketing purposes. Such a rule could have the effect of increasing confidence in the use of biometrics in various areas of life. The last rule enshrined in the GDPR is the proportionality rule, which stipulates that

d) processing shall be carried out within the framework of authorized activities carried out in compliance with the relevant safeguards by a foundation, association or other non-profit entity with political, philosophical, religious or trade union purposes, provided that the processing relates only to members or former members of the entity or persons in regular contact with it in connection with its purposes and that the personal data are not disclosed outside the entity without the consent of the data subjects;

e) the processing concerns personal data obviously made public by the data subject;

f) processing is necessary for the establishment, investigation or defense of claims or in the administration of justice by the courts;

g) the processing is necessary for reasons of substantial public interest, on the basis of Union law or Member State law, which are proportionate to the stated purpose, do not prejudice the essence of the right to data protection, and provide for adequate and specific measures to protect the fundamental rights and interests of the data subject;

h) the processing is necessary for the purposes of preventive health or occupational medicine, assessment of the employee's fitness for work, medical diagnosis, provision of health care or social security, treatment or management of health care or social security systems and services under Union or Member State law or in accordance with a contract with the health care professional and subject to the conditions and safeguards referred to in paragraph 3;

i) the processing is necessary for reasons of public interest in the field of public health, such as protection against serious cross-border health threats or ensuring high standards of quality and safety of healthcare and medicinal products or medical devices, on the basis of Union or Member State law, which provides for appropriate specific measures to protect the rights and freedoms of data subjects, in particular professional secrecy;

j) the processing is necessary for archival purposes in the public interest, scientific or historical research, or statistical purposes in accordance with Article 89(1), on the basis of Union or Member State law, which are proportionate to the designated purpose, do not prejudice the essence of the right to data protection, and provide for appropriate, concrete measures to protect the fundamental rights and interests of the data subject."

[7] The obligation to provide information is to inform the person whose data is being processed of this fact, as well as to indicate the way to correct or delete the information collected.

data collection must be relevant to the intended purpose. Consequently, the processing of excessive data will be considered a violation of the described rule. An example illustrating the situation of disproportionality in the case of biometric data was the Supreme Administrative Court's recognition of the processing of biometric identifiers for time control[8]. This is because the Supreme Administrative Court ruled that in this situation the interference with an employee's right to privacy was too far-reaching compared to the benefits of collecting fingerprints in this case. To date, however, there have been no rulings indicating a situation in which verification based on biometric signatures would violate the principle of proportionality. In conclusion, there is currently no legal contraindication to collecting biometric signature templates. However, one should be guided in any situation of processing biometric data by the data protection principles outlined in the regulations.

The lack of prohibitions is currently not matched by the adaptation of the law (in this case, mainly civil) to the possibility of using biometric devices, which are becoming increasingly popular in everyday life. The literature already recognizes this problem, for example, concerning inheritance law in the context of the possibility of using a biometric signature to draft a will[9]. As Katarzyna Sikora points out, the law cannot fail to take into account the increasing digitization, especially when the use of modern technology makes it possible to authenticate the testator more effectively. Therefore, consideration could be given to introducing the possibility of drawing up a will in electronic form, signed using the testator's biometric identifier (e.g., signature). The biometric trait used for authentication can be an additional element in this case to confirm the authenticity of the document. This example merely demonstrates the possibilities inherent in using biometric technology within the public sector as well.

Technological aspects of biometric data processing

In addition to the legal permissibility of biometric data processing, it is also necessary to lean into the technological problems that may arise in connection with the implementation of modern solutions for identifying a person or verifying his identity. This is because it is important to remember that the effectiveness of algorithms is never 100% and that the use of biometric devices involves the risk of error. In terms of biometric technology, there are three types of errors: FER, FAR, and FRR. The former is known

[8] Cf. e.g., Judgment of the Supreme Administrative Court I OSK 249/09.

[9] K. Sikora, *Technologie biometryczne sposobem uwspółcześnienia przepisów o formie testamentu holograficznego*, "Legal Studies. Dissertations and Materials" 2020, no. 2(27), pp. 207–225.

as registration error (FER). *Failure to Enrol Rate* involves the inability to enrol a biometric pattern. This can occur when a person does not have a particular trait (e.g., lack of a hand that prevents fingerprinting) or when the quality of the trait does not allow the creation of a biometric template from it (e.g., diseases that cause atrophy of the fingerprint, and consequently the inability to create a template of sufficient quality to make a registration). Regarding the signature, the error in question may occur in connection with a person's physical handicap (lack of a hand, advanced hand disease that does not allow the person to sign) or lack of ability to sign (for example, in the case of illiteracy). If a system based on biometric signature comparison is implemented, the occurrence of FER, therefore, necessitates the implementation of so-called emergency procedures. These are procedures that allow authentication of a person's identity based on non-biometric characteristics. Implementing emergency procedures is necessary from the point of view of identity comparison monitors, as it gives clear guidelines for behavior in an unusual situation. This is equally beneficial to the system user, as he is not discriminated against due to the inability to collect a biometric ID template from him. It is also important to determine how many registration attempts should be made. Keep in mind that persistent repetition of the pattern registration process can have negative consequences related to a decrease in user confidence in the system. In addition, registering a "compromise" pattern can lead to problems in the future when performing biometric authentication. In a FER situation, it is also worth identifying the reason for the inability to record, as it may only be temporary (e.g., temporary damage to the hand). In this case, too, it is worth implementing emergency procedures and downloading the image of the identifier pattern at a later date.

In the case of biometric algorithms, a high percentage of FER has serious implications, as it may cause a rethinking of the sense of collecting biometric data due to the forced duality of the authentication process. In addition, the main purpose of introducing biometrics-based solutions is to increase the security level of a given system. The consequence, on the other hand, of not being able to register a person is the inability to authenticate at the comparison stage, thus preventing the basic premise behind the implementation of biometric security.

The other two errors that can occur due to the use of biometric technology are: *Failure Rejection Rate* (FRR error), and *Failure Acceptance Rate* (FAR error). Both of the indicated errors already occur at the feature comparison stage, that is when the identifier pattern is in the system. The FRR error is the recognition of a person authorized as unauthorized to access a specific

system. The occurrence of a failure rejection error can be troublesome for the user, and if it occurs frequently, it can lead to a lack of acceptance of the system and user reluctance to use biometric security. In the case of FER, it is necessary to apply emergency procedures, which should clearly define the rules of conduct in the situation of negative verification of a person's identity. These procedures should first and foremost indicate when it should be considered that a negative comparison result is not related to an attempted fraud but represents a system error. Then you need to determine what alternative method of verifying a person's identity should be used in such a case (e.g., using a different biometric trait or showing an identity document). The failure acceptance error is a result of a device malfunction, which, as a result of the comparison, indicates the identity of the biometric trait with the template, while this is not true. FAR is an extremely dangerous error from a system security perspective. This is because inadequate control of the system can result in improper verification going undetected, thus granting privileges to an unauthorized person. Therefore, it is always necessary to monitor the correct operation of the device and be mindful of the possibility of an error by the algorithm.

Problems related to the possibility of using writing as a biometric trait used in the person identification/identity verification process

Each feature to be used in the biometric comparison process should have certain characteristics. These are: prevalence, immutability, uniqueness, downloadability, and acceptability. These properties were described in more detail in the first part of the study *Handwriting as a Biometric Trait*. Here it is only necessary to focus on those elements that seem problematic in the context of creating a biometric signature template. In particular, this will be: uniqueness and immutability of the identifier in the form of a letter (Table 1).

Tab. 1. Characteristics of writing as a biometric trait

Biometric identifier property	Identifier in the form of a letter (signature)
Versatility	Yes
Uniqueness	Partially yes
Immutability	Partially yes
Downloadable	Yes
Acceptability	Yes

Source: M. Tomaszewska-Michalak, *Handwriting as a biometric trait. Part I*, "Current Problems of Forensic Science" 2022, vol. XXVI, p. 427.

Although the literature indicates that writing is characterized by personal individuality[10], many factors can be listed that potentially affect the image of the drawn characters[11]. The first is undoubtedly the frequency of writing. Since writing belongs to behavioral traits, it becomes unique to a person due to the repetition of certain behavior. The more often we make a signature, the more characteristic of its owner are both graphic characteristics and dynamic features (including the speed and time of drafting). The lack of handwriting/signatures may lead to the failure to fully develop the individualizing features of the handwriting image. This does not preclude the possibility of biometric verification of the writer, but it can make the process significantly more difficult. The second problem that can stand in the way of proper signature-based authentication is the use of different signature designs. In this case, the biometric device will not be able to be used. Changes in the appearance of the handwriting image related to a person's age may also be important from the perspective of device dysfunction. This is inherent in the partial variability of the writing image. This is because a biometric device will not be able to correctly compare the signature of a child who is just learning to write with that of an adult whose graphism is already considered to be fully developed. However, it is not only young age that can stand in the way of conducting an effective biometric comparison. The image of an older person's signature may also differ from the pattern that was recorded several years earlier. This may be due, for example, to reduced writing ability or to diseases that manifest themselves most often in the elderly, such as Parkinsonism. Diseases or damage to the hand can also affect the handwriting image. All of the factors indicated above should be taken into account when implementing a biometric system based on signature-based authentication. This is because by realizing the potential problems associated with the use of the identifier in question, appropriate procedures can be put in place to minimize the risk of algorithm malfunction. First of all, the biometric signature template should be renewed after a certain time. If a person customarily uses more than one form of signature, two templates can be created in the system, for example. Such a solution will be convenient for the user and avoid negative identity verification. In addition, given the various scenarios (e.g., illness, hand injury), emergency

[10] Cf. e.g. A. Feluś, *Podpisy – studium z pismoznawstwa*, University of Silesia, Katowice 1987; Z. Czeczot, *Badania identyfikacyjne pisma ręcznego*, Publishing House of the Department of Forensic Science of the Central Committee of the Citizen Militia, Warsaw 1972.

[11] Cf. e.g. M. Całkiewicz, *Kryminalistyczne badania patologicznego pisma ręcznego*, Wydawnictwa Akademickie i Profesjonalne, Warsaw 2009.

procedures should be put in place to verify the person without the need for a signature. Anticipating potential problems associated with biometric authentication based on the signature pattern allows better preparation for abnormal situations, thus maintaining an adequate level of system security even if an alternative procedure to biometric comparison has to be used. User convenience is also of great importance here, which can influence the acceptance of biometric solutions.

Summary

The purpose of the study was to address problematic issues related to the use of biometric technology based on the authentication of a person based on writing, with particular emphasis on the signature. The first part of the paper deals with the legal aspects of biometric data processing. The analysis showed that there are no clear contraindications in the current legislation to implementing security features based on biometric identifiers. There is even a direct reference to biometric traits in some legislation (cf. GDPR), which means that the EU legislator recognizes that biometric devices are becoming more popular in everyday life. At the same time, the sensitivity of the indicated data makes the possibility of processing it subject to certain rules. Noting the existence of biometrics, however, has not prompted the Polish legislature to introduce changes to facilitate the integration of biometric signature-based authentication into civil law activities. However, this does not prevent it from being used in the private sector, especially the financial sector.

The second part of the study dealt with algorithmic errors that can occur in the signature authentication process. It is important to remember that any device can make a mistake, and proper monitoring of the system's performance can allow you to effectively nullify the consequences of its occurrence.

The final part of the study attempts to analyze the problems that are associated with the use of a signature in the process of biometric identity authentication. This is because the proper functioning of a biometric system involves not only overseeing the effective operation of the algorithm but also identifying factors that can affect various stages of the authentication process. Proper diagnosis in this area allows for informed improvements to be made to the biometric system.

This article is the second part of the study *Handwriting as a biometric trait*. Both parts provide a more complete understanding of the problem of using writing as a biometric identifier used in the process of identifying a person or verifying his identity.

Bibliography

Literature

Całkiewicz M., *Kryminalistyczne badania patologicznego pisma ręcznego*, Wydawnictwa Akademickie i Profesjonalne, Warsaw 2009.

Cieśla R., *Współczesne wyzwania wobec badań dokumentów*, University of Wroclaw Publishing House, Wroclaw 2021.

Czajka A., Pacut A., *Biometria podpisu odręcznego*, in: P. Zając, S. Kwaśniowski (eds.), *Automatyczna identyfikacja w systemach logistycznych*, Wroclaw University of Thechnology Publishing House, Wroclaw 2004.

Czeczot Z., *Badania identyfikacyjne pisma ręcznego*, Publishing House of the Department of Forensic Science of the Central Committee of the Citizen Militia, Warsaw 1972.

Feluś A., *Podpisy – studium z pismoznawstwa*, University of Silesia, Katowice 1987.

Goc M., *Badania podpisów w kryminalistycznej ekspertyzie pismoznawczej – wybrane zagadnienia metodyczne*, "Current Problems of Forensic Science" 2009, no. 263.

Mendyk-Krajewska T., *Biometryczne metody sprawdzania tożsamości w nowych zastosowaniach*, "Yearbooks of SGH" 2019, no. 54.

Sikora K., *Technologie biometryczne sposobem uwspółcześnienia przepisów o formie testamentu holograficznego*, "Legal Studies. Dissertations and Materials" 2020, no. 2 (27).

Tomaszewska-Michalak M., *Prawne i kryminalistyczne aspekty wykorzystania technologii biometrycznej w Polsce*, Difin, Warsaw 2015.

Legal sources and case law

Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, on the protection of individuals concerning the processing of personal data and on the free movement of such data, OJ. 1995, L281.

Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons concerning the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), OJ. 2016, L119.

Law of August 29, 1997, on the protection of personal data, Dz.U. 1997, no. 133, item 883.

Judgment I OSK 249/09 of Supreme Administrative Court of Poland.