STUDIA POLITOLOGICZNE VOL. 63
DOI: 10.33896/SPolit.2022.63.7

Magdalena Tomaszewska-Michalak[*]

Biometric Technology 20 Years After 9/11 – Opportunities and Threats

Keywords: *Biometric technology, identification, verification*

Abstract: *The aim of the article is to present the development of biometric technology as a consequence of 9/11 terrorist attacks in the USA and issuing the PATRIOT ACT in 2001. Nowadays biometric technology is popular not only in the public security area (e.g. criminal data bases, face recognition surveillance systems) but is also used in everyday life (e.g. smartphones with touch ID/face recognition). The article shows both sides of biometric devices utilization: advantages and potential negative consequences for individuals.*

Introduction

This article presents the development and consequences of using biometric technology in the twenty-first century. The twentieth anniversary of the terrorist attacks on the World Trade Center and Pentagon on September 11, 2001 seems an excellent occasion to review this topic, as the current development of biometrics is one of the events' consequences. The above gives an opportunity to pose a research question whether the use of biometric technology nowadays has a positive effect on state security. The introduction of biometric solutions in documents

[*] ORCID ID: https://orcid.org/0000-0001-5441-0396. PhD, University of Warsaw. E-mail: tomaszewska.m@uw.edu.pl

(e.g. passports, visas) and public spaces like airports shows that state authorities noticed the advantages of biometric algorithms. On the other hand highlighted problems of biometric algorithm biases lead to pose the second research question: is using biometric devices may have a negative influence on the individuals rights. Many non-governmental organizations raise the problem of biometric technology interference with the right to privacy. As ACLU[1] pointed out: *One of the many privacy intrusions inherent in that goal is the end of anonymity as we know it. As law enforcement authorities continue to add to the network of cameras monitoring our public spaces, it will become increasingly difficult to evade their watchful eye and, soon enough, their automated biometric identification*[2].

The mentioned questions are going to the answered based on the analysis of literature and legal documents.

History of Biometric Technology

To fully understand the functioning of modern biometric technology, it is necessary to firstly focus on the definition and history of biometrics in the public security sector.

Biometrics is the study of characteristics variability among living organism populations. The scientific assumptions of biometrics have led to development of biometric technology, which allows for automatic personal / verification of identity using individual characteristics. The indicated features may be biological or behavioral in nature. The former are related to the properties of the human body and include, among others: fingerprints, facial geometry, the vain pattern or iris. Behavioral characteristics are formulated through an individual's specific and repetitive behavior. Examples include gait, the dynamics of hitting the keyboard or a signature. It is important for the trait used in the comparison process to be common among the studied group and that it be characterized by individuality and relative invariability over time.

When reviewing the definition of biometric technology, the comparison of features may occur in two forms: verification or identification. This stems from the technical infrastructure for processing the feature patterns used in the comparison process. Identity verification is based on

[1] ACLU – American Civil Liberties Union.

[2] https://www.aclu.org/issues/privacy-technology/surveillance-technologies/biometrics (26.11.2021).

a 1:1 comparison. Taking fingerprints as an example, it means that the fingerprints of a person are compared with a specific pattern previously recorded on a specific medium. Identification, on the other hand, is a 1:n comparison, i.e., it is based on an attempt to determine whether any patterns in an existing fingerprint database match the one being checked. The first case seeks only to verify identity, while the second attempts to learn it. The history of biometric technology begins in the twentieth century, with the emergence of technology capable of automatic comparison of an individual's characteristics[3]. However, the most spectacular development of biometric security measures can be observed after the terrorist attacks of September 11, 2001[4]. In response to these events, the US declared a "war on terrorism." This is evidenced by, among others words spoken by President George W. Bush during his speech to Congress on November 20, 2001, *Our war on terror begins with Al Qaeda, but it does not end there. It will not end until every terrorist group of global reach has been found, stopped and defeated*[5]. The Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism (USA PATRIOT ACT), one of the legal tools to fight terrorism, also became quite important in the development of biometrics[6]. The PATRIOT ACT legally sanctioned research on technology enabling effective verification of the identity of individuals wishing to enter the United States. While US authorities wanted to develop biometrics domestically, they also tried to persuade other entities, especially the European Union, to introduce security measures based on individual characteristics[7]. The implementation of biometric security entry systems resulted from efforts to develop technology that identifies people crossing borders. Examples include the American US-VISIT system and the European Union's introduction of biometric passports for citizens of the Schengen area. The former is based on collecting ten fingerprints from a foreigner applying for a US entry visa

[3] S. Mayhew, *History of Biometrics*, https://www.biometricupdate.com/201802/history-of-biometrics-2, (4.08.2021).

[4] K. Gates, *Identifying the 9/11 'faces of terror'. The promise and problem of facial recognition technology*, «Cultural Studies» 2006, Vol. 20 (4–5), pp. 417–440.

[5] *President Bush's address to a joint session of Congress and the nation*, https://www.washingtonpost.com/wp-srv/nation/specials/attacked/transcripts/bushaddress_092001.html, (4.08.2021).

[6] Pub. L. No. 107–56.

[7] M. Gonçalves, M. Gameiro, *Security, privacy and freedom and the EU legal and policy framework for biometrics*, «Computer Law & Security Review» 2012, Vol. 28(3), pp. 320–327.

and registering them in the system[8]. The recorded biometric templates can be used to verify whether the person crossing the border is the same person who applied for the visa. Biometric comparison can, however, also be used in the identification process, which in this case would consist of checking whether the fingerprints belong to a person wanted in connection with a crime. Meanwhile, implementation of the so-called e-passports in the European Union is somewhat different. The obligation to issue travel documents containing a biometric photo and a chip with the encrypted two fingerprints of the holder of the document was introduced on the basis of Council Regulation (EC) no 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by member states amended then by 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[9]. Despite the parallel implementation of border security biometric measures, EU citizens are only subjected to a passport authenticity verification. The identification and verification system operating in the EU is called VIS and, with respect to biometrics, involves taking fingerprints from foreigners who apply for an entry visa into Schengen territory[10]. Both the US authorities and the EU legislator emphasize that biometric security aims to increase the level of security, as well as efficiently search for people officially deemed a threat to the state or Community.

Biometric Technology in Private Sector

The above-mentioned systems are merely examples of the use of biometric technology on a large scale in the public security sector. Today, however, biometrics has become equally popular in the private sector.

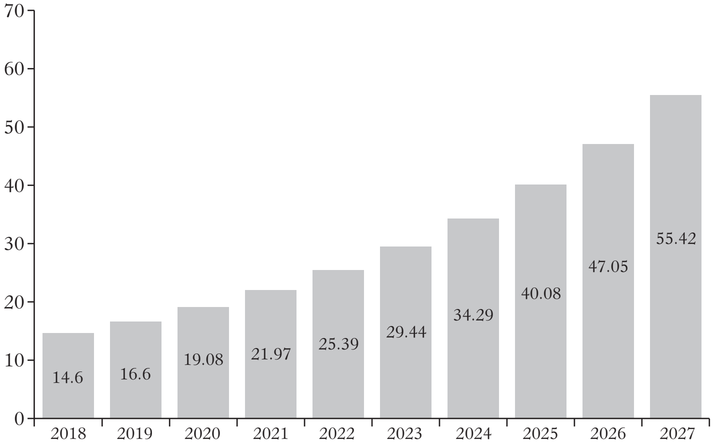
[8] U.S. Department of Homeland Security, https://www.dhs.gov/how-do-i/visit-united-states (4.08.2021).

[9] Council Regulation (EC) no 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by member states, L 385, 29.12.2004; 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, L142, 6.06.2009.

[10] Council Decision of 8 June 2004 establishing the Visa Information System (VIS) (2004/512/EC), L213, 15.6.2004.

This is evidenced by, among others, statistics on current and forecast revenues from the global biometric technology market (Figure 1).

Figure 1. Global biometric technologies market revenue from 2018 to 2027 (in billion U.S. dollars)



Source: https://www.statista.com/statistics/1048705/worldwide-biometrics-market-revenue/

Such popularity of biometric security likely results from advantages cited by users of devices that automatically compare a person's characteristics. The first is certainly an effective identity check with rapid feedback. This goes hand in hand with a high degree of confidence in the correct operation of the device, as the monitor of the comparison process knows the percentage of error the algorithm generates. Additionally, biometrics is convenient for the user, who does not have to remember passwords or a PIN number to confirm access. Biometrics is also the only form of confirming access rights that allows for verification of the identity of an authorized person, rather than merely checking whether that individual possesses specific information (e.g., knows the password). This undoubtedly increases such a system's security, as the password or PIN can be stolen, which is difficult to imagine in the case of biometric identifiers. Due to the discussed advantages, biometrics is very popular in many areas of life. First of all, it is the previously mentioned security industry that uses biometric security to fight crime, including terrorism. In addition to the examples of systems related to the movement of people mentioned above, the use of biometric technology such as national forensic fingerprint databases (AFIS), or the increasingly common systems of population monitoring based on facial recognition are worth mentioning in this context. In the private sphere, biometrics has become very popular, especially in the financial sector. Biometric ATMs or biometric identity verification in a banking mobile application are just examples of the possibilities offered by biometric security. Confidence in the effectiveness of biometric comparison is so high in that realm that the use of such solutions is even required by legislation. An example of this may be Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC[11]. It indicates the mechanism of the so-called 'strong customer authentication' which means "authentication based on the use of two or more elements categorized as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data" (art. 4 (30)). Therefore, biometrics is one of the recommended forms of securing financial transactions. Biometric security is also being used increasingly often in common devices, such as phones, tablets and other electronic devices. It is expected that by 2024, 90% of smartphones will be equipped with software using biometric facial recognition[12]. It is worth considering this particular biometric identifier for a moment, because facial verification is one of the most frequently used features by public and private entities. This is due to the non-invasive nature of the biometric comparison based on the image of the face, as well as the possibility to carry out verification / identification from a distance, even without the knowledge of the individual being identified. This may be particularly important in the case of scanning a crowd (e.g., at an airport). This is evidenced by, among others, statistics on current and forecast revenues from the global biometric technology market (Figure 1); it is estimated that in 2025 this market will reach USD 8.5 billion[13].

[11] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, L337 23.12.2015.

[12] L. Pascu, *Biometric facial recognition hardware present in 90% of smartphones by 2024*, biometricupdate.com/202001/biometric-facial-recognition-hardware-present-in-90-of-smartphones-by-2024, (4.08.2021).

[13] *Facial recognition market size worldwide in 2020 and 2025*, https://www.statista.com/statistics/1153970/worldwide-facial-recognition-revenue (4.08.2021).

Biometric Technology Impact on Society

The implementation of biometrics, while highly effective in identification or verification of identity, may, however, entail serious social and legal effects. The opponents of biometrics point out, first of all, the possibility of violating the right to privacy in the case of collecting biometric patterns. Biometric data is directly related to the human body, and obtaining unauthorized access to patterns will have many more far-reaching consequences than in the case of the theft of a password or PIN. Therefore, the possibility of collecting data should be limited by appropriate legal regulations. An example is the GDPR, i.e. 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)[14]. This EU legal act classifies biometric data as part of the so-called sensitive data catalog, i.e., data, the processing of which is subject to additional restrictions. Data processing in accordance with the GDPR is possible only when one of the grounds for collecting biometric data is invoked (Art. 9). Additionally, sensitive data requires a risk analysis, which consists of determining the impact of data processing on the rights and freedoms of individuals (Art. 35). The EU legislator also introduced three principles for correct processing of collected information: proportionality, accuracy and purpose. Therefore, the processing must firstly be proportional to the purpose that the entity wants to achieve. Proportionality in this regard should be considered in the context of a breach of the right to privacy. In addition, the collected data should be up-to-date and processed only for the purpose for which it was collected. Therefore, the data collected, e.g., for the purpose of issuing a passport, should not be transferred to the police or other services, citing merely public security needs without specifying a reason for requiring the collected information. Such legislation is to protect individuals against unauthorized use of data, as has happened numerous times in the history of the use of biometric patterns. An example is the situation reported by The Guardian in 2017, which described that the FBI, using facial rec-

[14] 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), L119, 4.5.2016.

ognition technology, searched non-criminal photo databases for suspects (e.g. the photo database of people applying for a driving license). The searches took place without the knowledge and consent of the persons concerned[15]. In this context, the basic advantages of biometrics, which are the speed and efficiency of comparison, can become a threat in the hands of authorities that use biometric safeguards to discipline citizens. This is the case in e.g., China, which uses the Social Credit System (SCS)[16]. The SCS awards points to citizens for socially desirable behavior while points are deducted for behavior that is inappropriate from the authorities' point of view. An insufficient number of points results in the inability to perform certain activities, e.g., buy a plane or train ticket, which leads to a significant limitation of individual rights and freedoms. SCS is closely related to the Skynet system[17], which applies biometric facial recognition to quickly identify individuals sought by authorities[18]. Both the American and Chinese examples clearly show that the advantages of biometric technology can be used against the individual under the pretext of ensuring the security of citizens.

A completely different risk stemming from the widespread use of biometric technology is overconfidence in the infallibility of algorithms employed to recognize individuals using their unique characteristics. It is important to remember that every algorithm makes mistakes and the case is no different with biometric algorithms. In the case of biometrics, there can be two types of incorrect verification / identification errors: false acceptance rate (FAR) and false rejection rate (FRR). FAR involves the device incorrectly finding that the compared features are the same. From the perspective of security systems, this error is significant as it may lead to the granting of rights to an unauthorized person who, for example, gets access to rooms they be barred from. The occurrence of FAR from the perspective of the user himself also seems to be dangerous. It may turn out that the data of the person will be incorrectly

[15] O. Solon, *Facial recognition database used by FBI is out of control, House committee hears*, https://www.theguardian.com/technology/2017/mar/27/us-facial-recognition-database-fbi-drivers-licenses-passports (4.08.2021).

[16] K. Li Xan Wong, A. Shields Dobson, *We're just data: Exploring China's social credit system in relation to digital platform ratings cultures in Westernised democracies*, «Global Media and China» 2019, Vol. 4 (2), pp. 220–232.

[17] X. Qiang, *The Road to Digital Unfreedom: President Xi's Surveillance State*, «Journal of Democracy» 2019, Vol. 30 (1), pp. 53–67.

[18] The government might be interested in identifying suspects or in identifying citizens to take away someone's social credit points because of "improper" behavior.

matched with patterns assigned to a wanted or undesirable person in a given country resulting in detention or rejection of access/exit. A practical illustration of FAR is the case of an American, Robert Williams, arrested by the Michigan State Police because he was incorrectly identified by a facial recognition algorithm that recorded a theft[19].

The other error, FRR, occurs when the algorithm finds a mismatch among the compared biometric identifiers, despite the individual's identity actually matching the test pattern. As in the case of FAR, the negative consequences of the occurrence of FRR can be considered both from the perspective of the user and the system security. The user may not be granted due rights (e.g., entering a room) or may be deprived of a specific right (e.g., the right to enter a country). From a system security perspective, an FRR error will mean that a person whose data may be on the wanted or undesirable lists will not be identified as posing a threat. Taking into account the possibility of errors, it should be remembered that the operation of any system using biometric security should be monitored by an authorized individual. Lack of adequate control over the system may decrease the system's effectiveness and may also reduce the level of acceptability for biometric solutions.

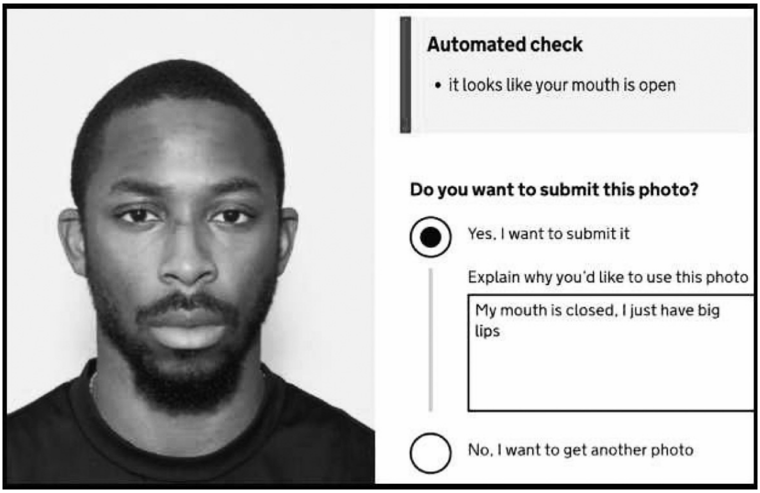
However, there are additional problems with the widespread use of biometric technology. First of all, it is possible that the individual does not have a feature required in the registration process or possesses the feature with a quality that does not allow for correct sampling. It should be noted that this cannot be the reason for refusal to obtain a specific entitlement, e.g., issuing a passport. In this case, it is necessary to implement so-called Emergency procedures that clearly define the procedure to be followed in the indicated situations and allow the use of an alternative solution to biometrics. Applying fallback procedures when the registration process is monitored by an individual does not present any major difficulties. However, the problem arises when the registration process is automatic. An example is the case of a 28-year-old resident of Great Britain, Joshua Bada, who, when applying for a passport, was obliged to upload a biometric photo to the system. The system refused to accept the photo as it found that the applicant had an open mouth on it, which was not in line with the requirements of biometric photography[20]. The

[19] V. Burton-Harris, P. Mayor, *Wrongfully Arrested Because Face Recognition Can't Tell Black People Apart,* https://www.aclu.org/news/privacy-technology/wrongfully-arrested-because-face-recognition-cant-tell-black-people-apart (4.08.2021).

[20] T. Kenney, *'I Just Have Big Lips': Facial Detection System Decried as 'Racist' After Rejecting Black Man's Passport Photo Even Though It Met Required,* Standards https://atlan-

error that the system made was probably due to the lack of proper facial recognition of people of a specific ethnic origin.

Figure 2. A photograph form Joshua Bada application form



Automated check

- it looks like your mouth is open

Do you want to submit this photo?

● Yes, I want to submit it

Explain why you'd like to use this photo

My mouth is closed, I just have big lips

○ No, I want to get another photo

Source: https://atlantablackstar.com/2019/09/22/i-just-have-big-lips-facial-detection-system-decried-as-racist-after-rejecting-black-mans-passport-photo-even-though-it-met-required-standards

However, the problem of demographic bias in security sector biometrics may have farther-reaching consequences than the inability to apply for a visa. As research has shown[21], facial recognition algorithms tend to generate a higher percentage of errors when verifying / identifying people of ethnic origin other than Caucasian. The algorithms make the most mistakes involving women with dark skin tone. Therefore, putting too much stock in the infallibility of biometric technology, combined with a lack of knowledge about an algorithm's bias may lead to misdiagnosis, the consequences of which may be severe for the individual. This is especially so considering the fact that the police used facial recognition algorithms that could be contaminated with demographic bias. In the United States, concerns about the proper operation of facial recognition

tablackstar.com/2019/09/22/i-just-have-big-lips-facial-detection-system-decried-as-racist-after-rejecting-black-mans-passport-photo-even-though-it-met-required-standards (4.08.2021).

[21] J. Buolamwini, T. Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, «Proceedings of Machine Learning Research» 2018, Vol. 81, pp. 1–15.

algorithms have become so strong that the companies that create them have announced moratoria on their use by the police[22].

Biometric Technology – Opportunities and Threats

After the 9/11 attacks, biometric technology appeared to the authorities wishing to fight terrorism as an ideal means of identifying people posing a real threat to public security. Over the last twenty years, biometrics has become an increasingly popular method of supporting the fight against crime, including terrorism. At the same time, biometric security has become a permanent feature of our everyday lives. After analyzing the literature and the legislation it is possible to answer both research questions posed in the article's introduction. Biometric technology gives the authorities the opportunity to identify or verify the identity of the person in a fast and effective way. Their belief in biometric algorithms is seen in introducing systems and documents based on physical features such as fingerprints and face geometry. In consequence it become much more difficult to steel someone else's identity. So biometry has become a way to rise the level of state security.

Apart from the undoubted advantages of implementing biometric identifiers, the consequences that a system malfunction may have for the rights and freedoms of an individual should always be taken into account. The article presented the examples of the problems which may occur letting the algorithm decide without supervision and understanding how the features comparison process works. The moratoria on the use of facial recognition technology by law enforcement agencies allow with even greater certainty to positively answer the second research question that using biometrics devices may have a negative influence on the individuals rights. In consequence it need to be highlighted that only the full awareness of the advantages and disadvantages of biometric technology allows for its proper use, especially in the sphere of public safety.

Bibliography

Buolamwini J., Gebru T., *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, «Proceedings of Machine Learning Research» 2018, Vol. 81.

[22] See e.g. *We are implementing a one-year moratorium on police use of Rekognition*, https://www.aboutamazon.com/news/policy-news-views/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition (4.08.2021).

Burton-Harris V., Mayor P., *Wrongfully Arrested Because Face Recognition Can't Tell Black People Apart,* https://www.aclu.org/news/privacy-technology/wrongfully-arrested-because-face-recognition-cant-tell-black-people-apart/ (24.01.2022).

Gates K., *Identifying the 9/11 'faces of terror'. The promise and problem of facial recognition technology*, «Cultural Studies» 2006, Vol. 20 (4–5).

Gonçalves M., Gameiro M., *Security, privacy and freedom and the EU legal and policy framework for biometrics,* «Computer Law & Security Review» 2012, Vol. 28 (3).

Kenney T., *'I Just Have Big Lips': Facial Detection System Decried as 'Racist' After Rejecting Black Man's Passport Photo Even Though It Met Required,* Standards https://atlantablackstar.com/2019/09/22/i-just-have-big-lips-facial-detection-system-decried-as-racist-after-rejecting-black-mans-passport-photo-even-though-it-met-required-standards (24.01.2022).

Li Xan Wong K., Shields Dobson A., W*e're just data: Exploring China's social credit system in relation to digital platform ratings cultures in Westernised democracies,* «Global Media and China» 2019, Vol. 4 (2).

Mayhew S., *History of Biometrics,* https://www.biometricupdate.com (24.01.2022).

O'Connor S., *Biometrics and Identification after 9/11,* «7 Bender's Immigration. Bulletin» 2002, Vol. 7.

Pascu L., *Biometric facial recognition hardware present in 90% of smartphones by 2024,* biometricupdate.com/202001/biometric-facial-recognition-hardware-present-in-90-of-smartphones-by-2024 (24.01.2022).

Qiang X., *The Road to Digital Unfreedom: President Xi's Surveillance State,* «Journal of Democracy» 2019, Vol. 30 (1).

Solon O., *Facial recognition database used by FBI is out of control, House committee hears,* https://www.theguardian.com/technology/2017/mar/27/us-facial-recognition-database-fbi-drivers-licenses-passports (24.01.2022).

Terhörst P. et. al., *A Comprehensive Study on Face Recognition Biases Beyond Demographics,* «Journal of Latex Class Files» 2015, Vol. 14 (8).

Zureik E., Hindle K., *Governance, Security and Technology: the Case of Biometrics,* «Studies in Political Economy» 2004, Vol. 73.