REDUCED-PARAMETER BIOMETRIC IDENTIFICATION CAPABILITIES TO PROTECT CRITICAL INFRASTRUCTURES AND SPECIAL OBJECTS

CSÖKKENTETT PARAMÉTERŰ BIOMETRIKUS AZONOSÍTÁSI LEHETŐSÉGEK A KRITIKUS INFRASTRUKTÚRÁK ÉS A SPECIÁLIS OBJEKTUMOK VÉDELMÉNÉL

KOVÁCS Tibor[1] – UJHEGYI Péter[2]

Abstract

The identification parameters of biometrics are decreased severly due to protection devices. In this article, keeping the focus on biometrics, I will conduct a theoretical examination of possible biometric identification solutions for critical infrastructures and certain special objects. In the theoretical study, I take into account the fact that due to the COVID epidemic, the number of measuring points used in biometric identification, i.e. the number of identification parameters, is significantly reduced in some identification solutions. We wear masks that inhibit the effectiveness of facial recognition tools and algorithms, or we use facial protection that protects our eyes, which can put us at a disadvantage with various optical solutions. Rubber gloves are used in many areas, but it can be a difficult and possibly exclusionary factor when using a hand geometric or palm vascular identification solution. These few examples show that the possibilities of biometric identification are limited in these circumstances.

Keywords

critical infrastructure, biometric identification, protection of water bases, entry, identification solutions, pandemic, identification, authentication, AI

Absztrakt

A védelmi eszközök használata miatt az azonosítási paraméterek számának csökkenésének hatása a biometrikus azonosítási megoldásokra. A cikkemben a biometrián tartva a fókuszt, elméleti oldali vizsgálat alá vonom a lehetséges biometrikus azonosítási megoldásokat a kritikus infrastruktúráknál és egyes speciális objektumoknál. Az elméleti vizsgálat során figyelembe veszem azt az aktualitást, hogy a COVID járvány miatt a biometrikus azonosítás során használt mérési pontok, azaz az azonosító paraméterek száma az azonosítási megoldásokban jelentősen csökken. Maszkot hordunk, ami gátolja az arcfelismerő eszközök és algoritmusok működésének hatékonyságát, vagy olyan arcvédelmet használunk, ami a szemünket is védi, emiatt hátrányba kerülhetnek az optikai megoldások. Számos területen gumikesztyűt alkalmazunk, ami kizáró faktor lehet egy kézgeometria, vagy egy tenyér érhálózat azonosítási megoldás használatánál. Ez a pár példa is megmutatja, hogy a biometrikus azonosítás lehetőségei beszűkülnek ilyen körülmények között.

Kulcsszavak

kritikus infrastruktúra, vízbázisok védelme, beléptetés, pandémia, személyazonosítás, hitelesítés, AI szabályozás

[1] kovacs.tibor@bgk.uni-obuda.hu | ORCID: 0000-0001-7609-9287 | associate professor, Óbuda University | egyetemi docens, Óbudai Egyetem

[2] ujhegyi.peter@phd.uni-obuda.hu | ORCID: 0000-0001-9143-6712 | PhD student, Doctoral School on Safety and Security Sciences | doktorandusz, Óbudai Egyetem

INTRODUCTION

I was outraged to read an article the other day about a hacker, in a Florida town attacking the city's water purification plant and trying to poison the population of a city by multiplying the amount of sodium hydroxide, or alkaline, through a water purification station [1]. Fortunately, the operation did not succeed, but it is terrible to imagine what a disaster it could have been if the water supply infrastructure of a large city, or even a town of a few hundred or a few thousand people, had been the victim of an attack by bad-wishers. The reason I was so touched by this news, other than that such an act, or even thought, is hair-raising, because in one of my previous articles [2] in my doctoral studies, I highlighted the importance of protecting water resources and water bases. Although the Hungarian Government has already identified critical infrastructures for the provision of drinking water facilities, which must be given special care primarily in the fight against terrorism in order to protect civilians [3], if we believe in science and that drinking water will be the greatest asset of the next century, then more emphasis should also be placed on protection.

One of the effects of climate change is a drier climate and a decrease in precipitation. As riverside settlements spread and agriculture is on the rise, flooding areas are falling. Due to food constraints, water consumption has slowly reached unsustainably high levels, in proportion to the rapid growth of developing agriculture, textiles, food and many other industries. These are just a few facts as to why clean drinking water is our most important asset, but it is also a good feeling how at our service, because our lives are based on high water use. Such an important and vital resource could be a logical target for terrorists. In my opinion, the development of recent years in it and biometric identification solutions provides an opportunity to see which uses can benefit from them.

The attack on the aforementioned water treatment station was an attack on an IT border protection solution. In the current pandemic situation, more people are working remotely (Home Office), which necessitates the creation of remote access links, which open up new avenues and additional attack possibilities for hackers. The operator's machine, working from Home Office is much less protected on the home network, usually than the office, making it a much easier target for attacks. Of course, there are endpoint protection solutions that define and force rules and protection levels for the office environment in a home environment, and so-called VPN solutions that establish a special and secure connection between the operator's home computer and the other endpoint (well-protected workplace) through firewall systems, but it would also be necessary to include multi-factor identification solutions behind these solutions. An essential element of this, and unfortunately due to the increasing number of attacks, could rightly be expected that one of the factors of identification should be biometrics. Biometric identification clearly ensures that the authorised, identified person actually performs the task at the moment.

TYPES AND MEASURES OF BIOMETRIC IDENTIFICATION

It is important to distinguish between identification and authentication. We are talking about a type 1:n identification when the currently measured biometric sample ("1") is compared with all the samples stored in a database ("n") and if there is a match, the identity of the requester is established and, say, an entry takes place. So we have put together a sample with a set of data from a lot of people. A key part of this process is that the legal

conditions for storing biometric templates and samples must also be fulfilled, since the biometric template is considered personal data and is subject to appropriate regulation in order to protect personal data. During authentication ("1:1"), a template ("1"), i.e. a biometric data, is stored and compared to the pattern currently taken ("1"). For this method, we examine whether the person belonging to the sample in particular and stored is right there and gives the biometric sample at the moment of identification. This authentication process is used by our mobile phones for biometric verification if we enter the device or want to bank, or if we would like to pay, but from the point of view of the process, this includes how the biometric data stored by our passport is used. So the match between the newly taken sample and the sample previously stored is examined by this method.

The authentication process is usually much faster because you don't have to compare hundreds, thousands, or even millions of database records, and protecting a database with a lot of sensitive data is not a big risk because that is not how we store the data.

An important feature of the identification process and the biometric measurement solution used are the FAR and FRR values. The False Acceptance Rate (FAR) indicates the number of cases in which an unauthorized user is identified as an authorized user during enrollment. FRR (False Rejection Rate) seems less problematic than this indicator, i.e. the rejection of eligible users.

For identification solutions, the number of biometric characteristics captured by the technology used is also a characteristic consideration. The number of recorded data varies widely, we are talking about 15-35 points for a fingerprint, but a palm network-based solution can record up to 5 million reference points. Biometric solutions companies have their own professional ”know-how”, about how many of the data they record are accepted for successful identification and how much is at the limit where the process is rejected. The pandemic situation in the 2020s and 2021s is even more problematic because of the number of distractions that can affect the transmission of a successful sample. Before explaining this, let's look at the methods of identification and the interfaces that biometric identification can have in critical infrastructures or object security, including special objects, and how this changes in the pandemic situation.

Fingerprint, palm print biometric identification

The furnishings of the skin, on the surface of the finger or palm are made up of so-called frills and frill lines. It is one of the oldest biometric technologies due to its early use in law enforcement, so it is quite accepted and widespread. In the process, we measure 15-50 external features, but it is usually not contactless technology, so the detector needs to be disinfected continuously. The pattern can be easily copied because it may unwittingly remain on the suitable surface (e.g. glass). It is not applicable to 3-5% of humanity because they do not have fingerprints suitable for electronic sampling. Two palms or even ten fingers are sampled, but work with chemicals or physical activity in certain areas of the construction industry can cause the skin folds of the palms or fingers to be easily damaged, making such identification impossible. In case of failure of fingerprint-based identification at border crossing, the upper epithelium is damaged with strong acids to avoid clear identification. Over the years, the pattern does not change and develops from the age of 18 weeks. In the case of use in the health field, the use of medical rubber gloves may be a disqualifying cause.

Hand geometry-based biometric identification

It is a commonly used technology that takes into account the shape and physical dimensions and proportions of the hand. Az újabb technológiák már pozicionáló tüskék nélkül is (érintésmentesen) elvégzik az azonosítást. It is widely applicable in terms of population, there are no significant exclusion factors and no significant identification time (merely couple of seconds). The process of identification is acceptable to users, there is no revulsion at the process and technology of identification and the need to cooperate with the device is not very high. It measures an external parameter, identification is based on approximately 30 of them [4]. Weight gain, altered hand due to joint disease can cause identification problems, which is sensitive to technology, health, or the need for rubber gloves for pandemic protection can cause a decrease in the number of identification parameters.

Facial recognition-based biometric identification

One of the most well-known technologies and the most used solution in our daily lives. The biometric identification method used by tablets and notebooks to unlock phones has reached everyone and is a popular convenience. Today, most camera systems offer a facial identification solution. The acceptance of the technology is therefore high, authentication is based on external parameters, does not require physical contact during measurement, but the position of the camera and the person and many other external factors (e.g.lighting) significantly affects success.

There is no need for the consent or cooperation of the person for successful identification, which makes the solution suitable for multipurpose and hidden use. During identification, samples can be compared with the registered database of users who may not have consented to the purpose of the processing. It can work based on video taken or downloaded image, identification and AI-assisted solutions do not require a straight look in the camera and can be successfully identified based on very few parameters [5].

The technology measures the characteristic points of the face, their distance and proportions. The search for moles and other characteristic identifiers (scars, tattoos) helps the process, based on the examination of wrinkles and skin poles, it is possible to determine the age of the person [6]. This includes some identification based on the shape of the ear, and among the new solutions there are technologies that can identify from a profile, by head shape and ear shape as an additional solution.

The accuracy of the technology is low, the vulnerability is very high [7], is easily accessible to take advantage of the vulnerability of payment or identification services based on high-quality high-resolution images using masks. Typically, systems do not include live sample detection hardware software solutions.

Iris-based biometric identification

We process the pattern of the iris of the eye. The iris image does not change from the 8th month of the foetus to death, it is widely used and the pattern of two different persons is 1070 years of matching.[8] Internal biometric feature, the technology is contactless. In case of active solution, it is necessary to look up close to the sensor, which is why there is a high need for cooperation in the implementation of the identification process, as well as the acceptance of the method mainly due to the potential risk of infection. It takes into account about 400 characteristics in identification, one of the most accurate techniques, but these solutions are sensitive to various eye diseases.

Retina-based biometric identification

By scanning the vascular network running on the back wall of the eye, the structure of the retinal membrane is identified by the camera, which uses infrared light-based illumination. Very high precision solution and retinal uniqueness ensures that it can be widely used. The acceptance of the procedure is low, because those who do not know the technology are aversed to the "illumination" of the eyes. "Despite all this, retinal identification is one of the best performing biometric methods, with low FRR and near-zero percent FAR values, small data templates, and fast identification results." [9] The need of the head positioning is also not favourable for identification, it is disadvantaged by the mass rapid reading demand and is not advantageous from a hygiene point of view.

Vascular biometric identification

When identifying a finger or palm vascular network, internal data is measured. Illuminated by infrared light, the sensor detects the flow of blood enriched with carbon dioxide through the blood vessels, so it can only be used to measure a living sample. The measured reference points are in the order of millions, with high accuracy and fast solution. The latest technologies do not require any special cooperation, pulling the finger or hand over a surface will be identified contactless within a few seconds. Contaminated skin or surface damage does not affect the identification either. It can be used in the widest population, with few grounds for exclusion. Under the age of 12, due to changes in the growth of children, annual sampling is recommended. In the case of use in the health field during the pandemic period, the use of medical rubber gloves may be a reason of foreclosure.

Voice biometric identification

During voice identification, the frequency of the sound is first identified, and later on, other characteristics of the sound: tone, intonation, rhythm. There is a significant difference between two methods, in the case of "speech recognition", the speech is recognized, while the ”speaker recognition” method is used to recognize the sound itself and the unique characteristics of its emitter. The measured sound depends not only on the transmission medium, distance and method of recording, but also on the biological characteristics of the individual's vocal organs, as well as on his personality, sociocultural environment, intelligence and many other factors. Extremely unique for each pattern [10]. In general, the individual's consent is not required for sampling or identification. It's an internal identifier, an accepted technology. Its weakness is that the sound changes for diseases, even under emotional or physical exertion, which affects the sampling and the success of identification. Ideally, the technology is high-precision, but there is no live sample identification in general applications and ideal conditions are rare, so it is more of a secondary solution with great potential.

OBJECT SECURITY, SECURITY OF SPECIAL OBJECTS

"Object security or object protection is one of the largest and most diversiating areas of personal and property security. From the point of view of person and property security, objects are buildings, facilities, fenced or open areas which are at risk from someone or something and must be secured." [11]. We examine the case of special objects from the perspective of biometric identification solutions.

One important special object is the bank. "Banks are essentially threatened by two main acts of wilful unlawful conduct. One is bank robberies during opening hours, the other is post-closing burglaries. The latter is protected by the structure of the structure itself, the mechanical protection devices installed and the electronic protection systems installed." [11] A common feature of bank robberies is that robbers wear masks. Wearing a mask prevents the identity of the robber's face, so he can't take a photo that makes him easily wanted and recognizable by many. Fortunately, many of the biometric identification solutions are available, even if somebody is not identified immediately, - e.g. wearing a mask - but a number of unique parameters can be recorded: this improves the searchability in the future and increases the chance of gathering evidence. If the mask of the robber covers only the face, it is possible to record biometric uniquenesses based on the parameters of the eye by technique, or to measure the geometry of the ear and store them. Proper "cameraing" of the area in front of the bank may allow to record the dynamics of their gait and movement during the arrival and departure of the robbers (this possibility also exists within the object). In the bank area, the recording and analytic of their thermal image or sound is also a good starting point for later identification. Fingerprints, palm prints, DNA samples are almost impossible to record.

Featured special objects are hospitals, medical institutions. From the point of view of staff, patients and visitors, the composition of the population of entrants is heterogeneous. Passenger traffic is high and activities are wide-spread, a patient can even walk around the hospital during a check-up process. Identification should not be a burden on patients and workers. The safety of protected premises, where patients or visitors are not allowed to enter, should be a priority, but the protection of valuable medical equipment and even patient data should be ensured also.

The safety of patients and their property must be considered, especially in terms of the protection of children's section or even incapacitated, psychologically disturbed patients. Neither live guarding nor access control systems provide an adequate solution on their own.

The identity of the patient is also important in an other point of view: the injured person arriving without medical papers and identity documents is not always easily identified (special blood type, chronic diseases, exclusion drugs, etc.).

A well-thought-out and complex system can provide a satisfactory solution to the many needs of the hospital and medical institution. Workers' privileges can be secured with intelligent solutions that do not prevent them from working, but provide clear and continuous identification. A facial recognition system may be suitable for this purpose, which may be supplemented by gait dynamics and voice or iris identification. Thus, access to the building can be easily ensured, movement within it can be continuously controlled and qualified, or the use of special instruments can be carried out in addition to the daily routine of the task without taking time to complete the identification process. This requires the consent of the worker, the appropriate legal, data protection legislation and the coordination of technologies. Facial recognition alone is not enough, as protective equipment reduces the parameters that can be used for identification, and a vein-based solution is difficult to use because of the use of gloves.

Patients have different aspects and other solutions should be used. There are a large number of frequently changing sample and the registration and entry protocol should not take more than one or two minutes. A palm vein based identification guarantees contactless

high accuracy biometrically, fast and easy to register. The patient should also be treated with an external identification characteristic which helps a security guard or doctors to determine at 'on a glance' whether they are registered, duly admitted patients or guests. A vein-based identification solution may also be suitable in situations where the patient is incapacitated.

In the case of the safety of hazardous materials testing or storage facilities, access control systems must meet a number of requirements. In addition to the in and out function, you must support control and control of movements within an object depending on the permission level. Such systems can greatly assist in cooling the building depending on the number of visitors, or the management and continuous monitoring of guests, or the coordination of rescues during a fire. It is a common need to control the maximum number of occupants in a room, the guest can only enter with an escort. The biometric identification used for entry may vary depending on the characteristics of the field of use, but it must be selected in proportion to the risks and typically involves the integration of several systems. Unique, more expensive technologies can also come to the fore when designing.

CRITICAL INFRASTRUCTURES, CRITICAL INFORMATION INFRASTRUCTURES AND BIOMETRIC IDENTIFICATION

Critical infrastructures and critical information infrastructures should always be examined for their scope, scale and impact over time. Each country has a slightly different interpretation of the concept, but overall, they mean the infrastructure elements and their environment that are vital to that country and their environment, which are essential for the operation of the country's main social and economic life.

The Brussels Summit of Heads of States and governments of 16-17 December 2004 called on the European Commission to draw up a proposal for a European Critical Infrastructure Defence Programme. In November 2005, the European Commission published its so-called Green Paper, which divided European critical infrastructures into 11 sectors and 37 products/services.

Published in Hungary "2080/2008. (VI.30.) government decision, annexed the so-called Hungarian Green Paper, which was adopted by the Government on 30 June 2008. The Government Decision ordered the preparation of a regulatory concept for the protection of critical elements of domestic infrastructure and the preparation of a report on the examination of the possibility of connecting to the European Union's critical infrastructure warning and information network." [12] In Hungary, the legislation on the protection of critical infrastructure is solved both at systemic and sectoral level and, on the other hand, in harmony with European standards. Of course, the legislative environment is only a framework for defence activity, and strategies set out directions and priorities, and the quality of implementation depends on the activities of the professionals who implement it. As the Green Paper puts it, prevention, preparation and resilience are the main pillars of defence." [13]

"In view of international examples, we need to address the coordinated protection of attacks on critical information infrastructures at the government level globally. The protection of critical infrastructures is of paramount importance, in which several domestic governmental organizations are responsible. Among them are the Government Event Management Centre (govCERT) and the National Cyber Defence Institute. The Government Event Management Centre, as a coordination organisation within the country, manages and

coordinates incidents using the Internet as an attack channel with Hungarian and international network security and critical information infrastructure protection organisations, and publishes software vulnerabilities that have been detected and published. The National Cyber Security Institute provides its services (preventive information sharing and operational incident management) to government organisations and municipalities. The Institute has a key role to play in protecting IT systems vital to the national economy and state functioning." [14]

On the basis of the above, it can be summed up that critical infrastructures and information infrastructures, as generally defined systems, cannot be proposed by simple generalisation as biometric identification solutions, nor should it be considered along this line how pandemic control methods affect them. Based on a very high level of professional recommendations in the European Union, but also in all Member States, professional recommendations apply to different systems of criticality and risk, for which industry actors develop defence and identification solutions individually, taking into account several pillars.

VULNERABILITY CAUSED BY THE PANDEMIC SITUATION

Although in 2020 we thought that the COVID epidemic could be overcome sooner, wearing a face mask in a public places remained with us until the end of May 2021. The mask covers a significant part of our face, covering the nose, mouth, animal, thereby strongly affecting the usability of certain methods of identification. As the number of identification parameters decreases, facial recognition software for mobile phones does not work. When wearing a mask, you can't unlock your phone, and contactless phone payments based on previous uncompromising and prevalent NFC chips can be difficult because face authentication requires you to pull the mask off the face when you want to pay. Of course, it can be some inconvenience to switch to a PIN password, but in this case the user risks the identification code being revealed during use, seen by a nearby bad-will, or even recorded by security cameras, and their subsequent analysis and subsequent detection and transfer to the wrong hands is difficult to trace and catch up with.

Similarly, masks used to protect against viruses affect the operation of facial recognition cameras, which can cause problems with a solution used in stadium surveillance or in the detection of a crime.

It may be a good solution to use several methods together in identification, simultaneous use of retina, fingerprints and face when unlocking the phone, or motion dynamics and ear shape identification in public space solutions, but manufacturers should be prepared for them. It can be assumed that integrating multiple identification methods can be used to achieve a more effective solution and to eliminate more weaknesses and vulnerabilities. These systems already require specific improvements and sometimes even AI support, which needs to be looked at in newer aspects.

EU AI REGULATION

Biometric identification solutions, in particular those supported by artificial intelligence (AI), will soon be regulated very seriously by the European Union [15], because regulation has long been behind the technological development of biometric identification in terms of the protection of personal data.

And the rapidly evolving and ever-expanding artificial intelligence-based systems in our present are not primarily a risk from science fiction films with rebellious robots that destroys humanity. For this reason, the European Commission has included its proposals in the White Paper on the future of the EU in order to help the EU catch up with the momentum of digitalisation, while at the same time ensuring fundamental human rights and, last but not least, man-made and controlling technology.

AI-based systems (including biometric identification solutions) are subjected to risk analysis by area of use. Unacceptable risk AI-based systems that are capable of being manipulated, have a major impact on people's safety, livelihoods or rights, or achieve a hidden purpose without the user's knowledge are already banned. Subsequent legislation in the proposal would also prohibit systems modelled on the Chinese Social Credit System [16], which are suitable for behavioural monitoring and thus for categorising users. Remote and automated bulk identification methods which are not tied to some well-limited and heavily regulated purpose are also not acceptable. High-risk systems include, for example, AI-supported systems for critical infrastructures, law enforcement systems, migration, border protection, or medical or financial institutions systems. In these cases, the study proposes to introduce a very high and strict regulation. The data serving the systems must be of very high quality, have a high level of and detailed logging, be documented in detail and be clearly and comprehensively informed.

SUMMARY, CONCLUSION

In this article, we examined what biometric identification solutions are available and what metrics can be used to evaluate their results and how they are related to the field of use and pandemic. We have also examined the entry and identification solutions for special objects and the strengths and weaknesses of the solutions in their specific environment. The investigation has been extended to critical infrastructures, critical information infrastructures. On the basis of theoretical study, it can be stated that the protective tools and solutions used in pandemic protection can significantly influence the successful identification of certain biometric solutions used in general and in an island-like system, but taking into account the field of use, these vulnerabilities can be managed through careful planning and the use of a variety of solutions. The good news is that significant progress is also expected in the regulatory area, which is expected to help protect personal data and provide an opportunity for a wider uptake of biometric solutions.

RESOURCES

[1] original article: https://www.tampabay.com/news/pinellas/2021/02/08/someone-tried-to-poison-oldsmars-water-supply-during-hack-sheriff-says/ (Date of download: 01.05.2021)

[2] Kun T, Ujhegyi P. Adatkezelés mesterfokon – a biometrikus azonosítás és a jogszabályi háttér. Biztonságtudományi szemle, 2020, II. grade, 3rd publication, page 27.
[3] A kritikus információs infrastruktúrák meghatározásának módszertana, ENO Advisory Kft. ©2009, page 55.
[4] https://www.securinfo.hu/termekek/biometria/1152-kez-alapu-azonositas.html (Date of download: 21.04.2021)
[5] https://clearview.ai/ (Date of download: 21.04.2021)
[6] https://oktel.hu/szolgaltatas/belepteto-rendszer/biometrikus-azonositas/arc-es-hangazonositas/ (Date of download: 11.05.2021)
[7] https://www.businessinsider.com/facial-recognition-fooled-with-mask-kneron-tests-2019-12 (Date of download: 21.04.2021)
[8] http://hadmernok.hu/2012_1_tajti.pdf, Tajti Balázs, A biometrikus ujjnyomat azonosítás alkalmazásának új lehetőségeI, Hadmérnök, VII. grade 1st publication, (Date of download: 08.02.2021)
[9] http://oldweb.mit.bme.hu/eng/research/search/downloads/tst/Irodalomkutatas.pdf, University of Technology and Economics of Budapest, Távoli személyazonosítási technikák, 2005 edition (Date of download: 21.03.2021)
[10] Fejes A, Beszéd alapján történő személyazonosítás új kihívásai a kriminalisztikában, Hungarian Law Enforcement 2018/2. 117—126.
[11] DR. Berek Lajos, DR. Berek Tamás, Berek László, Személy- és vagyonbiztonság, ÓE-BGK 3071, 2016 publication, ISBN 978-615-5460-94-4, Page 93.
[12] Muha L, A kritikus infrastruktúrák védelme, 2015, Relnet Technológia Kft, http://real.mtak.hu/78935/1/A_kritikus_informacios_infrastrukturak_vedelme_u.pdf
[13] Dely P, A kritikus infrastruktúra védelmének hazai jogszabályi környezete, Hadmérnök, 2017, XII évf, 3. grade, http://hadmernok.hu/173_17_dely.pdf, (Date of download: 21.04.2021)
[14] Rajnai Z, Fregan B, Kritikus infrastruktúrák védelme, XXI. Fiatal Műszakiak Tudományos Ülésszaka, 2016, DOI: 10.33895/mtk-2016.05. 78 https://eda.eme.ro/bitstream/handle/10598/29102/XXI.FMTU_078_RajnaiZoltan-FreganBeatrix.pdf?sequence=4&isAllowed=y (Date of download: 21.04.2021)
[15] Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence, https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682 (Date of download: 21.04.2021)
[16] www.independent.co.uk/news/world/asia/china-social-credit-system-flight-booking-blacklisted-beijing-points-a8646316.html?utm_source=reddit.com. (Date of download: 20.02.2020)