Remigiusz Lewandowski

Biometrics – new applications

Introduction

Biometrics is a field of expertise in recognition of living people on the basis of biological characteristics measurements (anatomic and physiological), both passive (iris pattern, retinal pattern, hand geometry, vascular structures) as well as active (handwriting dynamics, voice, lips movement, gait)[1]. Looking for an optimal biometric characteristic as an identification tool one should take under consideration many factors, some of them shown in the data table. As it shows each of the solutions applied have their advantages and disadvantages and the choice should be made on the basis of relevance of the solution to meeting the needs of identification.

Table. Comparison of some biometric characteristics.

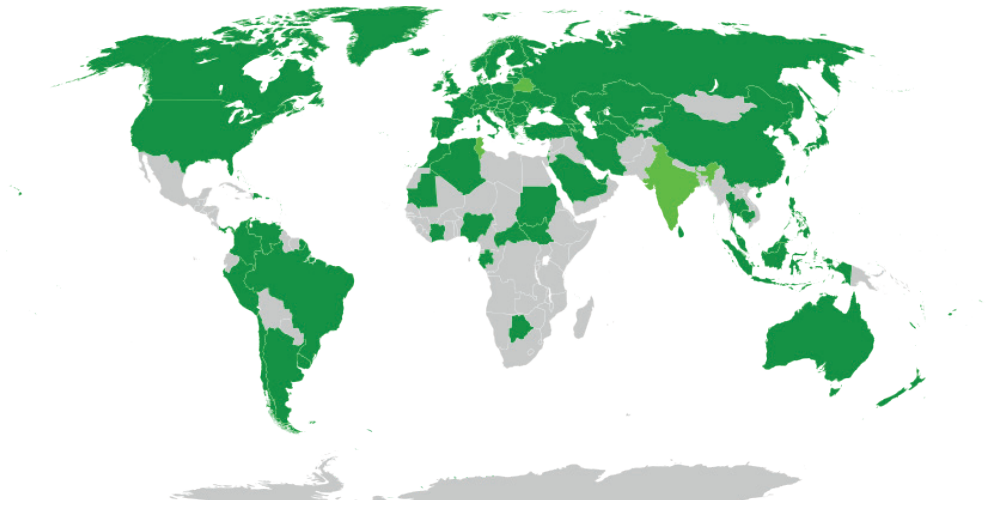
Description	Fingerprint	Hand geometry	Retina	Iris	Face	Signature	Voice
Simplicity of use	large	large	small	medium	medium	large	large
Vulnerability to errors	dry skin, soiling, age	hand laceration	glasses	low lighting	low lighting, age, glasses, hairdo	changes of one's own signature	noise, cold, weather
Accuracy	large	large	very large	very large		very large	large
Acceptability by user	medium	medium	medium	medium	medium	very large	large
Required level of security	large	medium	large	very large	medium	medium	medium
Long-term stability	large	medium	large	large	medium	medium	medium

Scale: very small, small, medium, large, very large.

Source: Private study based on S. Prabhakar, S. Pankat, A.K. Jain, *Biometric Recognition: Security and Privacy Concern*, „IEEE Transactions on Security & Privacy" 2003, no. 1, p. 33–42.

Currently biometrics is a constant and key element in identification documents chain of values. Biometric solutions shall be applicable in passports of most countries. A biometric passport has become virtually a standard nowadays. And this shows picture number 1.

[1] B. Hołyst, J. Pomykała, *Biometrics in certification systems*, „Biuletyn WAT"(„VAT Bulletin") 2011, no. 4, pp. 418–419.



Pic. 1. Introduced and planned biometric passports worldwide.

Legend: dark green: countries with biometric passports; light green: countries with planned biometric passports.

Source: https://commons.wikimedia.org/w/index.php?curid=47470662 [access: 10 X 2016].

1. Biometrics in public documents

Non-biometric passports have still been functioning practically only in African countries (with some exceptions) and some countries in Central and South America and Asia. International Civil Aviation Organization promotes biometric solutions in passports. Annex 9 to the *Convention on International Civil Aviation* recommends that the Contracting States to the Convention shall use biometric data in passports, visas and other official travel documents using one or more additional technologies to store data (point 3.9). Fingerprints and iris pattern are among optional biometric data (apart from obligatory digital recording of facial image). There is only a fingerprint in Polish passport as far as biometrics is concerned. How important development of biometric technologies is show the attempts to circumvent biometric systems. A classic example can be an attempt to go through a biometric gate at the border crossing point by a person hiding a child underneath clothes. This example indicates how wide range of solutions should be applied in situation of automatic control, especially in case of border control. In this particular case implementation of a system to verify whether only one person is going through the gate can be a solution. It can be done for example by registration while a person is going through a gate or by checking of there is a heartbeat of one or more persons heard. Picture 2 shows a test biometric gate developed by the Military University of Technology (VAT).

Pic. 2. Test biometric gate developed by Millitary University of Technology.
Source: http://www.ioe.wat.edu.pl/aktualnosci3/testy-systemu-do-automatycznej-odprawy-osob-na-przejsciu-granicznym-w-medyce/ [access: 10 XII 2016].

Project PROTECT[2] realized by an international consortium with the participation of Polish specialized company ITTI LLC seems to be very interesting. It advanced, multimodal system of biometric identification is intended as a response to growing number of travelling people and limited capacities of European border crossings. The project has the potential to be applied on all types of border crossings (i.e. land border crossings, seaport border points and airport crossings). An advantage of the system will be the possibility of passengers verification without any need to stop them with the minimum requirement of any interaction with the system. Gaining such assumptions will be possible due to application of modern biometric technologies and computer vision. The system is to enable identity verification on the basis of anthropometric measures and specification of walking. It is based on a network of cameras generating 3D picture and model a silhouette of the monitored person. Based on the data gathered, created algorithm uses unique anthropometric measures (for example segments of chosen body parts) and characteristic features chosen from a sequence of walking to verify the person's identity. An advantage of such solution is verification of people during their motion and increased resistance to common trials to forge biometric pattern.

Biometrics applies more and more in IDs. In Europe electronic ID (eID) equipped with a microprocessor with biometric data have become usual one. At present eID is used in 27 countries of the European continent. In Poland an eID project has been launched since 2007 but up to now it has not been fully completed yet for different reasons. Nevertheless, in February 2017 the Ministry of Digital Affairs published the conception of implementation Polish ID with electronic layer[3] which document is a re-

[2] Project realized under the Horyzont programme, Grant number 700259.

[3] https://mc.gov.pl/aktualnosci/nowa-koncepcja-wdrozenia-polskiego-dowodu-osobistego-z-warstwa-elektroniczna [access: 27 II 2017].

vised version of 2016 concept. According to this new updated version facial images are to be implemented in a new ID.

Apart from passports and IDs government authorities issue also other documents containing biometric data stored on microprocessors. In Poland it is for example biometric residence card with fingerprint. Some countries issue electronic driver's license in accordance with ISO standard 18013[4] and/or with Commission Regulation (EC) No 383/2012[5]: Salvador, some India states, Japan, Morocco, Mexico, Indonesia, Queensland in Australia, Croatia, Ireland and the Netherlands[6]. The decision on incorporating biometric data into these documents is up to every country. Commission Regulation (EC) No 383/2012 allows to place on driver's license microprocessor additional data like iris pattern and fingerprint of its owner.

Increasing application of biometrics in documents should come as no surprise. It is one of the most reliable methods of man's identity certification and verification (or a man's identification) but its effectiveness in not unconditional. In the literature there are some necessary conditions indicated that must follow effective biometric certification like optimum conditions of biometric measurement, the biometric measurement update and optimum tolerance level[7]. Biometrics effectiveness can be improved substantially by implementing measurement not only one but at least two biometric characteristics. This way a person can be tied much harder with a document that he/she is using. Nevertheless, biometrics like any other technology should not be treated uncritically[8].

In respect of documents, the most frequent model of biometric certification is verification. It consists of comparison in 1:1 scale a set of characteristics of a person (taken in a process of verification) with biometric data incorporated in a document. In case of compliance set of the data taken in a process of verification, the effect of verification is positive i.e. one can say that a person using a certain document is the person concerned by the document. The advantage of this method is the speed of the process of verification (higher than in identification process[9]) and security of data. Biometric data are stored by the document holder together with the document and central biometric databases of citizens are not created.

Effectiveness of biometric solutions seen by public authorities in state's security area and citizen's migration has been also noticed by other economic branches. Biometrics is more and more applicable in commercial transactions. It regards tablets, notebooks and smartphones, in which there are more and more often fingerprints sensors installed that al-

[4] Establishes frames for the form and content of driving license data.

[5] Establishes technical requirements for driver's license containing microprocessor.

[6] M. Stoltz, *Electronic Driver's Licences: Driving Towards the Future*, „ID & Secure Documents News" 2016 [online], vol. 4, https://www.reconnaissance.net/secure-document-news/issues/may-2016/ [access: 10 XII 2016].

[7] B. Hołyst, J. Pomykała, *Biometrics in certification*…, pp. 420–421.

[8] E. Jakielaszek, *Mechanisms shaping identity management* „Człowiek i Dokumenty" („Man and documents") 2017, no. 44, p. 58.

[9] In the identification process biometric data taken are compared with set of data from a certain database.

low to link a device (and data stored) with its holder. In some countries identification cards with biometric data are used by universities to improve access control and effective identification of students during exams[10]. Biometric system has also been used for identification of citizens during general elections[11]. In the future a widespread use of biometrics also in legal system is predicted including electronic signature[12]. Biometrics on a wider scale lies in two main areas: banking and access control systems based on microprocessor cards.

2. Biometrics in banking

Biometrics in banking appeared more than a decade ago. In 2004 Columbian Bancafe Bank made available ca. 400 biometric cash machines using fingerprints. In the same 2004 year in Japan a process of making available cash machines using vascular structures for identification (Mizuho Bank, Japan Post Bank, Bank of Kyoto, Resona Bank, Bank of Yokohama) was started. Biometry of an eye iris was applied for the first time in banking in Jordan (Cairo Amman Bank) in cash machines and bank branches and then in Internet banking.

In Poland, history of biometrics in banking started in 2010 when Polskiej Spółdzielczości Bank and Podkarpacki Spółdzielczy Bank introduced fingerprints (Pic. 3). Later on other banks like BPH Bank or Getin Bank followed their footsteps. Nevertheless, at present the most attractive solution as far as biometrics is concerned is mobile banking and also solutions applied in branches of the banks.

Pic. 3. Biometric cash machine of Polskiej Spółdzielczości Bank.

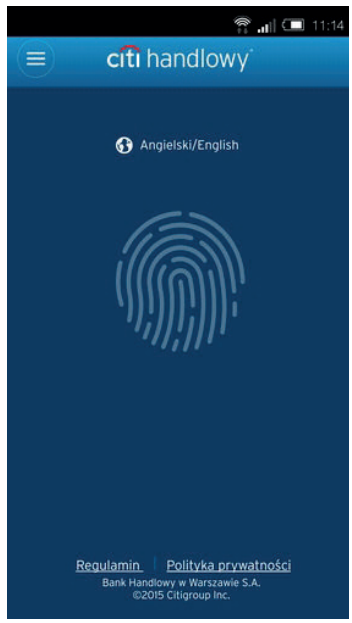
Source: http://prnews.pl/hydepark/bank-bps-rezygnuje-z-biometrii-6551894.html [access: 10 XII 2016].

[10] E. Harinda, E. Ntagwirumugara, *Security & Privacy Implications in the Placement of Biometric-Based ID Card for Rwanda Universities*, „Journal of Information Security" 2015, no. 6, pp. 93–100.

[11] W. Gutfeter, A. Pacut, *A Man in biometric system*, in: M. Tomaszewska-Michalak, T. Tomaszewski, *Documents and law. Practical aspects of documents and e-documents*, Warsaw 2015, p. 80.

[12] T. Dziedzic, *Biometric electronic signature*, in: M. Goc, T. Tomaszewski, R. Lewandowski, *Forensic – unity of science and practice. Combating crime review*, Warsaw 2016, pp. 93–102.

Some banks in Poland have already offered the option to verify identity via biometrics on Smartphones. Such mobile applications are offered by Millenium Bank, Meritum Bank, ING Bank, Euro Bank or Citi Handlowy Bank (Pic. 4). Unfortunatelly, such solution is possible on Apple devices only (Touch ID reader) except in the case of Millenium Bank. These are only insular solutions which are more like gadgets for clients who are fans of new technologies. In banking systems biometrics has not sojourned for good yet. This is a reason why this branch of business has been waiting with great interest for the results of the biometric project announced last year by PKO BP Bank which aims to embrace all access channels of the bank[13].

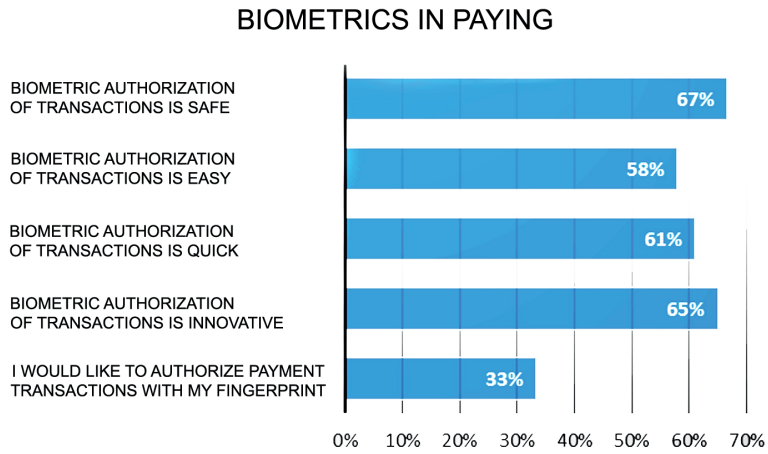


Pic. 4. Mobile application of the Citi Handlowy Bank.

Source: https://www.online.citibank.pl/landing/citimobile/index.htm [access: 10 XII 2016].

In September 2016 there was a survey carried out by MasterCard in Poland which proved that Poles are very much enthusiastic about biometrics in banking sector. As shown on picture 5 a majority of Polish citizens regard the process of payment authorization by biometric solutions as innovative, simple and secure. One in three is willing to use fingerprint as authorization method in payment transactions.

[13] http://wyborcza.biz/biznes/1,147879,18140726,PKO_BP_chce_wdrozyc_kompleksowy_system_biometrycznej.html [access: 10 XII 2016].



Pic. 5. Survey results on biometrics in banking.

Source: Private study based on: http://newsroom.mastercard.com/eu/pl/press-releases/badanie-mastercard-polscy-konsumenci-oczekuja-wiecej-cyfrowych-uslug/ [access: 10 XII 2016].

More and more Polish banks have been working on implementation of biometric systems as an effective way of clients identity supervision, which means more security for services[14]. The trend seems to be irreversible.

3. Biometrics in access control systems

Access control systems based on microprocessor cards belong to the second basic area of biometrics used in other than identity verification with public documents domain. Such systems are used practically in all large and medium-size companies and public administration. Their role is to block access to some spaces – usually by a closed gate or airlock – to unauthorized persons. Unfortunately, in most cases such access control is only illusory. It only checks whether a card itself is valid and whether it gives access to a particular room. It does not verify whether a person using the card is the same person whose access entitlement had been linked to the particular card. In case of a lack of identity checks while people enter particular rooms (which is a standard as far as workers using only badges – access cards, are concerned), it is relatively easy for unauthorized people to enter particular rooms or spaces. It is enough to steal a badge (access card) of an authorized person and use their access entitlement. Is a badge theft difficult? Each of us should give the answer after thinking of measurements he or she takes to protect their access card from a theft. The measurements are not particularly advanced and they do not guarantee actual safety.

[14] M. Tomaszewska, *Biometric technology in Poland*, in: *Forensic in the beginning of 21st century. Selected aspects*, B. Hołyst (ed.), Warsaw 2014, pp. 738–739.

Risk of an unauthorized access cards usage is particularly crucial in case of companies important to state security or some public institutions. Identification of such companies, both private and state controlled is not difficult. It can be done by sector analysis and isolating those economy branches that are strategic from the state security perspective. In a narrow scope these are the following[15]:

1. Production and procurement in electricity.
2. Extraction, transit, distribution and storage of gas fuels.
3. Production, transit and storage of liquid fuels.
4. Telecommunication.
5. Banking.
6. Documents and money production.
7. Arms industry.

In a wider sense economy branches in which access control from the perspective of state security is crucial embrace in addition extraction of hard coal and chemical industry[16] as well. Within these branches there are following state controlled companies: Polska Grupa Energetyczna S.A., Tauron S.A., Energa S.A., Enea S.A., Polskie Sieci Elektrenergetyczne S.A., Polskie Górnictwo Naftowe i Gazownictwo S.A., Gaz-System S.A., Orlen S.A., Lotos S.A., Pprzedsiębiorstwo Eksploatacji Rurociągów Naftowych "Przyjaźń" S.A., PKO Bank Polski S.A., Bank Ochrony Środowiska S.A., Bank Gospodarstwa Krajowego, Polska Wytwórnia Papierów Wartościowych S.A., Polska Grupa Zbrojeniowa S.A., Kompania Węglowa S.A., Jastrzębska Spółka Węglowa S.A., Katowicki Holding Węglowy S.A. and Grupa Azoty S.A. Some experts indicate additionally such branches as air transport, rail transport and maritime transport as well as media.

Furthermore, according to law there are also other companies important from the perspective of state interests and state security. The Act of 26 April 2007 on *crisis management*[17] makes it obligatory to protect facilities, plant and equipment of critical infrastructure (CI) for their owners and possessors both independent and dependent. Companies which own or possess critical infrastructure are listed on the harmonized list of critical infrastructure facilities, plant, equipment and services. The list is classified. Other group of companies is listed in the Cabinet Regulation of 3 November 2015 listing companies of particular economic and defense significance[18]. It comprises 185 companies. The Cabinet Regulation of 22 October 2010 on state-owned companies and single-member state companies of particular significance for state economy[19] comprises at the moment 12 companies.

Indeed, it must be assumed that also companies which are not strategic for the state security should be interested in securing access to their own premises and rooms.

---

[15] R. Lewandowski, *National security and strategic economy branches and regulatory role of the state*, in: *Dimentions of risk management in economic relations*, K. Raczkowski, S. Wojciechowska-Filipek (ed.), Warsaw 2016, pp. 363–394.

[16] Ibidem, p. 376.

[17] Journal of Laws 2007 no. 89 item 590 as amended.

[18] Journal of Laws 2015 item 1871 as amended.

[19] Journal of Laws 2010 no. 212 item 1387 as amended.

In such cases it is about protection of private interests and protection against spying by the competition. Such real protection for all entities gives only an unambiguous link between an employee with his/her access card (containing certain access entitlements). This link is being created by biometrics and putting some particular biometric data of the employee into the access card. Traditional access control methods in the contemporary world and any threats towards them do not work[20] anymore.

As far as public institutions are concerned biometrics is used to secure some isolated rooms but it is not widely applied. The Ministry of Digital Affairs is regarding implementation of biometric access control not only to certain rooms but also to whole buildings used by the Ministry[21]. If the plans enter into force they will definitely be a very interesting and precious test of effectiveness of this access control and physical security method.

By introducing a verification mechanism whether a person using certain access card is the person for whom the card had been issued, the risk of unauthorized access with somebody else's access card to the company's compound or institution can be fully eliminated. This increases significantly the level of security. It applies particularly to companies and institutions which are strategic for national security. In the time of global terrorist threats such security measures should be a standard for this group of entities.

Speaking about biometrics we cannot avoid the subject of personal data protection. Article 1 of the Act of 29 August 1997 on the Protection of Personal Data[22] states that everybody has the right his own personal data to be protected (point 1) and processing of personal data may take place for the benefit of public, the benefit of the person whose data are processed or the benefit of the third person in accordance with the procedure referred to in the Act (point 2). In addition, according to Article 23.1 of the Act data processing is allowed only when:

1) the person whose data are processed so agrees unless it is her data removal,
2) it is necessary to realize the right or fulfill duty in accordance with law,
3) it is necessary to implement an agreement if the person whose data are processed is a party to the agreement or it is necessary to take any actions before implementation of the agreement on the demand of the person whose data are processed,
4) it is necessary to carry out tasks for the benefit of public according to law,
5) it is necessary to fulfill legally justified goals by data administrators or data receivers and the data processing shall not affect rights and freedoms of the person whose data are processed.

Simultaneously, the problem of personal data handling in employer – employee relation is regulated in Article 22[1] of the Labour Code. Data which employer can de-

[20] A.K. Jain, A. Kumar, *Biometrics of Next Generation: An Overview*, in: *The Second Generation Biometrics: The Ethical, Legal and Social Context*, E. Mordini, D. Tzovaras (ed.), Springer 2012, pp. 49–79.

[21] http://www.money.pl/gospodarka/wiadomosci/artykul/dowod-strezynska-biometria-pwpw-mdokumenty,177,0,2234801.html [access: 18 IV 2017].

[22] Journal of Laws number 133, item 833 as amended.

mand are the following: name (names) and surname, mother's and father's name, date of birth, whereabouts (address for correspondence), education, professional career history. An employer can demand also an ID number and other information including names and surnames, dates of birth of children if they are crucial for the employer to benefit from special powers according to labour law. The employer can demand other data only if it is stated so in separate acts and in cases not regulated in this article, the Protection of Personal Data Act shall be applied, especially including Article 23 of the Act.

The law does not regulate precisely the way employers use biometric data of their employees with regard to security. It can be presumed that taking biometric data from employees and their processing is stated in Article 23.1.5 i.e. if it is necessary to fulfill legally justified goals by data administrators or data receivers and the data processing shall not affect rights and freedoms of the person whose data is processed. Security can be regarded as legally justified goal made by data administrator (biometric data). Nevertheless, it seems that this subject shall require more clarity in law.

It is worth noting that up to now the General Inspector of Personal Data (GIODO) has presented rather skeptical attitude towards the use of biometric data in employer-employee relations, for example in access control: *So the one and only reason to gather fingerprints may be a provision of law. But because there are no regulations that would allow employers to demand biometric data like fingerprints, iris scan or DNA from their employees so their gathering is forbidden*[23]*".* Such position of GIODO on biometrics does not seem to meet present threats, including terrorist threats. Article 29 Working Group[24] concluded in a working paper of 1 August 2003 on biometrics that "for the purpose of access control (identification/verification) biometric systems covering physical traits that do not leave traces (like for example shape of a hand but not fingerprint) or biometric systems covering physical traits that leave traces but are not based on recording data and their possession by others than the person whose data is processed present a lower risk of infringement of basic rights and freedoms[25]. In other words data is not recorded inside an access control gear or in a central data base. For such solutions with lower risk belong access systems based on biometric data stored on access cards (identification cards) used by employers. It seems that the way to implementation of such solutions is open.

Nevertheless, EU legislation is aimed at high security of biometric data. *Regulation (EU) No 2016/679of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and the free movement of such data and repeal of Directive 95/46/EC (general data protection regulation)*

[23] http://www.giodo.gov.pl/348/id_art/3358/j/pl/ [access: 10 XII 2016].

[24] A consultation body consisting of representatives of personal data protection institutions of EU member states. Its role is to ensure compliance with Data Protection Directive 95/46/EC by the Member States as far as personal data processing and free transfer of data is concerned.

[25] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf [access: 10 XII 2016].

introduces in Article 9.1 general ban on processing biometric data leading to unambiguous identification of a person or data regarding health, sexuality or sexual orientation. Simultaneously, the Regulation introduces a range of situations in which this general ban does not apply. It is worth noting particularly that the ban does not apply especially when:

1) the person whose data are processed gives a prior consent (unless national or EU law recognizes that such ban cannot be repealed);
2) data processing is necessary to fulfill duties and carry out rights by administrator or the data subject in the area of labor law, social security and social protection as far as it is allowed in national or EU law or in collective agreement which according to national law provides for an appropriate protection and interests of the data subject;
3) data processing is necessary to protect vital interests of the data subject or other person and the data subject is physically or legally incapable of giving his or her consent;
4) data processing is necessary because of important public interest, according to EU or national law, which is proportionate to the objective pursued, do not affect the substance of data protection right and shall provide for appropriate and concrete measures of basic rights and interests security of the data subject.

The above provisions of the Regulation shall not preclude biometrics in security area especially in physical access control or access to IT systems (for example in on-line banking) even with lack of consent from the person whose biometric data shall be processed. In this case precise and specific law is necessary. It is also necessary to underline that according to Article 9.1 of the Regulation Member States can keep or introduce new conditions including limits of biometric data processing. European legislator has left quite a big margin of discretion to shape the frames of biometric data processing.

Conclusions

Biometrics has become more and more common instrument of security improvement. Specific character of this identification method makes it applicable not only in documents issued by a state but also in a non-state environment like banking or companies of strategic importance for state security. Analysis of implementation of biometric solutions in Poland allows to assume that apart from the chosen categories of public documents they are not common. They are applicable on a larger scale by some banks as an instrument of client authentication in electronic banking systems. As a tool of physical access control biometrics is still a technology used on a small scale despite the existence of objective grounds for such need, especially in companies owing or possessing critical infrastructure facilities. It shows a great need of constant awareness raising on possible threats to key economic entities in our country. Simultaneously, entrepreneurs should also be more aware of accessible technologies and solutions which can minimize such threats.

It is very important though, that a proper legislation would keep up with more frequent usage of biometrics, including personal data protection legislation. On the

one hand it should allow to increase the level of security in companies and public institutions while using biometric systems, and on the other hand, it should set minimum security standards while storing and processing biometric data. These standards should protect biometric data from loss of confidentiality, availability, integrity and accountability[26] and particularly from the attacks on biometric systems.

Abstract

The article presents an analysis of new applications of biometrics in the field of security. There are two such key applications. Firstly, apart from documents such as IDs and passports, biometrics can be efficiently used as a physical access control tool in companies that play strategic functions in the public security system. Secondly, it can be applied in the e-banking industry as a customer identification and transaction authorization instrument. In both cases biometrics significantly increases the security level comparing to traditional alternatives. However, a common application of biometrics requires legal regulations that, on the one hand, will allow public and private organizations to use biometrics as a security instrument and, on the other hand, set minimal standards of biometric data protection.

Keywords: biometrics, access control, banking.

[26] W. Krawczyk, *IT security of finger prints data bases (AFIS) and DNA*, in: *New techniques in forensic and security of information*, B. Hołyst, J. Pomykała, P. Potejko (ed.), Warsaw 2014, p. 181.