ELECTRONIC WRITTEN DOCUMENTS AND BIOMETRIC OPTIONS OF THEIR SIGNING – PROBLEM OF EVIDENTIARY RELIABILITY AND PERSONAL DATA PROTECTION

Ján Matejka,* Vojen Güttler**

Abstract: *The development of information society services presumes an effective, legally permitted and, when it comes to evidence, reliable tool enabling electronic communication and the archiving of electronic records and other written documents, in particular, contracts. Electronic written documents form a dominant part of the standard contracting processes today, both in public and private laws – a typical example of this are consumer contracts. The simplicity, speed, ergonomics, and overall efficiency of these contracting tools lead not only to electronic written documents being used more and more often than paper documents but also, among other things, to electronic written documents being used where other (traditional) forms of legal acting, predicated on tangible (paper) record carriers, were used before. Hence, electronic written documents and their new forms of signing penetrate practically in all legal spheres, even in those where traditional documents have never prevailed due to their ponderousness and various functional limitations. For these reasons, it seems appropriate and useful to analyse the importance of the behavioural and biometric methods inseparably associated with the signing of relevant electronic legal acts, as well as deal with related legal problems ensuing from the nature or the essence of use of these non-traditional electronic tools, including the crucial issue of their evidentiary reliability and actual protection in processing the sensitive personal data so generated.*

Keywords: *electronic contracting, electronic signature, evidence-based reliability, GDPR, personal data protection, biometric data, signatories' responsibility*

INTRODUCTION

A highly significant group of the behavioural biometric methods[1] through which the identity or the authentication of a particular person can be determined is, in particular, the analysis of the handwriting and the signature.

The thing is that the current technologies, or, more precisely, their applications, enable a detailed evaluation of not only the resulting static image of handwriting but also the highly sophisticated and detailed process of creating (writing) a signature. We speak about the so-called dynamic signature verification methods evaluating, in real time, the speed of writing a signature, the pen pressure in the individual phases of handwriting, etc. What is also evaluated are the direction and the sequence of writing certain elements, such as

* JUDr. Ján Matejka, Ph.D., Institute of State and Law of the Czech Academy of Sciences, Prague, Czech Republic. The research reported in this article was supported by the Czech Science Foundation (GA ČR) under grant No. 16-26910S Biometric Data and Their Specific Legal Protection.

** JUDr. Vojen Güttler, Institute of State and Law of the Czech Academy of Sciences, Prague, Czech Republic. The research reported in this article was supported by the Czech Science Foundation (GA ČR) under grant No. 16-26910S Biometric Data and Their Specific Legal Protection.

[1] Biometrics, as a field devoted to the observation of living organisms, is divided into two spheres – physical biometrics and behavioural biometrics (also known as behaviometrics). While physical biometrics monitors specific physical attributes of living organisms (for example, in the event of people, voice, fingerprints, palm bloodstream map, face shape or eye cornea), behavioural biometrics focuses on monitoring their behaviour.

striking out, accentuation of certain parts, writing periods, etc. Some people, for example, write diacritics only at the end, while others continuously. Someone underlines or strikes out from left to right, while another the other way around. All this is missing in the static evaluation of the final signature like we all visually evaluate it today in day-to-day practice. Similar to dactyloscopy, two absolutely identical signatures (their graphical images) are understood today as the possible results of forgery or falsification rather than an ideal sameness of the signature and its original specimen, absolutely regardless of the fact that nobody ever provides an absolutely identical signature at all times. From the application analytical perspective, it is possible to discern a certain determinant uniqueness within the meaning of the overall logical, time, grammar or other behaviourally determinant sequence of the individual lines of a pen in its overall context.[2] These technologically relatively new signature verification methods then logically lead to the search for new and promising ways of unambiguously anchoring this specific type of signature at legal and general levels.

A signature at the general legal level represents a summary issue significantly overlapping a number of legal domains, both public and private. While, in the domain of public procedural law, it is an issue that has already been resolved in substantial part[3] or, more precisely, is associated, on a judicature basis, with the use of either handwritten or electronic[4] signature or with the use of fiction signature in acts undertaken through a data box,[5] the public regulation of the processing of dynamic biometric signatures provides numerous yet unsolved legal application and purely security practical problems.

The solution to these problems needs be found, in particular, both in the current practice and the analysis of related provisions of the Czech and European legislations, specifically, in Regulation of the European Parliament and of the Council (EU) No. 910/2014, on electronic identification and trust services for electronic transactions in the internal market ("eIDAS"), in Act No. 297/2016 Coll., on trust services in electronic transactions, as amended ("ETTSA"), and the provisions of Act No. 89/2012 Coll., the Civil Code, as amended ("CC"). With regard to the essence and the meaning of the dynamic verification methods of this type, it is also necessary to responsibly consider the related issue of the further processing of this behavioural personal data generated in the process of creating (writing) a signature both pursuant to the current, soon-to-be-amended, legislation of Act No. 101/2000 Coll., on Personal Data Protection ("PDPA"), and the upcoming legislation drawing from the general Regulation of the European

[2] For more details see, for example, RAK, R., MATYÁŠ, V., ŘÍHA, Z. et al. *Biometrie a identita člověka ve forenzních a komerčních aplikací.* Grada Publishing, a.s., 2008, p. 134.

[3] See, for example, the opinion of the Supreme Court's plenum of 5 January 2017 on the filings made electronically and the delivery of documents electronically issued by the court through public data network (Opinion No. Plsn 1/2015); available online at http://www.nsoud.cz/.

[4] As in the event of signing an electronic document expressing a legal act towards a public signatory or another person in relation to the exercising of their competencies pursuant to Section 6 et seq. of Act No. 297/2016 Coll., on trust services for electronic transactions, as amended.

[5] Pursuant to Section 18 (2) of Act No. 300/2008 Coll., on electronic acts and the authorized conversion of documents, as amended, an act undertaken by an authorized or designated person through a data box shall have the same effects as an act undertaken in writing and signed.

Parliament and of the Council No. 2016/679, on personal data protection ("GDPR"). It is not possible either to set apart the important related issue of the evidentiary reliability of these signatures, in particular, in comparison with the other traditionally used alternatives of electronic or handwritten signatures.

SIGNING OF ELECTRONIC WRITTEN DOCUMENTS (LEGAL ACTS)

Private law is traditionally predicated on relatively unchanging legal principles entailing certain limits for both the legislator and the permissible interpretation application scope of the legislation. These principles undoubtedly include the principle of the directory nature of legislation and the principle of legal certainty, including the related postulates, such as the prohibition of retroactivity, protection of acquired rights, foreseeability of the decision-making, etc. Both these principles are thoroughly reflected in Sections 559-564 of the CC, regulating the forms of legal action, including the so-called electronic legal acts as specific written documents implemented through electronic means, including the requirement for their signature.

In principle, a legal act may take any form, unless written form is required pursuant to the laws (Section 559 of the CC), **in general, in cases when the meaning and the nature of such act so require**. Hence, in this respect, it is possible to differentiate between an informal legal act, the form of which is not legally regulated, and a formal legal act, for which a particular (usually written) form is prescribed, fulfilling, at the same time, a certain warning function. The failure to observe such form may result in both relative[6] and absolute[7] invalidity of a legal act,[8] but not always. The judicial practice usually restricts the consequences of invalidity to cases where the sense and the purpose of the laws so require (NS 29 Cdo 3919/2014).

Where written form is required pursuant to the laws,[9] an act (undertaken in writing) has to be signed by the acting person to be valid. Through a blanket legal rule, the laws refer to **another regulation stipulating the method of electronically signing a written**

[6] In particular, in situations when the statutory requirement for legal form is set only to protect a certain person's interest, i.e. fulfils, in essence, only the warning function for the parties to such act (Section 586 of the CC).

[7] In particular, in situations when the chosen form seems to be contrary to good morals or the laws and evidently breaches the public order (Section 588 of the CC). The absolute invalidity is in place, in particular, when the requirement for the form does not fulfil only the warning function but also the security function to the benefit of third parties or in the public interest – see, for example, the transfer of a real right to real estate property pursuant to Section 560 of the CC), etc.

[8] We speak about an element of a legal act within the meaning of Section 545 of the CC. The prescribed form should be observed in relation to an entire legal act. Nevertheless, the judicature does not exclude that parts of a legal act be undertaken in various forms; compare decision NS 29 Odo 14/2001 or NS 2 Odon 76/97.

[9] The obligation of a written form may be prescribed in the laws or may be pre-agreed between the parties (Section 559 of the CC). Where no written form is prescribed, any form of an electronic act may be taken, even without electronic signature. Nobody can be forced to choose a form or accept it (Section 559 of the CC). Pursuant to the laws of the Czech Republic, no legal act the signature of which requires third-party certification (official certification) can be undertaken through electronic means, not even those legal acts for which the laws stipulate more elements rather than the written form, such as the requirement for a last will being handwritten pursuant to Section 1533 of the CC. For more details see KMENT, V. Nahradí elektronický podpis prostý ten tradiční vlastnoruční? *Advocacy Bulletin*. 2016, No. 12, p. 5.

document in a legal act undertaken through electronic means (Section 561 (1) of the CC). Such law is, in particular, the ETTSA, the so-called adaptation regulation to the eIDAS stated above. In the event of electronic legal acts, the requirement for written form is fulfilled by attaching electronic signature to the content of a legal act within the meaning of the ETTSA.

However, the applicable legislation allows an exception to the stated requirement for signing a written legal act. It ensues from Section 562 (2) of the CC that written form shall be preserved in legal acts undertaken through electronic or other technical means enabling the depiction of the content of a legal act and the identification of the acting person, completely regardless of whether the legal act has been signed or not. It is **a special regulation of electronic written instruments without signatures** (lex specialis[10] in relation to Section 561 (1) of the CC), to which the laws ascribe the legal effects of written documents provided they enable the depiction of an act and the identification of an acting person.[11] **On the one hand, the laws do not expressly require signature for these other forms, but, on the other, stipulate an essentially similar requirement for the acting person's identification, which can be considered as a legal alternative of a signature, the purpose and the main function of which is usually the actual identification. In this respect, it can be stated that this 'identification' requirement can be fulfilled, for example, through a biometric or other similar identifier which *stricto sensu* does not constitute a signature in the legal sense, but meets similar purpose and function.** The stated concept both reflects the parties' autonomous intentions in private law and constitutes a step towards expanding electronic contracting and legal acting.[12]

As already stated above, **the Civil Code stipulates the condition of attaching electronic signature to electronic legal acts** within the meaning of the ETTSA, the only law **stipulating the method of signing such written documents.** The provision of Section 5 et seq. regulates the types of signature based on the signatory or, more precisely, on the public nature of a signature, as well the individual legally admissible types of electronic signature regulated in the eIDAS. It unambiguously ensues from Section 7 of this Act that *"guaranteed electronic signature, recognized electronic signature, or, **possibly, an-***

[10] A similar conclusion is also contained in the commentary literature MELZER, F., TÉGL, P. a kol. *Občanský zákoník. Velký komentář. III. Svazek*. Leges, 2014, p. 637, or, possibly, also ŠVESTKA, J. a kol. *Občanský zákoník. Komentář. Svazek I-VI*. Wolters Kluwer, 2014, p. 1387, or also PETROV, J., VÝTISK, M., BERAN, V. a kol. *Občanský zákoník. Komentář*. C. H. Beck, 2017, p. 597.

[11] Nevertheless, the provision of Section 3026 (1) of the CC, stipulating that, unless the nature of a written document so enables, the provisions of this Act shall apply accordingly even to other written documents regardless of their form, seems problematic in this sense. Hence, the stated provision expressly allows using the analogy of the legal provisions regulating the form of a document even for other forms of written documents, i.e. including electronic written documents and other tests not portable on tangible carriers, etc.

[12] In relation to the foregoing, it is also necessary to mention the related Section 562 (2) of the CC, regulating the so-called presumption of reliability of electronic records stating that records on legal acts in an electronic system shall be considered as reliable if undertaken systematically and gradually and protected against changes. If a record is made in the operation of an enterprise and the other party invokes it to his benefit, it shall be considered as reliable.

other type[13] ***of electronic signature*** *can be used for electronic signing* ***if the electronic document through which a legal act is undertaken is signed in a way other*** *than the one stated in Section 5 or Section 6 (1)*". The so-called *'another type of electronic signature'* within the meaning of this provision is also the basic (common) electronic signature pursuant to the eIDAS, whereby the *'other way'* shall be a legal act within the meaning of the CC, i.e., typically, the signing of private electronic written documents. Therefore, it ensues from the applicable legislation that, in essence, any type of electronic signature pursuant to the eIDAS is sufficient in private relationships to meet the formal elements.

Perusing the relevant provisions of the eIDAS, we can notice that the basic form of electronic signature is defined in Article 3 (10), stipulating that electronic signature shall mean:

– *data in electronic form;*
– *data attached to, or logically associated with, other data in electronic form;*
– *data used by a signatory for signing*

Through a mere analysis of the definition stated above, it can be concluded that the respective defining provision does not per se contain any qualitative requirements towards the identification or determination of a signatory's identity. The only qualitative element is the highly general reference to the common usage of the signatory attaching *'the data used for signing'*, **which, in essence, may be any data in electronic form**. The stated non-restrictive provision obviously meets the principle contained in Article 25 (1) of the eIDAS, pursuant to which electronic signature must not be denied legal effects and must not be rejected as a proof in court or administrative proceedings only because it is electronic or because it does not meet the requirements for qualified[14] electronic signatures[15]. The issue of electronic contracting and the individual elements and functions are discussed in more detail, though with different legal qualification, for example by J. Matejka,[16] R. Polčák,[17] F. Korbel with F. Melzer,[18] K. Čermák,[19] and V. Kment.[20] However, the actual issue of the legal admissibility and, hence, the validity or permission of electronic signature based on the attachment of, in essence, any *'data used for signing'* pursuant to the eIDAS or the procedure as per Section 562 (1) p) of the CC, constituting a special regulation of valid written documents without a signature (in contrast with

[13] The Act considers as exceptions in this sense only the acting of the state or, more precisely, its organizational units and other public signatories pursuant to Section 5 (1) of the ETTSA, which requires qualified electronic signature within the meaning of eIDAS.

[14] Qualified electronic signature has legal effects identical to handwriting (Article 25 (2) of the eIDAS).

[15] Even the reasoning of the eIDAS (Article 48 et seq.) stipulates that, to ensure the mutual recognition of electronic signatures, a high level of security is necessary, but electronic signatures of a lower security level should also be accepted in special cases, for example, in the context of Decision of the Commission 2009/767/EC 10).

[16] J. MATEJKA, J. Úprava elektronického podpisu v právním řádu ČR. *Právník*. 2001, Vol. 140, No. 6, p. 582–611.

[17] R. POLČÁK, R. Elektronické právní jednání – změny, problémy a nové možnosti v zákoně č. 89/2012 Sb. *Advocacy Bulletin*. 2013, No. 10, pp. 34–40, p. 36, or also POLČÁK, R. Praxe elektronických dokumentů, *Advocacy Bulletin*. 2011, No. 7–8, p. 55.

[18] KORBEL, F., MELZER, F. Písemnost, elektronický a biometrický podpis v elektronickém právním jednání, *Advocacy Bulletin*. 2014, No. 12, pp. 31–36, p. 32.

[19] ČERMÁK, K. jr. Elektronický podpis: pohled soukromoprávní. *Advocacy Bulletin*. 2002, No. 11, pp. 64–77.

[20] KMENT, V. Nahradí elektronický *podpis* prostý ten tradiční vlastnoruční? *Advocacy Bulletin*. 2016, No. 12, p. 5.

the general regulation of written documents with signature in Section 561 (1) first and third sentences of the CC), does not and cannot even come as a surprise since similar conclusions were already deduced[21] in the past in relation to the previous legislation.

SIGNING OF ELECTRONIC WRITTEN DOCUMENTS THROUGH PHYSICAL OR BEHAVIOURAL BIOMETRICS DATA

As already stated above, the valid legislation allows an electronic document (i.e. a legal act in private electronic documents) being signed electronically, for example, by affixing, in essence, any *'data used for signing'* to it. In terms of their significance, possible use and legal force, electronic written documents have a position equivalent to other traditional forms, including paper ones (typically paper record carriers).[22] **Hence, this equivalency of paper and electronic forms has much broader impacts in many respects than just on written documents since, from the legal perspective, it relates not only to writing but also to image, sound or other records;** therefore, these documents are limited, in particular, by the existing technical possibilities of recording on paper rather than by legal limitations of their use.[23]

In the traditional (i.e. in particular, paper) form, a signature usually represents a handwritten name (autograph). Hence, it concerns a handwritten expression through characters amounting to letters. The specific nature of a signature is determined, primarily, by the legal usage, whereby the validity of a written legal act is not conditional upon the completeness (i.e. for example, the statement of full name and surname) or legibility of the signature; however, the acting person's identity needs to be obvious in the overall context. Regarding the place of the signature, the essence of a signature is something that 'constitutes a written deed', meaning that it typically 'completes' or 'confirms' the text or the act to which it relates.[24]

One of the consequences of the stated equivalency of **the paper and electronic forms is the fact that not only a written electronic document but also an electronic written document containing, for example, a visual, audio or other similar record[25] may be signed electronically**. An electronic written document may be signed electron-

[21] For more details see, for example, MATEJKA, J. Úprava elektronického podpisu v právním řádu ČR. *Právník*. 2001, Vol. 140, No. 6, pp. 582–611.

[22] The stated principle is indirectly accentuated, among other things, in Section 2 e) of Act No. 499/2004 Coll., on Archival Science and the Filing Service, pursuant to which a document is any written, visual, audio or other recorded information, whether analogue or digital.

[23] The CC does not, in essence, prefer deeds to other forms of written documents. For example, pursuant to Section 3026 (1), all provisions of the CC pertaining to deeds shall also apply to other written documents regardless of their form, unless the nature of the written documents excludes it.

[24] However, even here it is necessary to consider the tradition. For example, in lawyer-signed documents, the lawyer, as a representative, is signed on the first page of a written document (usually in the identification of a party to the procedure with a supplement that the lawyer is his legal representative).

[25] However, for a document to be considered as written, the content of a legal act needs to be depicted in a way constituting a graphical depiction of a group of characters representing writing. For more details see HULMÁK, M. Commentary on Section 40. In: ŠVESTKA, J., SPÁČIL, J., ŠKÁROVÁ, M., HULMÁK, M. et al. *Občanský zákoník. Komentář*. 2nd edition. Prague: C. H. Beck, 2009, p. 369.

ically pursuant to the eIDAS (see above), for example, through the so-called biometric forms of electronic signature constituting *'data used for signing'*. These biometric forms of signature conform not only to the characteristics of the (plain) electronic signature but also to the general definition of a signature, i.e. its traditional form (see above). In the event of biometric options, regardless of whether they concern dynamic biometric signature or other behavioural forms of signature, similar problems as in the electronic signature arise, in particular, when it comes to the attachment of this signature to an electronic written document. For this reason, requirements identical to those imposed on electronic signatures need to apply to this signature as well. In this respect, it is possible to admit that the mere attachment of a scanned signature, the entry of a specific password or code, or the fulfilment of another authentication procedure may constitute the signature of a written document in the form of (plain) electronic signature pursuant to Section 561 (1) third sentence of the Civil Code. The same applies to **recorded voice attached to an electronic written document, the content of which is the confirmation of the respective legal act.**[26]

The electronic forms of signing in the form of attachment of biometric (physical or behavioural) data to electronic written documents (legal acts) not only follow the traditional (i.e. in particular, graphical) form of signature but also constitute a seemingly ideal interconnection of the traditional and the electronic concepts of signing within the meaning of the applicable legislation. Hence, in many respects, the allowed use of these modern forms of signing not only strengthens the position of electronic written documents and their legal use but also undoubtedly leads to the standardization of new practical procedures combining biometric methods (as an ideal authentication or quasi-identification tool) and cryptologic methods (qualified electronic signature).

EVIDENTIARY RELIABILITY OF ELECTRONIC WRITTEN DOCUMENTS INCL. THEIR BIOMETRIC SIGNATURES

From the evidentiary procedural perspective, all forms of electronic written documents (including their signatures) can be considered as equal or equivalent (see above) and, thus, can serve as proofs within the meaning of all Czech procedural laws; however, the laws contain a relatively non-trivial procedure regulating the evidentiary reliability of certain related evidence, in particular, in Sections 565[27] and 566 of the CC[28] where the legislator

[26] However, with regard to Section 562 (1), the practical difference between both situations is minimal since, in electronic form, it is possible to validly undertake a written act without a signature if the used means allow depicting the content of the act and identifying the acting person.

[27] It is up to the one seeking the validity of a private document to prove its genuineness and correctness. If a private document is used against a person who has obviously signed it or his heir or against a person who has acquired assets in the transformation of a legal entity as its legal successor, the genuineness and correctness of the document shall be considered as recognized.

[28] (1) If a private document is not signed, it is up to the one who has used it to prove that it comes from the person about whom he claims it. (2) It shall be assumed that written documents relating to legal facts associated with the common operation of an enterprise prove, if the other party is seeking their validity to his benefit, what is contained in them and that they were issued on the date stated in them, which shall also apply if they have not been signed.

relatively redundantly expressly speaks about a 'private document' rather than 'a private written document'. Nevertheless, with regard to the conclusions of the legal doctrine[29] and the provisions of Section 3026 (1) of the CC,[30] it is possible to arrive at the conclusion that these provisions apply also to private (electronic) written documents.

The stated provisions are relatively crucial in terms of the actual evidentiary reliability of the biometric forms of a signature, including dynamic biometric signature (see above). Considering that this technology of signing must, in some of its phases, gather the signatory's biometric characteristics (regardless of whether legitimately with the signatory's consent or illegitimately under a false pretext), it is not possible to exclude that this data may be misused in the future to develop other derivatives of the original signature. The thing is that biometric signatures exist 'per se' and are independent of the signed documents. Hence, on principle, it is not possible to exclude that they be removed from original electronic written documents and attached to other written documents.

For this reason, to practically use biometric signatures for signing electronic documents, we need some 'sufficiently reliable and firm' relation between a signature and a document that could not be severed and that immediately reveals any manipulation (alteration of the document or the actual signature). However, with regard to the development of neuron networks (artificial intelligence), these procedures are more and more non-trivial, but it is still possible to interconnect them with asymmetric cryptography methods (see below), where the obtained biometric data (dynamic biometric signature) is attached to the document to be signed, and, subsequently, the resulting signature is generated by the system in the form of qualified electronic signature.[31]

However, the stated procedure imposes major requirements on the quality and the functional properties of the relevant systems, adding the need for a sophisticated evaluation of biometric data (against the signature specimen) and, hence, the possible jeopardy of the entire system (the possibility of misuse of the signature specimen database), etc. These aspects have not yet been satisfactorily resolved.

However, from another perspective, it is, in particular, the provision of Section 562 (2) second sentence of the CC,[32] containing a clear presumption of evidentiary reliability (refutable legal conjecture) which reflects on modern approaches to the essence of electronic written documents and, concurrently, considerably facilitates the use of typical and more and more frequent forms of electronic contracting,[33] that can be considered as cru-

[29] See, for example, MATEJKA, J. Úprava elektronického podpisu v právním řádu ČR. *Právník*. 2001, Vol. 140, No. 6, pp. 582–611.

[30] If the nature of a written document does not exclude so, the provisions of this Code pertaining to documents shall apply accordingly to other written documents regardless of their form.

[31] For more details, see PETERKA, J. Elektronický podpis na rozcestí. In: *LUPA* [online]. 6. 6. 2011 [cit. 2011-12-28]. Available at: <http://www.lupa.cz/clanky/elektronicky-podpis-na-rozcesti>.

[32] It shall be assumed that records on legal acts in electronic system are reliable if made systematically and consecutively and protected from alterations. If a record is made in the operation of an enterprise and the other party invokes it to his benefit, it shall be considered as reliable.

[33] For more details, see, for example, MASON, S. *Electronic Signatures in Law*. Cambridge: Cambridge University Press, 2012, p. 259.

cial in terms of evidentiary reliability. This direction chosen by the Czech legislator is more convenient in many respects than reliance on various attempts aimed at preventing the known evidentiary reliability of electronic written documents by attaching other authentication mechanisms (usually, for example, other qualified signatures, marks and stamps) to a document. **However, the trend of the electronic processing of documents unambiguously leads to their evidentiary reliability being established through the qualified method and procedure through which they have been developed or are saved on a long-time basis**[34] **rather than through the individual electronic signatures in them. Hence, it is the electronic system, or, more precisely, its functional properties, architecture and design, which provides guarantees through which the genuineness or the authenticity of the electronic written documents processed in it can be presumed or, subsequently, proven.** If the one invoking a written document proves that the system in which the written document is saved has the stated parameters, the burden of proof passes to the one claiming its falseness.

DYNAMIC BIOMETRIC SIGNATURE & PERSONAL DATA PROTECTION

Comparing the traditional methods of signing electronic written documents through qualified signatures (i.e. based on asymmetric cryptography methods) with physical or behavioural biometrics methods, we must necessarily conclude on highly significant differences. The main difference is, in particular, the fact that, in the event of biometric methods, signature data cannot be invalidated or otherwise revoked. If the data is compromised for developing electronic signatures (private key), it can be easily and quickly invalidated by means of standard and well-known tools and a new key can be generated if needed. If a person's basic biometric characteristics are obtained illegitimately, whether by fraud in the way as described above or by theft from the referential database of biometric samples, it is very difficult to prevent their misuse. The affected user (if he even learns about it) may try to knowingly change his signature specimen, which, however, would contradict, to a certain extent, the basic idea of collection and comparison of a person's unconscious biometric characteristics and would undoubtedly involve a lengthy and uneasy phase of determining and getting used to another signature.

Therefore, biometric signature needs to be viewed as highly sensitive personal data within the meaning of both the current legislation (Personal Data Protection Act) and the GDPR, which pays special attention to biometric data. The GDPR defines and classifies biometric data as the so-called special category of personal data to which the special rules stipulated in Article 9 of the GDPR apply. Pursuant to the GDPR, data is covered by the definition of biometric data only *'when processed through a specific*

[34] For more details see POLČÁK, R. Elektronické právní jednání: změny, problémy a nové možnosti v zákoně č. 89/2012 Sb. *Advocacy Bulletin*. 2013, No. 10, pp. 34–40. Also available at http://www.bulletin-advokacie.cz/elektronicke-pravni-jednani-zmeny-problemy-a-nove-moznosti-v-zakone-c.-892012-sb, or, possibly, also VOLAREVIC, M., STRASBERGER, V., PACELAT, E. A philosophy of the electronic document management. *Proceedings of the 22nd International Conference on Information Technology Interfaces*. 2000, p. 141.

technical means allowing the unique identification or authentication of a natural person' (recital 51 of the GDPR).[35]

Paragraph 1 of Article 9 of the GDPR provides a general clause on the prohibition of processing biometric data for the purpose of the unique identification of a natural person; however, it also stipulates an exception to this prohibition (see below). In this respect, it is interesting that it leaves out the term 'authentication' as it is used in the stated recital 51. Authentication can be understood as the confirmation of identity (one-to-one comparison) against its determination (one-to-many comparison). Hence, it can be stated that GDPR excludes from this clause the prohibition of processing biometric data, such as the verification of a phone owner's identity through a fingerprint reader, since in this type of processing a phone compares the already saved template with the submitted identifier (fingerprint) and only ascertains whether a person is identical. Therefore, the system alone does not search any fingerprints database and does not identify persons through their fingerprints. It is, however, necessary to take into account the actual definition of biometric data pursuant to Article 4 (14) stipulating that biometric data 'allows or confirms the unique identification', whereby Article 9 does not stipulate the method of achieving the unique identification. Hence, although, with regard to the technical terms, Article 9 (1) may not be completely clear, it applies to both cases, i.e. to both authentication and identification.

Although the processing of biometric data is generally prohibited, Article 9 (2) of the GDPR provides ten exceptions to this prohibition. Pursuant to Article 9 (2) a) of the GDPR, biometric data can be processed if *"**the data subject has given explicit consent** to the processing of those personal data for one or more specified purposes, except where Union or Member State law provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject*". The conditions of the granting of consent are then stipulated in Article 7 of the GDPR and the recitals.[36] Another related case when an administrator can process biometric data for the purposes of the unique identification is a case when **the processing is necessary for *"the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity"*** [Article 9 (2) f)].

In this respect, it is worth reminding that both co-authors of this text are aware of the individual parts of their text often touching both private and public laws. Such situation may sometimes evoke an impression of confusion of these two spheres. However, it is not possible to ignore that the relevant constitutional judicature itself has stated, in the form of an award of the plenum of the Constitutional Court of the Czech Republic, that the legislation of the Czech Republic is, on the one hand, predicated on the dualism of public and private laws, but, on the other, public and private laws are not separated by the 'Chi-

[35] Biometric data is characterised as data that can be relatively easily read from a person's body and recorded, for example, in a photo, video or voice record. However, this data constitutes the so-called 'raw data', i.e. not yet processed data, and is not per se considered as biometric. Only after it is processed, biometric data, the so-called template, is developed within the meaning of the GDPR. Special processing rules then apply to this type of personal data.

[36] The special conditions relating to children's consent are stipulated in Article 8. The recitals relating to the granting of consent are recitals Nos. 32, 33, 38, 40, 42, 43, 50, 51, 65, 68, 71, 111, 112, 155, 161 and 171.

nese wall'. Hence, the elements of public and private laws more and more frequently and narrowly overlap, combine and intensively influence each other[37] and it is necessary to count on this situation even in the future.

Therefore, the normative basis of the solution should be, in particular, the better application and strengthening of the principle of proportionality, including the appropriate comparison of the protection of the fundamental right to private life, on the one side, and the protection of public interest and third-party rights through the collection, processing and saving of biometric data, on the other. The special legal protection of biometric data and, in contrast, the protection, in particular, of the fundamental right to private life (and to the related fundamental rights) are usually interconnected and can hardly be examined separate from each other.

The actual application of the principle of proportionality should draw from the principle that biometric data can be collected, processed and saved only for such purposes a reasonable person considers as appropriate and necessary under specific circumstances. This can be identified as a reasonableness and appropriateness test of its kind, which should be predicated on four criteria following or associated with the constitutional test of proportionality (compare above). According to these criteria, prior to collecting or processing biometric data, it should be examined and confirmed that the collection, administration and processing of biometric data of individuals is necessary to achieve the defined goal or need and that it is the most efficient method of achieving the given goal or need, that the loss of privacy associated with a particular method of processing biometric data is proportional (certain proportionality of the intervention in privacy in comparison with the benefit obtained through such processing of biometric data is ensured), and that there is no other suitable method of achieving the set goal that would constitute a smaller intervention in the affected individuals' privacy.[38] It is, however, necessary to strengthen the guarantees against the misuse of biometric data. In this respect, it is possible to rely, among other things, on the judicature of the European Court of Human Rights. In the case Gardel vs. France, judgment of 17 December 2009, App. 16428/05[39], the court held that security guarantees should ensure that biometric data was (in relation to the purpose for which it was stored) relevant rather than excessive for a period not longer than as required by the given purpose and that other adequate guarantees were adopted against its misuse.[40]

In other words, the personal data protection legislation (including the GDPR) requires that electronic documents are signed based on biometrics in compliance with its principles, both within the meaning of sufficient legal and technological guarantees against misuse and the existence of the legal title stated above. Hence, dynamic biometric signature

[37] Compare the award of 10 January 2001, file number Pl.US 33/2000.

[38] Compare, for example, the Parliamentary Institute: Biometrics Legislation. Answer to Question, July 2014, pp. 6 and 7 – Canada, Personal Information Protection and Electronic Documents Act, S. C., 2000, c. 5.

[39] RAINEY, B., WICKS, E., OVEY, C. *The European Convention on Human Rights*. 6th edition. Oxford: Oxford University Press, 2014, p. 378.

[40] For more details, see GUTTLER, V., MATEJKA, J. K otázkám některych základních lidskych práv a svobod v souvislosti s právní ochranou biometrickych údajů. *Právník*. 2016, Vol. 155, No. 12, p. 1055.

needs to be viewed as sensitive personal data, whereby in the cases of its further automated processing (see the system above), it is necessary to proceed in compliance with Section 9 of the PDPA. The only legal title based on which such processing is generally implementable is the express and informed consent of each data subject pursuant to Section 9 a) of the PDPA (Article 9 of the PDPA), which an administrator must be able to prove throughout the processing. Hence, the data subject must be duly informed about the processing of his sensitive data and the administrator has to fulfil other obligations relating to the processing of both personal and sensitive data pursuant to the PDPA or the GDPR. Increased attention needs to be paid, in particular, to the fulfilment of the information and notification duty and the safeguarding of biometric data.[41] With regard to the current development and new trends, it needs to be stated that the personal data protection rules stated above will apply accordingly even to other technologies that process biometric data enabling data subjects' identification and authentication.[42]

FINAL REMARKS & SUMMARY

The crucial condition of functioning of the current legislation is, in particular, the fact that the law is able to flexibly and, particularly, efficiently react to the developed use of information and communication technologies. This prerequisite should constitute a completely natural and logical development in all legal domains, in particular, where there is no objective reason for public or mandatory legislation. This is undoubtedly the case even in the sphere of private law, which has recently been extensively re-codified. It is apt to question its efficiency, including the formal and material requirements imposed both on legal forms (written documents) and in relation to the evidentiary or other similar application problems.

As ensues from the analysis above, the solution to these problems needs to be found in both the application practice and the analysis of related provisions of the Czech and European legislations, specifically, the eIDAS, the GDPR and the related Czech legislation, including the Civil Code, the Trust Services Act, the Personal Data Protection Act, and others. In relation to the conclusions made above, it is necessary to deduce that the current legislation does not contain per se any qualitative requirements for a signatory's identification; the only qualitative element is the highly general reference to the signatory's per-

[41] For completeness, it needs to be added that, if, for example, one-way hashing is used in signing based on biometrics, i.e. a certain numerical detail whose reverse reconstruction to biometric data (sample) is not possible is generated, this detail can no longer be considered as biometric and the use of such system may be admissible in certain cases even without a data subject's consent if the administrator's obligations pursuant to Section 5 (1) and some of the conditions of Section 5 (2) a), b) or e) of the PDPA are met since no sensitive data is stored. For more details, see, for example, Opinion No. 1/2017 of the Office for Personal Data Protection – Biometric Identification or Authentication of Employees. In: *The Office for Personal Data Protection* [online]. 8. 6. 2017 [2017]. Available at: <https://www.uoou.cz/stanovisko-c-1-2017-biometricka-identifikace-nebo-autentizace-zamestnancu/d-23849>.

[42] Opinion No. 2/2014 of the Office for Personal Data Protection – Dynamic Biometric Signature pursuant to Personal Data Protection Act. In: *The Office for Personal Data Protection* [online]. 18. 7. 2014 [2017]. Available at: <https://www.uoou.cz/stanovisko-c-2-2014-dynamicky-biometricky-podpis-z-pohledu-zakona-o-ochrane-osobnich-udaju/d-11298>.

se habit of attaching *'data used for signing'*, which, in essence, may be any data in electronic form. Hence, this relatively liberal approach of the legislator not only fulfils the principle ensuing from the eIDAS but also confirms the traditional respect for the parties' autonomous will as an irreplaceable value for private law parties. Electronic signature, regardless of whether it is based on the methods of physical or behavioural biometrics, is not, therefore, denied legal effects and is not rejected as a proof in court proceedings.

For the communication through these modern forms to be efficient, the forms need to thoroughly draw from time-proven and established private law principles. The electronic forms of signing in the form of attachment of biometric (physical or behavioural) data to electronic written documents (through a legal act) not only thoroughly follow the traditional (i.e. in particular, graphical) concept of signature but also constitute a seemingly ideal interconnection of traditional and electronic concepts of signing aimed at the desirable natural development of law. Hence, the possible use of these modern forms of signing strengthens in many respects the position of electronic written documents and their legal use and undoubtedly leads to the standardization of new practical procedures combining biometric methods (as an ideal authentication or quasi-identification tool) and cryptologic methods (qualified electronic signature).

Despite the current liberal concept of this private-law matter, reflected in the CC, even the relatively essential limitations ensuing from personal data protection laws, stipulating that the signing of electronic documents in the simultaneous use of biometric methods (physical and behavioural biometrics) has to be implemented in compliance with all principles of personal data protection, need to be respected. For these reasons, it is also necessary to insist on the thorough application of all related legal and technological guarantees against the misuse of this sensitive data and on the simultaneous existence of a clear legal title (informed consent); all this with regard to the legal framework of public legislation and human rights where the protection of the fundamental right to human dignity, i.e. the right to the fulfilment of which practically almost all other human rights directly or indirectly lead, necessarily plays a leading role.[43]

[43] For more details of the issue of human rights with regard to biometrics see GUTTLER, V., MATEJKA, J. K otázkám některých základních lidských práv a svobod v souvislosti s právní ochranou biometrických údajů. *Právník*. 2016, Vol. 155, No. 12, p. 1055.