DOI 10.5817/MUJLT2018-2-3

ONLINE BEHAVIOR RECOGNITION: CAN WE CONSIDER IT BIOMETRIC DATA UNDER GDPR?*

by

ALŽBĚTA KRAUSOVÁ**

Our everyday use of electronic devices and search for various contents online provides valuable insights into our functioning and preferences. Companies usually extract and analyze this data in order to predict our future behavior and to tailor their marketing accordingly. In terms of the General Data Protection Regulation such practice is called profiling and is subject to specific rules. However, the behavior analysis can be used also for unique identification or verification of identity of a person. Therefore, this paper claims that under certain conditions data about online behavior of an individual fall into the category of biometric data within the meaning defined by the GDPR. Moreover, this paper claims that profiling of a person can not only be done upon existing biometric data as biometric profiling but it can also lead to creation of new biometric data by constituting a new biometric template. This claim is based both on legal interpretation of the concepts of biometric data, unique identification, and profiling as well as analysis of existing technologies. This article also explains under which conditions online behavior can be considered biometric data under the GDPR, at which point profiling results in creation of new biometric data and what are the consequences for a controller and data subjects.

KEY WORDS

Behavior Analysis, Behavior-based Tracking, Behavioral Biometrics, Biometric Data, General Data Protection Regulation, Personal Data, Privacy, Profiling, Unique Identification

* This paper was supported by the Czech Science Foundation (GA ČR) under grant No. 16-26910S Biometric Data and Their Specific Legal Protection.

** alzbeta.krausova@ilaw.cas.cz, Head of CICeRo – Center for Innovations and Cyberlaw Research, Institute of State and Law of the Czech Academy of Sciences, Czech Republic (www.cicero.ilaw.cas.cz).

1. INTRODUCTION

According to Eurostat, in 2017 92 % of European citizens aged 16 to 24 years, 81 % of European citizens aged 25 to 54 years, and 57 % of European citizens aged 55 to 64 years use the Internet on a daily basis.[1] Their activity leaves traces about their online behavior. Identity of these individuals can be verified[2] or determined with help of cookies, i.e. pieces of data stored in a device that provides information to servers with which a device is communicating.[3] Determination and verification of users' identities with help of cookies is called explicit tracking and it relies on the cooperation of either users or their web browsers.[4] However, Internet users can be identified also solely based on their online behavior with behavior-based tracking techniques that do not need cookies or any other explicit identifiers.[5] Such identification happens unobtrusively and, in principle, without the knowledge of people whose behavior is being monitored. This technique exploits methods of pattern recognition and applies them either on web surfing behavior, activity of applications installed on a device, or environmental peculiarities.[6] With regard to its purpose, behavior-based tracking partly corresponds to the definition of behavioral biometrics that seeks to

> *"quantify behavioral traits exhibited by users and use resulting feature profiles to successfully verify identity".*[7]

---

1 Eurostat. (2017) *Individuals – frequency of internet use [isoc_ci_ifp_fu]*. [online] European Commission. Available from: https://ec.europa.eu/eurostat/web/products-datasets/-/isoc_ci_ifp_fu [Accessed 29 August 2018].

2 See Recital 25 of ePrivacy directive. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). *Official Journal of the European Union* (2002/L 201/45) 31 July. Available from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML [Accessed 1 November 2017].

3 European Commission. (2016) *Cookies*. [online] European Commission. Available from: http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm [Accessed 22 December 2017].

4 Banse, C., Herrman, D. and Federrath, H. (2012) Tracking Users on the Internet with Behavioral Patterns: Evaluation of its Practical Feasibility. In: Gritzalis, D., Furnell, S. and Theoharidou, M. (eds.) *27th IFIP TC 11 Information Security and Privacy Conference, SEC 2012*, Heraklion, Crete, 4–6 June. Berlin: Springer, p. 235. Available from: https://link.springer.com/chapter/10.1007/978-3-642-30436-1_20 [Accessed 24 November 2017].

5 Op. cit., pp. 235 and 246.

6 Op. cit., p. 242.

7 Yampolskiy, R. V. and Govindaraju, V. (2010) Taxonomy of Behavioral Biometrics. In: Wang, L. and Geng, X. (eds.) *Behavioral Biometrics for Human Identification: Intelligent Applications*. [online] IGI Global, p. 2. Available from: https://www.researchgate.net/publication/254217766_Taxonomy_of_Behavioural_Biometrics [Accessed 15 September 2017].

With regard to the techniques used, behavior-based tracking can also partly correspond to the definition of profiling within the meaning of the EU General Data Protection Regulation[8] (GDPR) as certain aspects relating to a natural person are being analyzed and evaluated in order to establish profiles for this type of tracking.[9] Both biometric data as well as profiling are concepts that have been researched in law substantially due to their potential to seriously infringe privacy of individuals.

From a legal point of view, biometric data is a specific type of personal data that is *"directly linked to an individual"*[10] as it refers to her biological or behavioral characteristics. Biometric data that allow or confirm unique identification of an individual is recognized by the General Data Protection Regulation as a special category of personal data under Art. 9. Due to their potential to significantly increase vulnerability of individuals, processing of special categories of personal data is subject to stricter rules and prohibited in general.

In order to assure the appropriate level of protection of individuals with regard to their personal data, it is legitimate to ask whether profiles set up based on behavior-tracking fulfill the definition of biometric data under the General Data Protection Regulation and, thus, whether service providers who monitor web requests of users and create users' profiles leading to their identification need to comply with specific obligations such as gaining an explicit consent with this practice, appointing a data protection officer, or carrying out a data protection impact assessment. Until now, the literature has dealt only with the question of biometric profiling that aims to extract additional information from existing biometric data and

---

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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) (Text with EEA relevance). *Official Journal of the European Union* (2016/L 119/1) 4 May. Available from: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679 [Accessed 1 November 2017].

[9] Technical papers in the field specifically use the term "profile". See for instance Gu, X., Yang, M., Shi, C., Ling, Z. and Luo, J. (2016) A novel attack to track users based on the behavior patterns. *Concurrency and Computation Practice and Experience*, 29(6). Available from: https://onlinelibrary-wiley-com.ezproxy.techlib.cz/doi/full/10.1002/cpe.3891 [Accessed 24 July 2018]; or Herrmann, D, Banse, C. and Federrath, H. (2013) Behavior-based tracking: Exploiting characteristic patterns in DNS traffic. *Computers & Security*, 39 Part A. Available from: https://www-sciencedirect-com.ezproxy.techlib.cz/science/article/pii/S0167404813000576 [Accessed 24 July 2018].

[10] Article 29 – Data Protection Working Party. (2012) *Opinion 3/2012 on developments in biometric technologies*. 00720/12/EN WP 193. Brussels: Directorate C of the European Commission. Available from: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf [Accessed 20 October 2017].

with *"enriching online profiling data gathered for e-commerce purposes"* with biometric characteristics for instance in order to assess emotional states of a human.[11] However, a possibility of constituting a biometric profile from data gathered for the purpose of profiling based on online behavioral data needs to be discussed as processing this type of data has serious legal consequences for operation of businesses processing these kinds of data. In this regard, the relationship between biometric templates and profiles arising from profiling that can be used for identification of a person also needs to be clarified.

This paper claims that under certain conditions data about online behavior of an individual fall into the category of biometric data within the meaning defined by the GDPR. Moreover, this paper claims that profiling of a person can not only be done upon existing biometric data as biometric profiling but it can also lead to creation of new biometric data by constituting a new biometric template. This claim is based both on legal interpretation of the concepts of biometric data, unique identification, and profiling as well as analysis of existing technologies. This article also explains under which conditions online behavior can be considered biometric data under the GDPR, at which point profiling results in creation of new biometric data and what are the consequences for a controller and data subjects.

2. BIOMETRIC DATA UNDER THE GDPR

GDPR defines biometric data in Art. 4 point 14) as

> *"personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data."*[12]

The term behavioral characteristic is not defined in the GDPR. Behavioral-based biometric data are considered dynamic while still having general characteristics of being universal to all people, unique for each

[11] Kindt, E. (2008) Need for Legal Analysis of Biometric Profiling. In: Hildebrandt, M. and Gutwirth, S. (eds.) *Profiling the European Citizen. Cross-Disciplinary Perspectives*. Dordrecht: Springer.

[12] Op. cit.

person, and permanent.[13] According to Article 29 Data Protection Working Party (A29 WP), an advisory body set up by EU Data Protection Directive,[14] that was replaced by European Data Protection Board but whose opinions stay valid, typical behavioral biometric data

> *"include hand-written signature verification, keystroke analysis, gait analysis, way of walking or moving, patterns indicating some subconscious thinking like telling a lie, etc."*[15]

As this definition refers to patterns of thinking and moving that are then manifested and recorded in an objectively perceivable manner, online behavior of a person perceivable through her specific usage of devices or contents searching patterns should also fall under the definition of behavioral data if it serves as a means for unique identification.

Unique identification is the key term of the definition that determines whether behavioral data will fall in the category of biometrics. The term unique identification is used only at two places in the GDPR – in the very definition of biometric data in Art. 4 point 14) and in the Recital 51. However, the GDPR does not provide any explanation as to the meaning of unique identification.

From a semantic point of view, "unique identification" can refer to recognizing someone as being the one and only person.[16] According to A29 WP, however, this term is relative as it

---

[13] Article 29 – Data Protection Working Party. (2003) *Working document on biometrics*. 12168/02/EN WP 80. Brussels: Directorate E of the European Commission, p. 3. Available from: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp80_en.pdf [Accessed 15 November 2017].

[14] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Union* (1995/L 281/38) 23 November. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046 [Accessed 1 November 2017].

[15] Article 29 – Data Protection Working Party. (2012) *Opinion 3/2012 on developments in biometric technologies*. 00720/12/EN WP 193. Brussels: Directorate C of the European Commission, p. 4. Available from: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf [Accessed 20 October 2017].

[16] According to a dictionary, the term "to identify" means *"to recognize or establish as being a particular person or thing"*, while "unique" can be understood as *"existing as the only one or as the sole example; single; solitary in type or characteristics"*. See (1996) *Webster's Encyclopedic Unabridged Dictionary of the English Language*. New York: Random House, pp. 950 and 2074.

> *"depends on different factors including the size of the database and the type of biometrics used"*.[17]

Moreover, it is generally known that no type of biometrics is fully reliable. Biometric accuracy differs with regard to the technology used. In order to achieve higher degree of accuracy, dual biometrics is sometimes recommended.[18] Unimodal biometric systems often suffer from inaccurate data caused for instance by noise that occurred during extraction of features, non-universality of extracted features or due to lack of their individuality.[19] Nevertheless, if no biometric system can guarantee unique identification in all cases, it is then questionable what degree of probability would be sufficient to classify a technology as processing biometric data within the meaning of the GDPR. It is questionable whether reliability should be assessed individually in each case taking into account for instance a number of people enrolled in a system or whether a certain type of error rate should be preferred.[20] As the Recital 15 of the GDPR states that

> *"the protection of natural persons should be technologically neutral and should not depend on the techniques used,"*

various biometric technologies should not be discriminated with regard to their performance. Rather, effects of a particular technology need to be considered.[21] That is to say that the potential level of uniqueness in a biometric system should not *per se* exclude a less reliable system such as one based on behavioral biometrics from the definition of a system

---

[17] Article 29 – Data Protection Working Party. (2003) *Working document on biometrics*. 12168/02/EN WP 80. Brussels: Directorate E of the European Commission, p. 2. Available from: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp80_en.pdf [Accessed 15 November 2017].

[18] See for instance Meena, K. and Malarvizhi, N. (2017) An Efficient Human Identification through MultiModal Biometric System. *Brazilian Archives of Biology and Technology*, 59(2). Available from: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1516-89132016000300403&lng=en&tlng=en [Accessed 24 July 2018]; or earlier Wilson, C. R. (2003) *Biometric Accuracy Standards*. [online] National Institute of Standards and Technology. Available from: https://csrc.nist.gov/CSRC/media/Events/ISPAB-MARCH-2003-MEETING/documents/March2003-Biometric-Accuracy-Standards.pdf [Accessed 20 November 2017].

[19] Meena, K. and Malarvizhi, N. (2017) An Efficient Human Identification through MultiModal Biometric System. *Brazilian Archives of Biology and Technology*, 59(2). Available from: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1516-89132016000300403&lng=en&tlng=en [Accessed 24 July 2018];

[20] In some systems, higher false rejection rate (the ratio of individuals wrongly denied access to a system) may be considered safer than higher false acceptance rate (the ratio of individuals wrongly authorized to access a system).

[21] Koops, B. J. (2006) Should ICT Regulation Be Technology-Neutral? In: Koops, B. J., Lips, M., Prins, C. and Schellekens, M. (eds.) *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*. The Hague: T. M. C. Asser Press.

in which biometric data is processed. In the opposite case, this might lead to circumvention of obligations set out in the GDPR and result in harm to data subjects, i.e. natural persons whose personal data is processed. Determining acceptability of an accuracy level is then a different question that should not influence classification of a system as being a biometric system.[22]

Technological neutrality is crucial also in determining whether mere monitoring users' online behavior, its analysis for creating identification profiles, and consequent application of these profiles qualifies as biometrics. Some may argue that special sensors are needed for a system to be considered as biometric system. For instance, traditional biometric systems use sensors, such as cameras (facial recognition) or microphone (voice recognition), that directly measure some natural property of a human and modify it into an electric signal.[23] In biometric systems monitoring users' online behavior the functions of sensors are performed by the very devices of these users. Data gathered from these devices are then remotely analyzed just as data from sensors that are traditionally considered as biometric sensors. Utilization of a keyboard, mouse or touchpad in fact provides information about behavior that is converted into an electric signal. Identity of users is digitalized[24] such as with any other type of biometrics. Specific templates can be created based on these data as well.

The term biometric data within the meaning of the GDPR then includes any data resulting from electronic processing of data gathered based on physical, physiological or behavioral characteristics of a person regardless of sensors used if such resulting data are used for the purpose of unique identification. With regard to the technological neutrality and importance of effects of a technology, errors in accuracy should not *per se* discriminate a system from being considered as processing biometric data.

---

[22] A29 WP formulated several criteria for assessing acceptability of accuracy: the purpose of processing, false accept rate (probability of incorrect identification), false reject rate (probability of incorrect rejection during identification), population size, and "the ability to detect a live sample". Article 29 – Data Protection Working Party. (2012) *Opinion 3/2012 on developments in biometric technologies*. 00720/12/EN WP 193. Brussels: Directorate C of the European Commission, p. 6. Available from: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf [Accessed 20 October 2017].

[23] Mordini, E., Tzovaras, D. and Ashton, H. (2012) Introduction. In: Emilio, Mordini, Dimitros Tzovaras (eds.) *Second Generation Biometrics: The Ethical, Legal and Social Context*. Dordrecht: Springer, p. 7.

[24] Ghilardi, G. and Keller, F. (2012) Epistemological Foundation of Biometrics. In: Emilio, Mordini, Dimitros Tzovaras (eds.) *Second Generation Biometrics: The Ethical, Legal and Social Context*. Dordrecht: Springer, p. 40.

The resulting data become biometric data at the moment when they enable a system to recognize a person from all other people enrolled in the system.[25]

3. ONLINE BEHAVIOR RECOGNITION AS BEHAVIORAL BIOMETRICS UNDER THE GDPR

Online behavior recognition in the meaning of determining or verifying identity falls under the category of behavioral biometrics defined from the technical point of view. In general, there are five categories of behavioral biometrics and each of them is based on analysis of different features.[26] Online behavior recognition is based on monitoring the activity of a device. This activity can be caused either by a user (active use of applications as well as regular breaks and switching between applications that may result in identification of original patterns of behavior) or by a device itself.

With regard to the very nature of biometrics and the purpose of protecting personality of humans, only templates based on activity originating from a natural person can be considered as biometric data within the meaning of the GDPR. Behavioral patterns are expressions of one's own identity and, therefore, deserve strict legal protection. These patterns can be observed also indirectly from *"observable low-level actions of computer software"* such as call traces, audit logs, program execution traces etc.[27] On the other hand, activity of a device itself does not constitute a link to a personality of their users. Therefore, when assessing whether a certain template falls in a category of biometric data, one needs to analyze what types of data were used for creating this template. Activity of a device could

---

[25] According to A29 WP *"a natural person can be considered as ''identified'' when, within a group of persons, he or she is ''distinguished'' from all other members of the group"*. Article 29 – Data Protection Working Party. (2007) *Opinion 4/2007 on the concept of personal data*. 01248/07/EN WP 136. Brussels: Directorate C of the European Commission, p. 12. Available from: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf [Accessed 20 October 2017].

[26] These are authorship-based biometrics, biometrics based on monitoring human-computer interaction, indirect biometrics based on monitoring low level actions of SW, kinetics based on monitoring motor skills of people, and purely behavioral biometrics based on monitoring a human while performing mentally demanding tasks. For details see Yampolskiy, R. V. and Govindaraju, V. (2010) Taxonomy of Behavioral Biometrics. In: Wang, L. and Geng, X. (eds.) *Behavioral Biometrics for Human Identification: Intelligent Applications*. [online] IGI Global, pp. 1–43. Available from: https://www.researchgate.net/publication/254217766_Taxonomy_of_Behavioural_Biometrics [Accessed 15 September 2017].

[27] Op. cit., pp. 2–3.

constitute a link to a natural person only with help of additional information, including personalization of a device. So called device fingerprint that is based purely on data related to functional specificities unconnected to any activities of a user cannot be considered personal data for obvious reasons.

If both user's activity as well as device's activity would be analyzed together in order to create a device fingerprint, such analysis would result in a combined biometric template. How should one determine which data is biometric and whether a stricter legal regime would apply? The technique of combining more types of input data typically happens in multi-modal biometric systems and is called information fusion.[28] The fusion can be performed at three levels – at the feature extraction level when the system merges data from all sensors, at the matching score level when the system combines values of matching scores from various sensors, and at the decision level when decisions based on matching scores (accept/reject decision) are combined.[29] From the legal point of view, the problem arises only when data from all sensors would be merged (at the feature extraction level) so the resulting identification data would not be based solely on *"the physical, physiological or behavioural characteristics"* as defined in the GDPR. There are already solutions utilizing so called hybrid information fusion that combine a biometric component with a numerical component.[30] In special environments, especially in the online behavior recognition area, systems might start to utilize various types of data, including activity initiated solely by a device. Such identification data based on hybrid information fusion should be, however, considered as biometric data. The GDPR does not impose a requirement that specific technical processing needs to relate solely *"to the physical, physiological or behavioural characteristics"*. It only needs to relate to it and combination with a different kind of information should not prevent the data from being awarded a higher level of protection. However, a different situation would arise if behavioral data of a user would be unknowingly merged from a number

[28] Ross, A. and Jain, A. (2003) Information Fusion in Biometrics. *Pattern Recognition Letters*, 21(13), p. 2117. Available from: https://www.sciencedirect.com/science/article/pii/S0167865503000795?via%3Dihub [Accessed 2 November 2017].

[29] Ibid.

[30] Iovane, G., Bisogni, C., De Maio, L. and M. Nappi (2018) An encryption approach using Information Fusion techniques involving prime numbers and Face Biometrics. *IEEE Transactions on Sustainable Computing*, (99). Available from: http://ieeexplore.ieee.org/document/8259031/ [Accessed 15 January 2018].

of users falsely classified as one user. In that case, such inaccurate data could not be considered as a biometric template even though it could be used to identify for instance members of one family.

Creation of biometric behavioral templates relies on spotting patterns in behavior as well as in analysis of psychological traits of a person. Psychological-based biometric techniques measure individual's *"response to concrete situations or specific tests to conform to a psychological profile"*.[31] Therefore, utilization of such techniques might be also considered as profiling[32] within the meaning of the GDPR. Profiling is defined in its Art. 14 point 4) as

> *"any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements."*

In general, the difference of profiling and biometrics lies in their purpose. Biometrics is used for determining or verifying an identity of a person, while profiling aims at evaluation of a natural person and possibly placing that person in a certain group or a category. Profiling can be even based on biometric data themselves as a special category of personal data. It has been established a number of times that biometric data contains information that can be used for evaluation of certain aspects of a person, such as her health, gender, ethnicity, or emotional state.[33] In such case special obligations apply.[34] However, even the GDPR uses the term "profile" as a means of possible identification of a person.[35] Although the GDPR may not specifically refer to "profiling", this illustrates the technical interconnectedness of profiling and identification.

---

[31] Article 29 – Data Protection Working Party. (2012) *Opinion 3/2012 on developments in biometric technologies*. 00720/12/EN WP 193. Brussels: Directorate C of the European Commission, p. 4. Available from: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf [Accessed 20 October 2017].

[32] Profiling is based on use of algorithms *"to locate unexpected correlations and patterns"*. See Hildebrandt, M. (2015) *Smart Technologies and the End(s) of Law*. Cheltenham: Edward Elgar Publishing, p. 241.

[33] See for instance Yannopoulos, A., Androniku, A. and Varvarigou T. (2008) Behavioural Biometric Profiling and Ambient Intelligence. In: Mireille Hildebrandt, Serge Gutwirth (eds.) *Profiling the European Citizen: Cross-Disciplinary Perspectives*. [online] Dordrecht: Springer, pp. 89–110. Available from: http://www.springer.com/gp/book/9781402069130 [Accessed 21 August 2017]. Springer; or Kindt, E. (2013) *Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis*. Dordrecht: Springer.

The question is whether profiling itself can result in creation of biometric data, i.e. if a specific profile of a person based on her behavior that enables her identification is created, should it be considered as biometric data even if the initial intention of a controller was not to process biometric data?

The answer is yes. Determining an identity of a natural person for instance in cases when abnormal behavior is monitored is based on behavioral modelling which overlaps with the legal definition of profiling in the GDPR. Behavior-based tracking relies heavily on models of behavior. Information about such online behavior of a person relates to her physical, physiological, behavioral, or psychological characteristics as it refers to her state of mind (typically search for specific contents) or her ability and manners in using a device that serves as a sensor. A profile combining such gathered information can be compared to a biometric template created based on multi-modal biometrics. Accuracy of linking behavior to a person can vary. However, research suggests that on datasets of 3,800 users up to 87 % of users can be identified based on their behavior[36] and on datasets of 55 users up to 100 % of users can be identified.[37] Moreover, each session in which behavior of a user is monitored and used for updating a model of her behavior, needs to be considered as biometric features extraction and treated as such with regard to legal obligations defined in the GDPR.

From a legal perspective, it is worth to note that even though the main purpose of profiling is evaluation, the profiling does not need to include inference, i.e. any judgment based on the data.[38] This argument could not be used in order to avoid considering profiling also as constituting biometric

---

[34] See Art. 22 of the GDPR and for details Article 29 – Data Protection Working Party. (2017) *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*. 17/EN WP 251. Brussels: Directorate C of the European Commission. Available from: http://ec.europa.eu/newsroom/document.cfm?doc_id=47742 [Accessed 15 November 2017].

[35] Recital 30 of the GDPR stipulates the following: *"Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them."*

[36] Herrmann, D., Kirchler, M., Lindemann, J. and Kloft, M. (2016) Behavior-based tracking of Internet users with semi-supervised learning. *14th Annual Conference on Privacy, Security and Trust (PST)*, Auckland, New Zealand, 12–14 December. IEEE. Available from: https://ieeexplore-ieee-org.ezproxy.techlib.cz/document/7906992/ [Accessed 24 July 2018].

[37] Gu, X., Yang, M., Feit, J., Ling, Z. and Luo, J. (2015) A Novel Behavior-Based Tracking Attack for User Identification. *Third International Conference on Advanced Cloud and Big Data*, Yangzhou, China, 30 October – 1 November. IEEE. Available from: https://ieeexplore-ieee-org.ezproxy.techlib.cz/document/7435478/ [Accessed 24 July 2018].

data. Even though establishing a biometric template based on behavioral data was not initially on mind of a controller, identified behavior models can later serve for a different purpose which is a possibility presumed by the GDPR in Art. 6 par. 4. Moreover, identification is typically achieved based on evaluation of data through their comparison. Here the profiling represents a case of a function creep when certain technology develops and gains new unforeseen functionalities.

However, the condition for a profile to qualify as biometric data depends on its ability to distinguish a person to whom it relates from a group of people. The profile can be associated with a certain group (in biometric systems there are for instance groups of users with different access rights) but in order to be considered as biometric data, it must be possible to exclude the profile from that group (requirement of unique identification). On the other hand, the exact identity of a person does not need to be determined. The reason is that biometric data can be used also only to *"verify the identity without actually identifying the individual"*.[39]

If a controller creates a profile of a person based on her online behavior which allows her unique identification, then such creation has legal consequences both for controllers as well as data subjects. The most important obligation of controllers relates to respecting principles relating to processing personal data. In order to comply with the GDPR requirements, controllers must continually examine their data and profiles based on the data in order to determine whether they process biometric data or not. The crucial element here is the potential of the data to allow unique identification.[40] However, processing of biometric profiles needs to fulfill requirements for processing special categories of data under Art. 9 of the GDPR only if a controller uses the profile among other to distinguish a particular person from others. Especially in the context of an online environment where exceptions for processing biometric data other than

[38] Article 29 – Data Protection Working Party. (2017) *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*. 17/EN WP 251. Brussels: Directorate C of the European Commission, p. 7. Available from: http://ec.europa.eu/newsroom/document.cfm?doc_id=47742 [Accessed 15 November 2017]).

[39] Article 29 – Data Protection Working Party. (2012) *Opinion 01/2012 on the data protection reform proposals*. 00530/12/EN WP 191. Brussels: Directorate C of the European Commission, p. 10. Available from: http://www.europarl.europa.eu/document/activities/cont/201305/20130508ATT65841/20130508ATT65841EN.pdf [Accessed 15 October 2017].

[40] This can be perceived as parallel to the very definition of personal data as any information relating to an identifiable natural person.

explicit consent, controllers need to make sure to be able to prove that a data subject granted them an explicit consent.[41]

4. CONCLUSION

The paper argues that processing users' profiles based on analysis of their online behavior for the purpose of identifying them falls under the category of biometric data within the meaning of the GDPR. However, this applies on the profiles that are based on activity originating from a natural person, not on the activity of a device itself. Activity of a device could be considered as personal data in case additional information is provided and the activity of a device can be linked to an individual. In case of hybrid information fusion, one needs to distinguish at which level various kinds of data are combined. In case of merging biometric data with other type of data on a sensor level, the resulting data should still be considered as biometric data. At other levels of fusion, biometric data is distinguishable from other types of data.

Behavioral biometrics in the online environment overlaps with so called profiling. Biometric data can be used for profiling to evaluate qualities of a person. However, profiling can also lead to creation of a profile corresponding to a biometric template. This must be taken in account by controllers who at a certain moment need to assess whether they shall comply with a stricter regime of data processing. Distinguishing the purpose of processing will then determine the legal regime and requirements on the processing.

Qualification of behavior-based tracking has consequences for instance for service providers who monitor activity of users online that would be otherwise considered anonymous. If these providers are able to identify a person from a group of people based on her behavior regardless of the fact whether they can contact her in the offline world by other means, they process biometric data and must comply with all requirements set out by the GDPR.

Creation of online behavioral profiles can have serious consequences for the protection of privacy. These profiles could become so called identifiers of general application which would put an end to anonymous and

[41] For details about requirements on explicit consent see Article 29 – Data Protection Working Party. (2017) *Guidelines on Consent under Regulation 2016/679*. 17/EN WP 259. Brussels. Available from: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611232 [Accessed 8 January 2018].

untraceable behavior. This would seriously influence fundamental rights and freedoms of individuals on a large scale. Impacts of such practice shall be analyzed in further research.

LIST OF REFERENCES

[1] (1996) *Webster's Encyclopedic Unabridged Dictionary of the English Language*. New York: Random House.

[2] Article 29 – Data Protection Working Party. (2003) *Working document on biometrics.* 12168/02/EN WP 80. Brussels: Directorate E of the European Commission. Available from: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp80_en.pdf [Accessed 15 November 2017].

[3] Article 29 – Data Protection Working Party. (2007) *Opinion 4/2007 on the concept of personal data.* 01248/07/EN WP 136. Brussels: Directorate C of the European Commission. Available from: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf [Accessed 20 October 2017].

[4] Article 29 – Data Protection Working Party. (2012) *Opinion 01/2012 on the data protection reform proposals.* 00530/12/EN WP 191. Brussels: Directorate C of the European Commission. Available from: http://www.europarl.europa.eu/document/activities/cont/201305/20130508ATT65841/20130508ATT65841EN.pdf [Accessed 15 October 2017].

[5] Article 29 – Data Protection Working Party. (2012) *Opinion 3/2012 on developments in biometric technologies.* 00720/12/EN WP 193. Brussels: Directorate C of the European Commission. Available from: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf [Accessed 20 October 2017].

[6] Article 29 – Data Protection Working Party. (2017) *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.* 17/EN WP 251. Brussels: Directorate C of the European Commission. Available from: http://ec.europa.eu/newsroom/document.cfm?doc_id=47742 [Accessed 15 November 2017].

[7] Article 29 – Data Protection Working Party. (2017) *Guidelines on Consent under Regulation 2016/679. 17*/EN WP 259. Brussels. Available from: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611232 [Accessed 8 January 2018].

[8] Banse, C., Herrman, D. and Federrath, H. (2012) Tracking Users on the Internet with Behavioral Patterns: Evaluation of its Practical Feasibility. In: Gritzalis, D., Furnell, S. and

Theoharidou, M. (eds.) *27th IFIP TC 11 Information Security and Privacy Conference*, Heraklion, Crete, 4–6 June. Berlin: Springer, pp. 235–248. Available from: https://link.springer.com/chapter/10.1007/978-3-642-30436-1_20 [Accessed 24 November 2017].

[9] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Union* (1995/L 281/38) 23 November. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046 [Accessed 1 November 2017].

[10] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). *Official Journal of the European Union* (2002/L 201/45) 31 July. Available from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML [Accessed 1 November 2017].

[11] European Commission. (2016) *Cookies*. [online] European Commission. Available from: http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm [Accessed 22 December 2017].

[12] Eurostat. (2017) *Individuals – frequency of internet use* [isoc_ci_ifp_fu]. [online] European Commission. Available from: http://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do [Accessed 22 December 2017].

[13] Ghilardi, G. and Keller, F. (2012) Epistemological Foundation of Biometrics. In: Mordini, E., Tzovaras, D. (eds.) *Second Generation Biometrics: The Ethical, Legal and Social Context.* Dordrecht: Springer.

[14] Gu, X., Yang, M., Feit, J., Ling, Z. and Luo, J. (2015) A Novel Behavior-Based Tracking Attack for User Identification. *Third International Conference on Advanced Cloud and Big Data*, Yangzhou, China, 30 October – 1 November. IEEE. Available from: https://ieeexplore-ieee-org.ezproxy.techlib.cz/document/7435478/ [Accessed 24 July 2018].

[15] Gu, X., Yang, M., Shi, C., Ling, Z. and Luo, J. (2016) A novel attack to track users based on the behavior patterns. *Concurrency and Computation Practice and Experience*, 29(6). Available from: https://onlinelibrary-wiley-com.ezproxy.techlib.cz/doi/full/10.1002/cpe.3891 [Accessed 24 July 2018].

[16] Herrmann, D., Banse, C. and Federrath, H. (2013) Behavior-based tracking: Exploiting characteristic patterns in DNS traffic. *Computers & Security*, 39 Part A. Available from:

https://www-sciencedirect-com.ezproxy.techlib.cz/science/article/pii/S0167404813000576 [Accessed 24 July 2018].

[17] Herrmann, D., Kirchler, M., Lindemann, J. and Kloft, M. (2016) Behavior-based tracking of Internet users with semi-supervised learning. *14th Annual Conference on Privacy, Security and Trust (PST)*, Auckland, New Zealand, 12–14 December. IEEE. Available from: https://ieeexplore-ieee-org.ezproxy.techlib.cz/document/7906992/ [Accessed 24 July 2018].

[18] Hildebrandt, M. (2015) *Smart Technologies and the End(s) of Law*. Cheltenham: Edward Elgar Publishing.

[19] Iovane, G., Bisogni, C., De Maio, L. and Nappi, M. (2018) An encryption approach using Information Fusion techniques involving prime numbers and Face Biometrics. IEEE *Transactions on Sustainable Computing,* (99). Available from: http://ieeexplore.ieee.org/document/8259031/ [Accessed 15 January 2018].

[20] Kindt, E. (2008) Need for Legal Analysis of Biometric Profiling. In: Hildebrandt, M. And Gutwirth, S. (eds.) *Profiling the European Citizen. Cross-Disciplinary Perspectives*. Dordrecht: Springer.

[21] Kindt, E. (2013) *Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis*. Dordrecht: Springer.

[22] Koops, B. J. (2006) Should ICT Regulation Be Technology-Neutral? In: Koops, B. J., Lips, M., Prins, C. and Schellekens, M. (eds.) *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*. The Hague: T. M. C. Asser Press.

[23] Meena, K. and Malarvizhi, N. (2017) An Efficient Human Identification through MultiModal Biometric System. *Brazilian Archives of Biology and Technology*, 59(2). Available from: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1516-89132016000300403&lng=en&tlng=en [Accessed 24 July 2018].

[24] Mordini, E., Tzovaras, D. and Ashton, H. (2012) Introduction. In: Mordini, E. And Tzovaras, D. (eds.) *Second Generation Biometrics: The Ethical, Legal and Social Context*. Dordrecht: Springer.

[25] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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) (Text with EEA relevance). *Official Journal of the European Union* (2016/L 119/1) 4 May. Available from: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679 [Accessed 1 November 2017].

[26] Ross, A. and Jain, A. (2003) Information Fusion in Biometrics. *Pattern Recognition Letters*, 21 (13), pp. 2115–2125. Available from: https://www.sciencedirect.com/science/article/pii/S0167865503000795?via%3Dihub [Accessed 2 November 2017].

[27] Z. Li, S., Anil, K. Jain (eds.) (2009*) Encyclopedia of Biometrics*. [online] Dordrecht: Springer. Available from: https://link.springer.com/referencework/10.1007/978-3-642-27733-7 [Accessed 27 October 2017].

[28] Wilson, C. R. (2003) *Biometric Accuracy Standards.* [online] National Institute of Standards and Technology. Available from: https://csrc.nist.gov/CSRC/media/Events/ISPAB-MARCH-2003-MEETING/documents/March2003-Biometric-Accuracy-Standards.pdf [Accessed 20 November 2017].

[29] Yampolskiy, R. V. and Govindaraju, V. (2010) Taxonomy of Behavioral Biometrics. In: Wang, L. andGeng, X. (eds.*) Behavioral Biometrics for Human Identification: Intelligent Applications*. [online] IGI Global, pp. 1–43. Available from: https://www.researchgate.net/publication/254217766_Taxonomy_of_Behavioural_Biometrics [Accessed 15 September 2017].

[30] Yannopoulos, A., Androniku, A. and Varvarigou T. (2008) Behavioural Biometric Profiling and Ambient Intelligence. In: Mireille Hildebrandt, Serge Gutwirth (eds.) *Profiling the European Citizen: Cross-Disciplinary Perspectives*. [online] Dordrecht: Springer, pp. 89–110. Available from: http://www.springer.com/gp/book/9781402069130 [Accessed 21 August 2017].