ATTITUDE CHANGE TOWARDS BIOMETRY BETWEEN 2006 AND 2016

A BIOMEMTRIÁVAL KAPCSOLATOS ATTITÜDVÁLTOZÁS 2006 ÉS 2016 KÖZÖTT

FÖLDESI Krisztina; KOVÁCS Tibor

(ORCID: 0000-0001-5867-9958); (ORCID: 0000-0001-7609-9287)

foldesik@fejer.police.hu; kovacs.tibor@bgk.uni-obuda.hu

Abstract

Utilisation of technical novelties is continuous within the police organisation to make the police work more reliable. An example of this is the personal identification based on fingerprints, which was first used in law enforcement. The ongoing development of biometry, the use of 21st century technical novelties in police activity would mean further support in making the police work more efficient and high-standard. The only question is: what methods and control mechanisms will society accept, and to what extent the police force itself will support and accept the general use of these methods and mechanisms. This work contains the analysis of two studies and multiple investigations aimed at answering this question.

Keywords: safety and security, identification, personal identification, biometry, fingerprint, police

Absztrakt

A rendőri munka megbízhatóbbá tételének érdekében a technikai újítások alkalmazása a rendőri szervezeten belül folyamatos. Ilyen például az ujjnyomat alapján történő személyazonosítás, amelynek elsőszámú felhasználási területe a rendészet volt. A biometria szakterületének további fejlődése, a XXI. századi technikai nóvumok felhasználása a rendőrségi területen további támogatást jelentene a rendőri munka hatékonyabbá, színvonalasabbá tételében. A kérdés csupán az, hogy milyen módszerek, és milyen ellenőrzési mechanizmusok alkalmazását fogadja el a társadalom, és maga a rendőri állomány milyen mértékben támogatja, fogadja el azok általános alkalmazását. E kérdés megválaszolására lefolytatott két kutatásés több vizsgálat, elemzés összegzését tartalmazza e munka.

Kulcsszavak: biztonság, azonosítás, személyazonosítás, biometria, ujjnyomat, rendőrség

INTRODUCTION

Biometric procedures gain more and more ground also in the modern, application oriented technical scene. This is the situation in both the private and the public security sector. To determine the utilisation practice and developmental directions of biometric devices, it is crucial to study what changes occurred in the societal acceptance. The significance of biometrics based personal identification has particularly grown in the second millennia. The COUNCIL REGULATION (EC) No 2252/2004 of the European Union (adopted in December 2004) orders the Member States to include biometric identification information into the concerned documents, after the adoption of common technical and security requirements. In its commission decision from 28 June 2006, the EU determined the common requirements of second generation passports containing digitalised fingerprints. Furthermore, the EU also determined a deadline for implementation: 36 months. The European Union supported the development also through financial means, Hungary received close to HUF1 billion for this cause, thus starting June 28 2009, all passports issued contain fingerprints as well. The borderless nature and fear inducing characteristic of International terrorism and crime play a role in this [1]. In the course of crime investigations, we face countless new threats, and methods of perpetration, which supersede the opportunities provided by traditional investigation techniques and security systems. And after 9/11, a whole new era of safety and security began. From that time on, biometric data has been claimed to be the only and categoric method for establishing public safety and security. It is regarding this topic we conducted our research in the 2006-2016 period.

COMPARATIVE STOCHASTIC ANALYSIS OF RESEARCH RESULTS FROM 2006 AND 2014 CONCERNING AVERSIONS TOWARDS BIOMETRIC IDENTIFICATION [4]

A frequent point in social sciences is that whether in a base population providing different samples, the value of a variable X is generally the same in the groups providing the samples. Because in such cases we are working with quantitative variables the value range of which only meets the criteria of ordinality. We get such a variable for example, if we ask the test subject to judge on a scale of 1 to 5, how much s/he supports the practical usage of a procedure. And according to some people's approach, the comparison of size levels in such a case using the average is ambiguous, and the results are questionable. It is this problem, to which the method of stochastic comparison provides a solution. Concerning a variable X, stochastic equality can be defined between two populations if $P(X1>X2)=P(X1<X2)$ is true, i.e. X1 and X2 from the two populations are the result of two observations chosen randomly, and independent from one another. Basic concepts here are stochastic equation (StE) and stochastic homogeneity (StH). Thus, through the generalisation of these, we can determine the stochastic compliance of more than two base populations.

   In order to concretise these processes, we performed a comparison of the research projects completed in this field: both of them had been conducted at the University of Óbuda. The 2006 study was done at the predecessor in title, Budapest Technical College, Donát Bánki Faculty of Mechanical Engineering, Institute of Mechanical Structure and Security Technology, Security Technology Lab [2], and we personally conducted the 2014 study at the Doctoral School of Security Sciences [3], and involved security sciences majors as well as professional police officers.
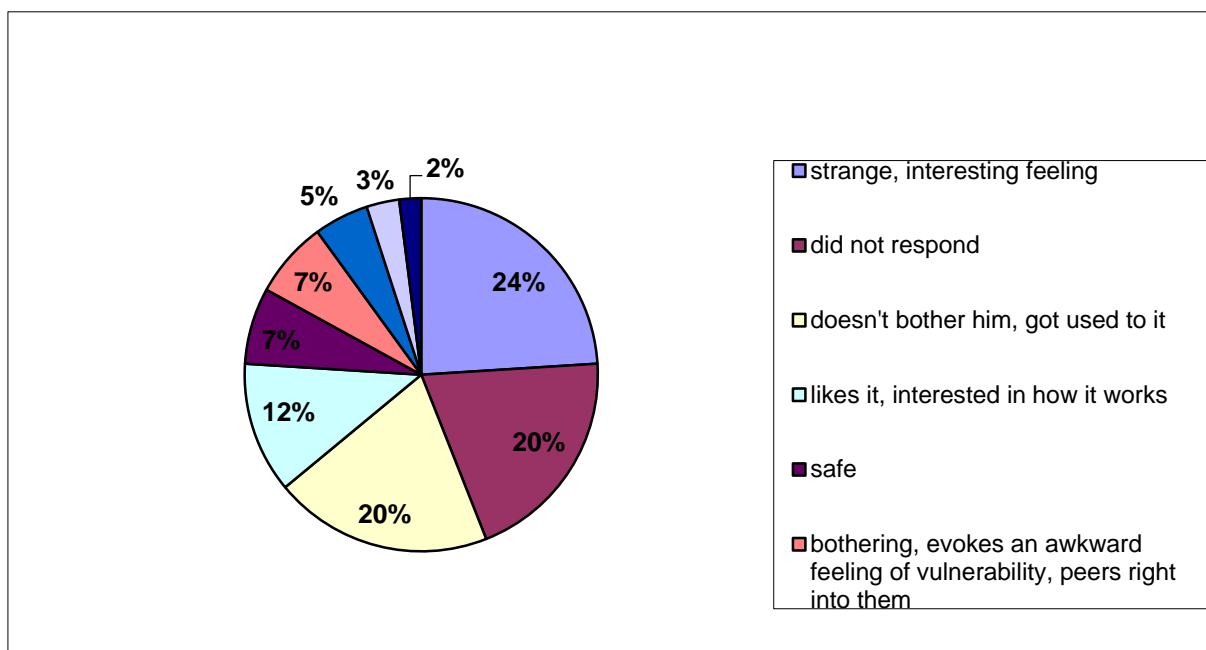
   Due to the societal background at the time of the 2006 research, the utilisation of biometric identification technology was considered relatively new. A largely incomplete legislative background, smaller technological repertoire, less practical experience in usage, but large installation and operation cost were to be expected in application. Based on the operation in

the professional field of the last 8 years, we can make statements of great significance concerning professional work as well. The 2006 research sample involved 59 people, which increased to 333 in 2014. To have the most nuanced conclusions possible and to get more solid results, we had created another control group composed of police officers beside the students, inevitable for the objective assessment of the situation. In the indicated period, 153 police officers from the Fejér County Police Department filled in the questionnaire (with the base population counting 924 police officers on duty). Student respondent count was 180.

Both researches presented a custom made questionnaire, which was filled in voluntarily and anonymously. In both instances, the questionnaire contained closed, attitude measuring questions to determine the sentiments in question.

To enhance the objectivity of the results and to clarify eventual cognitive dissonances, we integrated four questions requiring essay-like answers into the 2014 research. (60 students detailed their opinion on four questions of the questionnaire, with the help of which we gained accurate information on the value indicated in the attitude range).
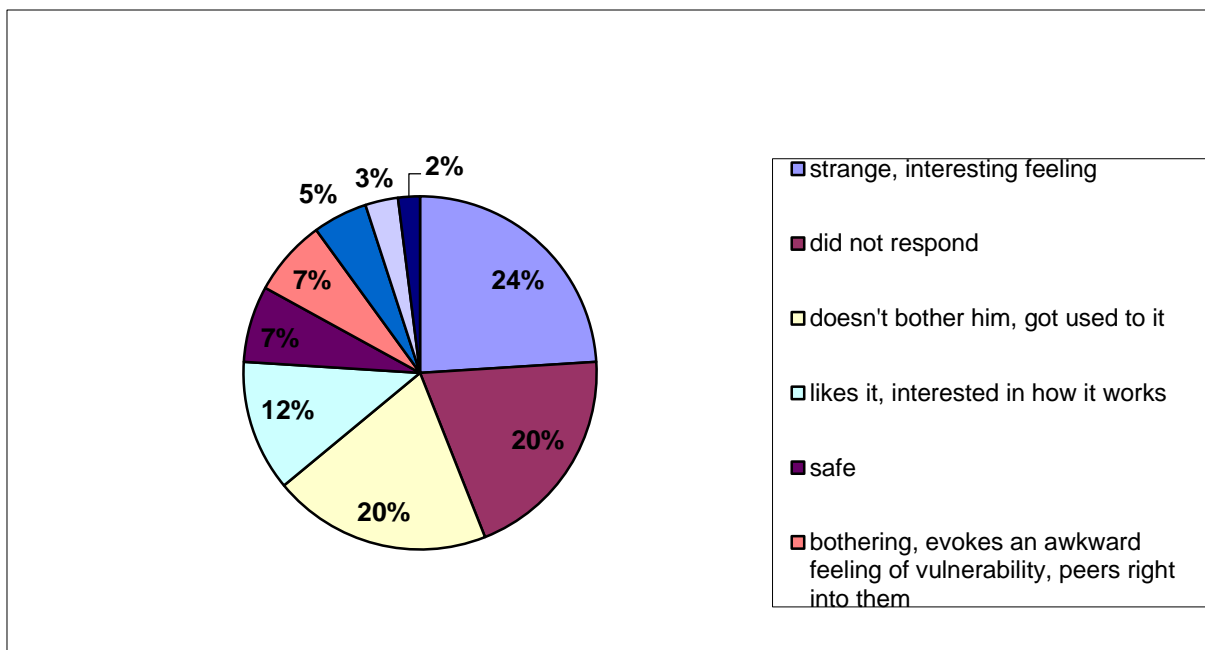
One of the central topics of the studies was: which emotional and mental attitudes are triggered in users by the use of biometric systems?

Figure 1 Emotional and Mental Attitudes Towards Access Control Systems (source: SUPLICZ, S. - FÜZI, B., 2006. [2])

According to the analysis of the 2006 source (**Figure 1**) 70% had a positive, accepting attitude, 20% did not answer, and 10% had a disapproving opinion due to bad feelings or slowness.
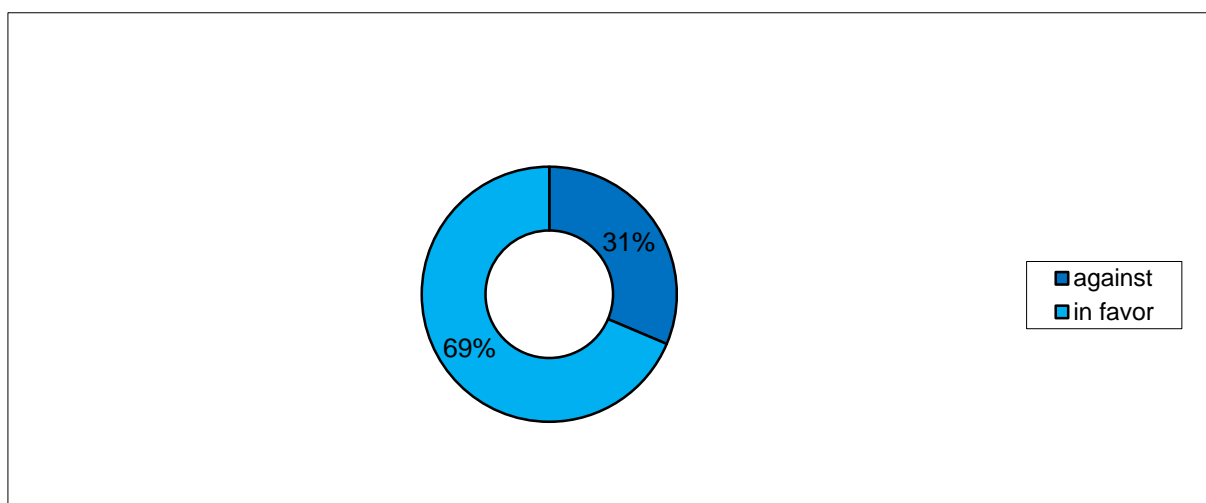
Relating to the usage of the biometric system, the results of the 2006 research showed 71% of all respondents stating that they fully trust the biometric system, and support its application (**Figure 2**).

Figure 2 Attitude towards the use of the biometric identification system (source: SUPLICZ, S. - FÜZI, B., 2006. [2])

A significant conclusion is that only 2% out of the 7% being averse were expressly rejecting the system. The above results allude to the great popularity of the product, since even a lot of those gave an accepting answer, who were concerned about the system from a privacy protection or emotional point of view. All these could be considered as very good results concerning a new system used for the first time.

It was this question to which a point in the 2014 research intended to find an answer for, namely, to what extent do the respondents support the introduction of biometry based systems. Since the age composition of the police force shows 55% in the 18-35 range, it is important to weigh the opinion of this age group in a proper manner (**Figure 3**).
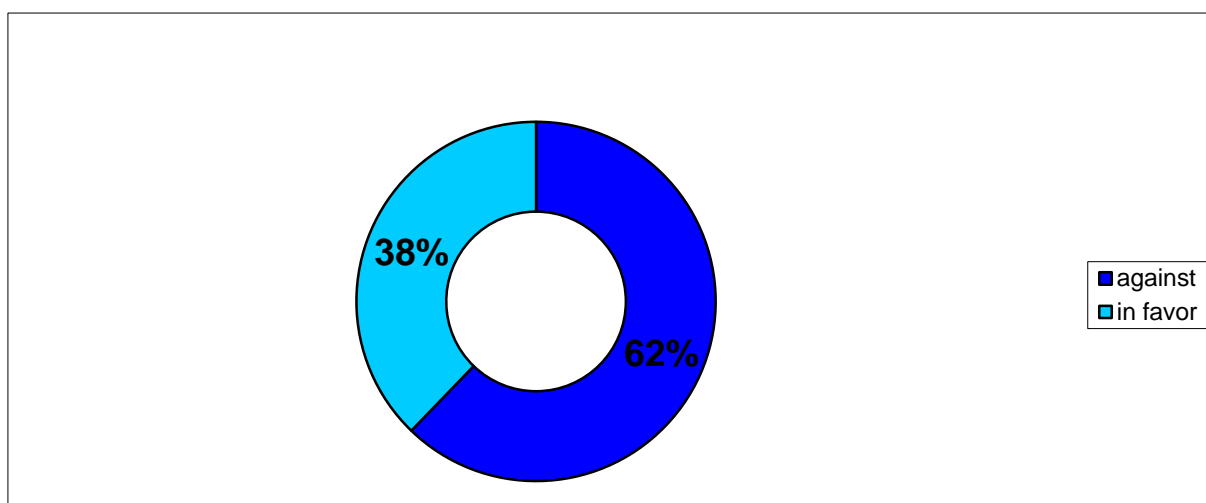

Figure 3 Attitude of police officers 18-35 years of age towards biometry.

It immediately became clear that not only did the 2006 results fail to become more positive and accepting in the eight years passed, but they turned fully rejective towards biometry considering that 31% of police officers is against the application of biometric identification procedures. This result is articulated even more by the fact that such high proportion of

rejection appears in a social group, where the application of certain components is job duty, and the eye-catching results of the efficient operation of these technologies are clearly visible.

The outcome of the survey conducted among university students unambiguously supports the above statement (**Figure 4**).

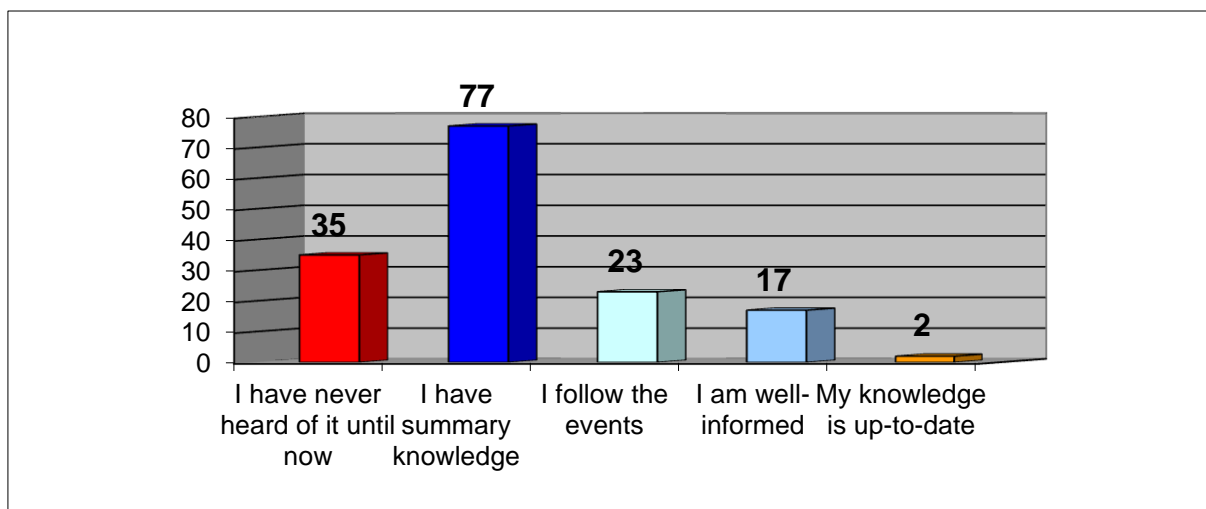**Figure 4** Attitude of university students towards general capture of biometric data.

Concerning the common aversion towards biometric device system, 62% of the respondents from university population unequivocally rejects these, and absolutely disagrees with the general scope, all-inclusive usage of these. Thus, it can be ascertained that the university population is in total rejection towards any kind of control, rule and checking.

Sixty of the students from the University of Óbuda, Donát Bánki Faculty of Mechanical Engineering and Security Technology left a detailed essay-like opinion concerning the statements 1 to 4 of the questionnaire (see further down). Formation of opinions was conducted in groups of six. Based on these, we received a more nuanced and, in a way, altered result concerning the above question.

They first examined the question of the universally required electronic fingerprint registry. From the ten groups formed, five groups supported it with conditions, and five groups categorically dismissed the possibility of a universal fingerprint registry. Then again, if we look at the detailed answers, we see that nine groups would not support the establishment of this. This fact seemed, as a matter of fact, to verify the statement that university students reject any manifestation of control on themselves, although the 69% measured in the questionnaires produced 90% here.

Analysing the justifications however, I ascertained that in many cases rejection appears for merely technical reasons. Since in their studies university students concern all forms of biometric identification in detail and thoroughly, they are also aware of the technical background of these. They also clearly see the incompleteness of the different procedures.
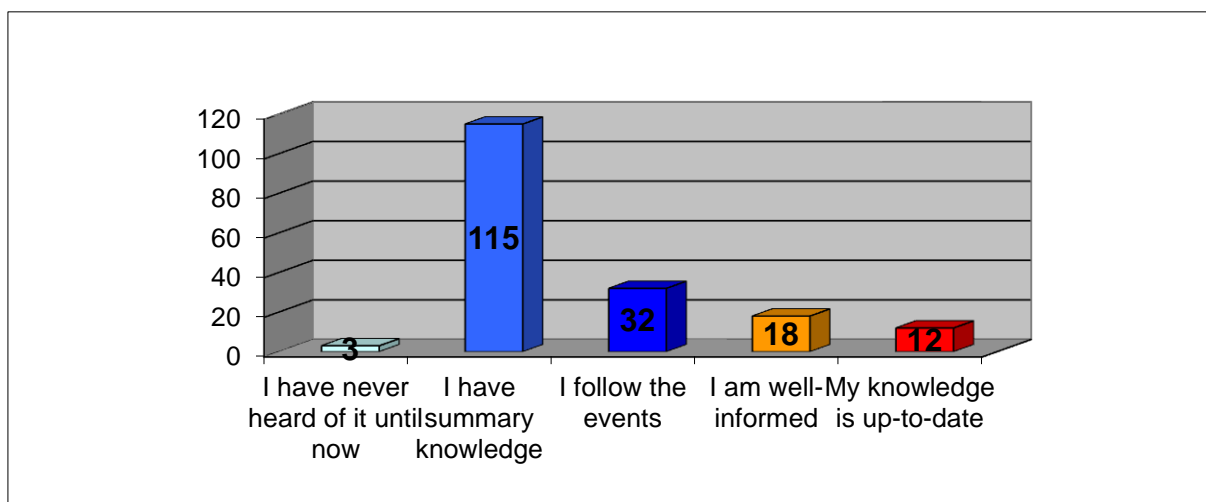
To the question of what level of knowledge do you have concerning biometry, I received answers from the professional police officers in the 2014 research refuting my hypothesis. Because I assumed that they possess far more knowledge than average people regarding biometry (**Figure 5**).

Figure 5 Knowledge level of the Fejér County Police Department police force regarding biometry.

23% of respondents did not even hear of biometry until now, and according to themselves do not have any knowledge concerning this discipline. The largest portion of police officers, 49% stated that they only have summary knowledge in this field. It is also a big problem that only 2% of the 153 respondents claimed to be well-informed in this topic. This fact is also thought-provoking because dactyloscopy, face recognition, and DNA-identification constitute an integral part of police force's basic education, and if the police force with an occupational duty to deal with biometry possesses such little knowledge in this field than the knowledge proportion amongst civilian population is even lower.

The knowledge level of university students involved in the 2014 research proved to be much higher (**Figure 6**).

Figure 6: Prior knowledge of university students regarding biometry.

30% of respondents stated that not only are they well-informed and are following the events in the world of biometry, but their knowledge is up-to-date. This is understandable, since they are Security Technology majors. Then again, the remaining 70% of "specialists" having only summary knowledge is an unexpectedly high proportion.

Examining the 8 years passed between the two studies, based on the above, it can be ascertained that no progress was made in improving society's knowledge level regarding biometric identification. In 2006, 31% answered that they did not have any substantial

information on iris identification / biometric identification, the remaining 69% also only possessed filtered information, incomplete knowledge. In 2014, the proportion of those not able to even explain what biometry is was 23% among police officers, and 49% only had very minimal knowledge in this field. That is, 71% of police officers did not know anything about biometric identification. The 30% knowledge level of university population can also not be considered an advancement, with the other 70% producing only summary knowledge.

The low knowledge level of the population providing the samples also has a major effect on other issues relevant to this field, and on the development of attitudes towards these issues. Evidence to this is presented in the justifications provided by the university students; e.g. in the second essay point, which was focused on the willingness to support the recording of iris recognition data of new-borns after delivery. Basically, the groups unequivocally stated that they agree with the application of this biometric identification method. However, they only agreed considering its reliability. A face recognition system is capable of sending a signal based on the criminal records, if a person wanted or only monitored by the police enters the district. Practically, it is able to connect to population registry data, where beside our personal data, our digitalised photos are kept as well. Thus, anyone possessing such a professional system can monitor the chosen individual – who, of course, may or may not be a criminal –; i.e. where, when, with whom and why s/he goes, what habits, illnesses, phobia etc. s/he has. Therefore, the technology itself is capable to create anyone's personality profile, which is clearly prohibited by numerous international treaties and regulations (e.g. Council of Europe regulation [5]). This system using a face recognition software is already part of Hungarian reality [6]: The Ministry of Interior installs camera systems using face recognition software in a HUF12 billion project and the National Security Service (NSS). The media and journalists, together with multiple human rights organisations termed this initiative a "cheeky face recognition" and the term "Orwell-land" was used in connection with it [7]. In their opinion, 1984 of our nightmares seems to be coming true, the possibility of the almighty "Big Brother", who sees all, who treats all ordinary people as subordinates, uses and exploits them according to its own interests.

Beside all of the above, we have to remark that a strong influence of the media was palpable in the case of students, namely the effect of numerous series on television portraying police investigation, and mustering techniques of securing evidence. Even in the population well-versed in this topic, these resulted in events of imagination. Regarding fingerprints, four groups remarked that they do not really support the universal capture of these because it is data easy to steel, and the fingerprint of an innocent person, or a fraction of it, can easily be placed in a crime scene, in order to have that person identified as the perpetrator.

The third statement concerned the establishment of a face recognition database, in order to monitor the movement of criminals in public places. Six groups elaborated in their opinion that they completely disagree with this proposal. The first and foremost reason for their decision was the unreliable nature of this method. Secondly, they argued that because this lack of reliability, a lot of false positive identifications would occur, through which honest people would be accused of crimes. There was a group that rejected the method referring to personal rights once again, since also people would be monitored, who only walk by the camera accidentally, and so their data could be manipulated.

THE QUESTIONNAIRE

Respondent's Sex: Male   Female

Respondent's Age: below 18   18 – 35 years   36 – 55 years   56 and above

Respondent's Highest Degree: Primary School   High School   Higher Education

Please read the following statements, and using the grades below indicate how much you agree or disagree with them.

1	2	3	4	5
Completely disagree	Slightly disagree	Neutral	Slightly agree	Completely agree

1. **I support the expansion of electronic fingerprint registry to all men and women.**   **1 2 3 4 5**

2. **I agree with collection and retention of iris recognition data of every child at birth by the police.**   **1 2 3 4 5**

3. **I agree with the establishment of a face recognition-arrest warrant database, with the help of which monitoring of faces involved in crimes becomes possible.**   **1 2 3 4 5**

4. **I agree with the police registering the DNA-sample, fingerprints and face recognition data of abusers (sexual abuse of children) and people committing deliberate homicide.**   **1 2 3 4 5**

5. **I agree with the police registering further biometric data (DNA, iris, vein pattern, etc.) of any person committing any deliberate crime, on top of their fingerprints.**   **1 2 3 4 5**

6. **I do not support the DNA-sample registration of every child at birth.**   **1 2 3 4 5**

7. **I support the face recognition and police registration of people committing robbery and other crimes against property.**   **1 2 3 4 5**

EFFECT OF A SUCCESSFUL APPLICATION ON ACCEPTANCE

Beside theoretical education, the University of Óbuda, Donát Bánki Faculty of Mechanical Engineering and Security Technology puts great emphasis on armouring students with as much practical experience as possible. In this effort, a hybrid access control system (biometric ID and chip) was established on the Campus in Népszínház Street, and has been operated by the school for multiple years. Following technological developments, there are new components introduced to the system from time to time, complementing, or in some cases, replacing the former technology used.

The system was installed in 2010 with the purpose of providing access control based purely on biometrics. However, the fingerprint reader crashed after capturing 1,000 users, despite the fact that the manufacturer's device specifications indicated handling of 10,000 samples (the total number of users is around 4,500). After some thorough examinations, the professional leadership decided to limit the fingerprint-based access control to 400 people, and to meet further access control needs using chips.

In 2015, we decided to replace the fingerprint recognition device with the palm vein recognition ("vein scanner") system used in the Groupama Arena, which by then had outgrown its minor initial flaws. The developer was also very keen on providing us with two

devices, because in the school building, there's a constant strain on the device, while in the stadium it is "floodlike", and so, gathering information of day-to-day use becomes possible.

The device accepting 500 users quickly became popular, since it answered a lot quicker than the former fingerprint recognition device (the pass-through time practically became comparable with that of the chip method), it worked with low levels of false rejections (around 1%), and it is quite comfortable if one does not need to grope around or go back for the access card, etc.

In 2016, we purchased licenses for another 700 people, thus our biometric access control capacity rose to 1,200 users. Although, based on our continuous assessments, the false rejection rate increased slightly, but this could be traced to application error in practically all cases (mostly, it was wrong positioning of the palm on the detector). The popularity, feasibility, and ultimately, the acceptance of this biometric identification method is shown by the fact that we managed to fill the user limit on a strictly voluntary base in a matter of a few days.

SUMMARY

As a conclusion, we can state that there are still some questions left regarding the practical applicability of biometric identification systems. Numerous misbeliefs, legends and false notions are distorting people's opinion concerning this. It is unfortunate that public opinion is often based on incorrect information from the wrong source, as a consequence of which their perspective evolves in the wrong direction, and the results of the two studies have shown the aftermath of this fact in a palpable way by demonstrating that during the eight years passed, members of society had not received appropriate information concerning biometry. This resulted in knowledge deficiency and uncertainty, and ultimately, in aversion and fear towards the use of biometric devices.

The most important component in this aspect is the use of correct terminology, conveying accurate information, and public disclosure of newest technology, in order for the larger public to have an accurate and precise idea of the current technical opportunities an capabilities of biometric identification.

It can be ascertained as a basic fact, that today many have already heard about the concept of biometry, however, its set of tools, and potential uses remained unknown to them. Our finding that, according to themselves, 23% of the people serving in law enforcement never even heard of biometric devices renders this topic especially sensitive. Another 49% has only summary knowledge of biometry. Their knowledge is summary, incomplete, however, this knowledge evokes fear and distress. The ongoing specialisation, and perfectioning of biometric devices, and also the expansion of utilisation areas are not followed by the information need, and information processing of those concerned. They might very well know of certain new biometric devices, but they fail to comprehend the practical applicability of them. A particularly sensitive point of this system is the field of law enforcement, where personal identification based on biometric features would render the subjective element of performing personal identification for the purpose of law enforcement in a traditional way – based on anatomic features containing high probability of error – controlled.

The fact that more than one-fifth of police officers had not even heard of biometry questions also the efficacy of police's basic training. Since an organic part of it is learning the elements, steps and basic concepts of dactyloscopy, face recognition and DNA-identification.

However, half knowledge in this topic serves only fear mongering and spreading hysteria, where in sci-fi like everyday life, the chosen ones hold biometry-based personal observation in their grasp, and play with individuals like with puppets.

In can be ascertained that individuals have a great need for safety and security, even if it means a minor curtailment of their freedom. In this regard, police officers have more

categorical, unambiguous opinion on biometric devices, which they see applicable in a more stringent manner and in a wider range than university students. In the end, also when taking all seven questions into consideration, it can be stated that the opinion and attitude of the police force is completely unequivocal, not influenced by the respondent's sex: all possible and already developed area and device of biometry is deployable and to be deployed in fighting crime, and the creation of public safety and security.

Based on our research and examinations, it could be confirmed that the need for safety and security is a relevant issue in all age categories, on all levels of education and both sexes. Then again, immense anomalies can be observed in the applicability of biometry. There is a consensus on the necessity of its application in registering and identifying criminals. Then again, the rejection observed in other cases, to a great extent, may be traced back to knowledge deficiencies. Thus, spreading more thorough and reliable information to a wider audience, and the precise, professional and all-encompassing creation of legal framework are primary tasks.

Tasks to improve the acceptance of biometric identification

Comparing the result of studies, examinations and analyses, it can be stated as a fact that the acceptance of technologies using biometric data was becoming worse in society up until the recent years. Being aware that the base population providing the sample is the user of these techniques, is familiar with them, and would be interested in a more successful application of theses in his/her everyday work, this result is even more significant. Then again, the 38-31% rejection rate compared to the 2% from 2006 makes it clear that the professional forums, practical work and information spreading in this field are not sufficient, misinformation and disinformation may occur, and forums conveying reliable, relevant information, technical specifications and innovations in a credible manner are completely missing. These forums – organized and working on a professional basis – will have a basic task split into four segments:

1. It is clearly necessary to immediately rectify and correct false information, which is entirely missing regarding this discipline.
2. The next element in public relation activities is making the outward communication of the discipline credible, professional and unified.
3. Missing harmonisation of law on an international level must be performed, subsequently, the legal framework of uncontrolled, excessively controlled or not properly controlled areas must be created and adopted.
4. Fourth, but indispensable task is to narrow the scope of the discipline, and to make it professional, in the course of which all "charlatans" doing unprofessional and technically insufficient work are done away with from the circle of professional teams installing biometric identification access control systems. This activity, of course, can only be done through elected professional bodies comprising credible individuals.

Independent from the criminal statistics, it is also a societal expectation and the need of people irrespective the type of settlement they live in, to be able to live their everyday life peacefully, free of crime, knowing that their children and they themselves are safe and secure. Also in the course of the European Union's law making and framework creating activity, public safety had been declared, and was worded in the Amsterdam Treaty adopted on 2 October 1997, and effective as of 1 May 1999. They defined creation of an area of "Freedom, Security and Justice" as the central objective (neither the Maastricht Treaty, nor the Amsterdam Treaty provided a definition for the area of freedom, security and justice).

The Fundamental Law of Hungary itself also enunciates this basic right [8]. Then again, it is important that we have a precise idea of the level of freedom society is willing to sacrifice in order to make everyday life more secure. Of course, we also have to be aware of the conclusions that biometric identification is not a "silver bullet", as many claimed it to be, e.g. in the fight against terrorism, or in crime prevention, but it surely needs to have a much more relevant role in creating public and private safety, in the implementation of which the largest responsibility falls on the professionals of this discipline.

BIBLIOGRAPHY

[1]   http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/HU/index.htm; letöltve: 21 June 2012

[2]   SUPLICZ, S. - FÜZI, B.: Study of Attitudes and Aversive Reactions Evoked by an Access Control System Using Iris Identification, a treatise, Budapest Technical College, Donát Bánki Faculty of Mechanical Engineering, Institute of Mechanical Structure and Security Technology, 2002

[3]   FÖLDESI, K. - KOVÁCS, T.: Study of Aversions Towards Biometry among Police Officers and University Students, a treatise, University of Óbuda, Doctoral School of Security Sciences, 2014

[4]   VARGHA, A.: Comparison of Independent Samples Through New Ranking Procedures http://www.ksh.hu/statszemle_archive/2002/2002_04/2002_04_328.pdf; downloaded: 01 December 2013

[5]   Munkaanyag a biometriáról - Working document on biometrics Adopted on 1st August 2003 by ARTICLE 29 - Data Protection Working Party MARKT/10595/03/EN, WP 80 www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp80_en.pdf

[6]   http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/HU/index.htm; downloaded: 12 October 2014

[7]   www.jozsefvaros.hu/hir/1965/kocsis_mate_a_biztonsag_mellett_tette_le_a_voksat/; downloaded: 02 October 2014

[8]   Fundamental Law of Hungary, *Article IV* "(1) Everyone shall have the right to liberty and security of the person."