Paper

The Practical Implementation of Biometric Technology – Legal Aspects

Magdalena Tomaszewska-Michalak

Faculty of Journalism and Political Science, University of Warsaw, Warsaw, Poland

Abstract—The article refers to legal and social problems, which may occur while implementing a biometric system. The research on biometric regulation made by the author while preparing the Ph.D. thesis resulted in finding general rules, which should be followed by legislator to introduce a well-functioning and user's friendly biometric system.

Keywords—biometric legislation, biometric system, data protection.

1. Introduction

Biometric technology is used to identify or verify a person's identity based on ones individual features. The unique features can be divided into two categories: biological and behavioral. Biological features are strictly connected with the body, i.e., fingerprints, iris, or vain pattern. Behavioral features are associated with a process of repeating some actions what makes them individual, e.g. a signature.

Nowadays the most popular aim of using biometric devices is to raise the security level in the public safety area. This technology became popular also as an instrument to protect against the unauthorized access to the restricted zones. The biggest value of the biometric security measures is the fact that the process of features comparison is automatic. In consequence, it hinders the potential impostor to commit an identity fraud.

This technology is also very convenient for users, as passwords or PIN codes are not required to get the authorization, e.g., to withdraw money from the ATM machine. That is why biometric technology becomes popular also in private sectors of the economy, such as banking, labor, and mass events.

Furthermore, Poland, as a member of the European Union (EU), participates in biometrics' projects aiming to raise the level of safety on the territory of the European Community. These are: the Second Generation of Schengen Information System, Visa Information System and European Dactyloscopy (Eurodac). Moreover, passports with biometric photography and two encrypted fingerprints are now being issued to the EU citizens. Therefore biometric technology became nowadays commonly used both in documents and in the variety of security systems.

In spite of indubitable advantages, biometry arose a lot of controversy especially in the area of privacy policy and data protection. Opponents claim that collecting such sensible data might be very risky as it could be used improperly. It is always possible to modify a PIN code or a password but is not possible to "change" a fingerprint or an iris.

According to the report "Biometric at the Frontiers: Assessing the Impact on Society" [1] it is possible to name five areas in which the author of the text remark the potentially negative impact of utilizing the biometric technology:

- social aspect,
- legal aspect,
- medical aspect,
- economical aspect,
- technological aspect.

This article will focus on the first two areas, which can transpire to be crucial for the biometric system users. The text is based on the research made by the author for the Ph.D. purpose. The author analyzed legal acts, reports and other documents concerning biometric technology both on the EU level and on the domestic field. The research helped to identify the general problems, which can occur while implementing the biometric system. The results of the analysis may also be useful in a process of designing a legal framework for a new biometric system.

2. Social Aspects

As it was pointed in the numerous texts the important issue while implementing biometric technology is paying attention to the level of social acceptance of the existing system [1]–[3]. As the practice shows, several social issues may be identified:

- the use of biometric technology to keep the citizens under the police surveillance,
- the social fear of acquiring the biometric data,
- the misuse of the biometric technology,
- a fear of biometric fraud,
- ineffectiveness of biometric technology.

2.1. Biometric Technology in Person Surveillance

The biometric technology is claimed to be used to improve the security. Therefore, generally it is associated

with gathering and using biometric data by the police [4]. That causes questions about the appropriate use of the processed data in the non-police systems. As a consequence citizens are often concerned about their privacy rights. The city of Łomża is a good example of the mentioned situation. The Mayor of Łomża decided to introduce biometric fingerprints' devices to improve contacts between the City Hall and the citizen. As a result, the decision attracted a lot of criticism. It was claimed that the biometric data are too sensitive to gather them just to amend the efficiency of the City Hall.

2.2. The Social Fear of Acquiring the Biometric Data

It is not unusual that the opposers of the new technology try to discredit it in a spectacular way. Biometric technology was no exception. In 2008, the hacker group Chaos Computer Club acquired and published a fingerprint of German Federal Minister of Interior Wolfgang Schauble [5]. The group wanted to show how easy is to gather and improperly use a biometric data. They acquired a fingerprint from the glass after the Minister's press conference. As a consequence more and more people, not only in Germany, are protesting against proceeding biometric data.

2.3. The Misuse of the Biometric Technology

Although there are often no limits in implementing biometric technology in a private sector, it has to be bear in mind that irrelevant use of biometric data in one case may has an influence on general social acceptance of biometric technology. Facebook Deep Face software is an algorithm, which finds and tags the same person on different photos [6]. It is claimed that the accuracy of Deep Face is 97.25%. Notwithstanding Facebook introduced its application only for amusement purposes, it is possible to use it to track people's interests and Internet activities. In consequence, implementing such systems may cause social concerns and have an influence on acceptance of the biometric technology in other areas.

2.4. A Fear of Biometric Fraud

The social acceptance of biometrics technology is also associated with the fear of the consequences of biometric identity fraud. In order to deceive a fingerprint device a Chinese women Li Rong made a surgery to alter her fingerprints [7]. As a result, she manage to enter Japan illegally. Based on Li Rong case the opposers of biometric technology clam that too much faith in put it the effectiveness of biometric devices.

2.5. Ineffectiveness of Biometric Technology

Supporters of biometrics systems claim that the devices are improving the level of safety because their accuracy is very high. When, after such statement, it is reported that the facial recognition system failed in identifying the Boston marathon bombers, the citizens can lose confidence in biometric technology as such [8]. A feeling of disappointment is also intensifying by a lack of knowledge about a factors influencing the proper functioning of the biometric device.

3. Legal Aspects

It is important to understand that the legal and social aspects concerning biometric technology are inextricably linked. The social reluctance to biometric solutions can have variety of basis. One of them might occur when ambiguous legislation is being published. This can be a reason of concerns about the privacy law and the proper protection of biometric data. According to author's research, it is possible to indicate six areas, which should be taken into account while implementing biometric legislation:

- the aim of the regulation,
- the technical infrastructure,
- the gathering data rules,
- indicating the user's group,
- indicating the excluded groups,
- emergency procedures,
- the protection of biometric data.

In the author's opinion, similar problems can be identified in the public sector as well as in the private one.

3.1. The Aim of the Regulation and the Technical Infrastructure

The first and crucial issue before choosing a biometric solution should refer to the proper identification of a system's aim. Two forms of using biometric authorization can be named: identification and verification. During the process of identification, the biometric sample is taken from a person and compared with all the samples gathered in a database.
Verification instead is a comparison between a biometric sample taken from a person and a sample from the database, which is believed to come from the verified person. Thus, identification is used for recognize once personality whereas verification is a confirmation of the personality declared.
Every legal act implementing a new biometric system should indicate what is the aim of processing the biometrics data. There are system in which both: identification and verification are used, e.g. Visa Information System. The importance to make a distinction between identification and verification might be crucial mainly for the way of storing the biometric samples. Verification does not require gathering the biometric samples in a central database whereas identification in most cases does. This means in practical

terms that verification gives a person opportunity to store a data by his own, e.g. on a card. The case of implementing a EU's biometric passports shows the seriousness of this issue. The Council Regulation no. 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States [9] in Article 4 claims:

"[...] 3. For the purpose of this Regulation, the biometric features in passports and travel documents shall only be used for verifying:

(a) The authenticity of the document.

(b) The identity of the holder by means of directly available comparable features when the passport or other travel documents are required to be produced by law".

Taking into account the aim of the regulation (verification) the obvious consequence should have been storing fingerprints in a new passport. Notwithstanding, within EU there are countries in which the biometric data are processed in a central database (e.g. France). Such differences do not foster the acceptance of gathering biometric samples. Storing fingerprints in the central passports bases may be seen as a misuse of the biometric samples.

3.2. The Gathering Data Rules

Another important issue while implementing biometric legislation is to introduce a proper rules concerning gathering the biometric data. A complete regulation must contain not only a detailed instruction on the process of gathering data but it should also indicate a person accountable for the whole procedure. It is possible to find such a demand in the Regulation no. 444/2009 of the European Parliament and of the Council [10] amending council regulation no. 2252/2004 on standards for security features and biometrics in passports and travel documents issued by member states. Article 1a claims:

"1. The biometric identifiers shall be taken by qualified and duly authorized staff of the national authorities responsible for issuing passports and travel documents [...]".

Article 1a highlights the importance of taking the biometric identifiers by qualified employees as it is one of the amendments to the regulation 2252/2004 (the amendments were introduced after four years of biometric practice).
A second problem, mentioned above, is the existence of internal instruction for the employees, who are going to gather the data. In such cases the users will not know the exact procedures *a priori*. European Union legislation concerning gathering biometric data for the purpose of biometric systems or documents is terse in the indicated sphere. Article 1a Regulation no. 444/2009 claims only:

"[...] 2. Member States shall collect biometric identifiers from the applicant in accordance with the safeguards laid down in the Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms and in the United Nations Convention on the Rights of the Child. Member States shall ensure that appropriate procedures guaranteeing the dignity of the person concerned are in place in the event of there being difficulties in enrolling [...]".

More precise information is available in technical specifications, e.g. Commission decision no. C (2006) 2909 and in domestic regulations. For instance Polish passport legislation is an example of a proper legislation in the area of gathering a biometric data as it contains the whole process step by step.

3.3. Indicating the User's Group and Excluded Groups

The problem of proper users' indication is directly liked with a regulation's aim. Nevertheless, it is necessary to introduce a norm, which claims whose biometric data are going to be gathered in a concrete system. It can be done in a positive or negative manner. The difference lies in the recording method. The first one requires indicating the target group literally. Article 4 of the Council Regulation no. 2725/2000 of 11 December 2000 concerning the establishment of Eurodac for the comparison of fingerprints for the effective application of the Dublin Convention [11] may be an example:

"1. Each Member State shall promptly take the fingerprints of all fingers of every applicant for asylum of at least 14 years of age and shall promptly transmit the data referred to in points (a) to (f) of Article 5(1) to the Central Unit [...]".

The negative manner of recording indicates a general group as a first step and afterwards a list of exceptions. Again, the example may be passport regulation in Article 1, Regulation no. 444/2009:

"2a. The following persons shall be exempt from the requirement to give fingerprints: (a) Children under the age of 12 years [...]
(b) persons, where fingerprinting is physically impossible [...]".

Both recording manner are correct although the second one often allow remarking more groups, which should be potentially excluded from the process of biometric data storing. It has to be underlined that, in the author's opinion, all excluded groups should appear in the regulation, even if the group seems to be obvious (as it is in the regulation above in point b). It will give a future user the certainty of one's obligations.

3.4. Emergency Procedures

One of the crucial issues which has to be regulated are emergency procedures. They are activated in two cases. The first one is interrelated with the Failure to Enroll (FEE). FEE is a biometric system error, which occur during the process of taking a biometric identifier. In consequence, it is impossible to create a sample which can be register in a database. The reasons of occurring FEE may vary, e.g., improper way of taking the sample or technologi-

cal problem with the device. Regardless of the reason, the most important is to introduce the norm of behaving when the FEE will take place. The emergency procedure has to be explicit and non-discriminative what means that inability to register a person cannot be a reason for rejecting authorization, e.g., the inability to register fingerprints of a citizen can not be the reason for rejecting him issue a passport. Taking as example biometric passports, domestic regulation should contain a norm, which claims that when the FEE will occur the passport is being issued only with traditional security measures.

The second situation when it is necessary to use the emergency procedures occurs when there is no possibility to verify user's identity. In a case of fingerprints, the reason may be temporally injured finger which exclude the ability of comparing biometric samples. Such situation may be resolved only by comparing other data instead biometric identifiers.

The other issue may be the Failure Rejection Rate (FRR) which occur when an authorized person is not allowed to have an access to a system. In such cases, the question is if a detailed control of other data is enough to give a person potential privileges (e.g. a permission to cross the border) and who should be responsible for making such a decision. Usually, the regulations are very general such as the Article 4, Regulation no. 444/2009 in passport legislation:

"[...] The failure of the matching in [biometric data – authors note] itself shall not affect the validity of the passport or travel document for the purpose of the crossing of external borders".

The mentioned regulation is a consequence of the right to dignity, which should be guaranteed for every EU citizen. The lack of clear emergency procedures may in consequence result a social anxiety when using biometric systems.

3.5. The Protection of Biometric Data

One of the biggest concerns about using biometric system is connected with the proper protection of gathered data. The current legislation of the biometric data is not considering them as a sensitive data such as for example information on health, race and ethnic origins [12]. They are instead "ordinary" personal data, which of course have to be protected but without restrictions attributed to sensitive information. Nowadays we are on step to introduce the new European legislation[1] which, for the first time in the data protection acts, gives a definition of biometric data and treats them similar to the current sensitive data [13]. In consequences the new regulation will strengthen security of gathering and processing the biometric identifiers in general.

Apart from improving the general level of protecting the biometric data, a legislation regulating a particular biometric system may contain also specific norms which are linked with the aim of introducing the biometric security measures. For instance, taking into account Polish passport procedures [14], the Police officers are not allowed to have an access to fingerprints samples (for the time they are stored in a system before issuing a passport), whereas they are permitted to ask for other data if needed to fulfill their obligations. This norm is linked with the aim of the regulation, which is verifying the individuals identity.

Therefore, it must be assumed that protecting biometric data is not only connected with technical infrastructure of processing the information but also with legal procedures restricting the access to biometric samples.

[1]However it has to be taken into account that the new EU regulation classifies the data differently than the Directive 95/46/EC. There will be no closed catalogue of sensitive data and the classification will be done on the base of the analysis of the risk assessment.

4. Conclusion

The technological advancement has a huge influence on ability of using more and more effective biometric systems. This encourages introducing biometric systems for both security reason and users' comfort. Despite the undoubted advantages of biometric technology, it has to be always bear in mind that to create a well-functioning and socially acceptable system it is necessary to launch the legal frames relevant to the aim of the particular biometric system. A proper system should be therefore an effect of cooperation between engineers and lawyers with a background in privacy rights.

References

[1] "Biometric at the Frontiers: Assessing the Impact on Society", 21585 EN [Online]. Available: http://ftp.jrc.es/EURdoc/eur21585en.pdf

[2] "Perception and Acceptance of Fingerprint Biometric Technology" [Online]. Available: https://cups.cs.cmu.edu/soups/2007/posters/p153_heckle.pdf

[3] "Public Perceptions of Biometric Devices: The Effect of Misinformation on Acceptance and Use" [Online]. Available: http://proceedings.informingscience.org/InSITE2004/102moody.pdf

[4] "Biometryczna Łomża. Z odciskiem palca po zasiłek?", Fundacja Panoptykon [Online]. Available: http://panoptykon.org/wiadomosc/biometryczna-lomza-z-odciskiem-palca-po-zasilek

[5] "Hackers Publish German Minister's Fingerprint" [Online]. Available: http://www.wired.com/2008/03/hackers-publish/

[6] "Facebook's DeepFace Software Can Match Faces with 97.25% Accuracy" [Online]. Available: http://www.forbes.com/sites/amitchowdhry/2014/03/18/facebooks-deepface-software-can-match-faces-with-97-25-accuracy/

[7] "'Fake fingerprint' Chinese woman fools Japan controls" [Online]. Available: http://news.bbc.co.uk/2/hi/asia-pacific/8400222.stm

[8] "Why facial recognition tech failed in the Boston bombing manhunt" [Online]. Available: http://arstechnica.com/information-technology/2013/05/why-facial-recognition-tech-failed-in-the-boston-bombing-manhunt/

[9] "The Council Regulation no. 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States" [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0001:0006:EN:PDF

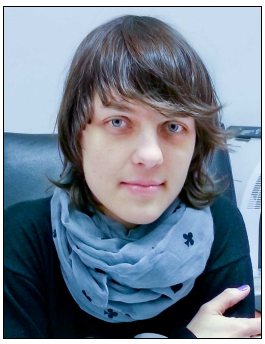
[10] "Regulation (EC) no. 444/2009 of the European Parliament and of the council of 28 may 2009 amending council regulation (EC) no. 2252/2004 on standards for security features and biometrics in passports and travel documents issued by member states" [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:142:0001:0004:EN:PDF

[11] "Council Regulation (EC) No. 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention" [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000R2725&from=PL

[12] "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" [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en

[13] "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" [Online]. Available: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[14] Ustawa z dnia 13 lipca 2006 r. o dokumentach paszportowych (Act on Passport Documents of July 13, 2006), Dz.U. nr 143, poz. 1027 (Journal of Laws, No. 143, item 1027) (in Polish).



Magdalena Tomaszewska-Michalak received her Master's Degree in Law in 2009 from the University of Warsaw, Poland. She did her Ph.D. in 2014 on legal aspects of biometric technology. From 2014 she is an assistant professor at The Faculty of Journalism and Political Science at the University of Warsaw.

E-mail: m.tomaszewska@wpia.uw.edu.pl
Faculty of Journalism and Political Science
University of Warsaw
Krakowskie Przedmieście st 3
00-047 Warsaw, Poland