MEDZINÁRODNÉ VZŤAHY
SLOVAK JOURNAL OF INTERNATIONAL RELATIONS

Faculty of International Relations, University of Economics in Bratislava
2020, Volume XVIII., Issue 2, Pages 156 – 181
ISSN 1336-1562 (print), ISSN 1339-2751 (online)
Submitted: 5. 5. 2020 | Accepted: 12. 6. 2020 | Published 15. 6. 2020

TECHNOLÓGIA SLUŽIACA NA ZADRŽIAVANIE KORONAVÍRUSU: POTENCIÁLNE HROZBY PRE OCHRANU ĽUDSKÝCH PRÁV

TECHNOLOGY IN THE SERVICE OF CORONAVIRUS CONTAINMENT: POTENTIAL THREATS TO HUMAN RIGHTS PROTECTION

Marta Kołodziejczyk[1]

Pandémia koronavírusu 2020 predstavuje výzvu nielen pre vnútroštátne systémy zdravotníctva, ale aj pre jednotlivcov na celom svete. Dôležitou otázkou sa stáva ochrana súkromia za okolností, keď technické spoločnosti ako Facebook, Apple, Twitter, Amazon a Google disponujú údajmi svojich používateľov a skúmajú spôsoby ich použitia v boji proti COVID-19. V prípade pandémie koronavírusu môžu byť z dôvodu bezpečnosti porušované individuálne práva a slobody, k čomu došlo napríklad po 11. septembri 2001 po teroristických útokoch v USA a potom aj v Európe. Berúc do úvahy túto skutočnosť, si musíme byť vedomý možných hrozieb. Článok popisuje vývoj sledovacích technológií a zariadení v podmienkach pandémie koronavírusu.
Kľúčové slová: biometria, pandémia, nefarmaceutické zásahy, sloboda prejavu, právo na súkromie

The Coronavirus pandemic 2020 constitutes a challenge to not only for national health systems, and individuals around the world, but also for ones privacy protection in a circum-stances where tech companies such as Facebook, Apple, Twitter, Amazon, and Google having at their disposal growing troves of its users' data, are currently exploring ways to use them in the fight against COVID-19. In a state of coronavirus pandemic emergency, individual rights and freedoms might be again sacrificed for the sake of security, as it occurred after September 11, 2001 terrorist attacks in the USA and as well in Europe afterwards. Bearing that in mind, one has to be aware of possible threats in order to balance one's priorities. Hence, this article describes the evolution of surveillance technologies and their appliance in the circumstances of coronavirus pandemic.
Keywords: biometrics, pandemic, Non-Pharmaceutical Interventions, freedom of the speech, privacy rights
JEL: K1, K14

[1] Marta Kołodziejczyk PhD., associate of the Jagiellonian University Center for European Studies, Krakow, Poland, e-mail: martakolodziejczyk3@hotmail.com

1 INTRODUCTION

The leader of the United Nations has called the coronavirus pandemic the most challenging crisis since the organization's founding after World War II. Hence, bearing in mind several severe global health threats in the past two decades: epidemics of SARS in 2003 (China), MERS in 2012 (Saudi Arabia), and Ebola in 2014-2016 (West Africa) and the likelihood of future outbreaks of epidemics and emer-gence of new diseases it is crucial to establish a much stronger global mechanism to intervene as intrusively as necessary to stop contagious outbreaks in its tracks (Bildt, 2020). Especially that epidemics are due to spread around the world more quickly than ever enabled by population growth, urbanization, deforestation accompanied by production and distribution processes that crowd together many different species; not to mention the expansion of global supply chains and international commerce reinforced by the growth in international air travel. It is crucial to mention in this context, that by the time Chinese officials acknowledged the risk of human-to-human coronavirus transmission on January 21, 2020, local outbreaks were already seeded in Beijing, Shanghai and other major cities that con-tinued to operate international travel as normal. Over 900 people went to New York every month on average, 2,200 to Sydney and 15,000 to Bangkok, where the first known overseas case appeared in mid-January (Wu et al., 2020). Other early cases turned up in Tokyo, Singapore, Seoul and Hong Kong. The U.S. confirmed its first case near Seattle. About 85% percent of infected travelers went undetected, they were still contagious. In this vein, recent studies (Lai et al., 2020) validate the idea that population movement and close contact had a major role in the spread of COVID-19 within and beyond China, indicating the global risk of a pandemic via travelers infected with this virus. It was only at the end of January that Wuhan was placed under lock-down and airlines started canceling flights. At this stage, however, outbreaks were already growing in over 30 cities across 26 countries; by March 1, thousands of cases were reported in Italy, Iran and South Korea. According to one recent study, if Chinese authorities had openly acknowledged the threat and responded properly just three weeks earlier than they did, the spread of COVID-19 could have been reduced by as much as 95%. Hence, this paper explores; in the first place, the policy choices focused on technological tools applied to combat the Coronavirus transmissions; secondly, investigates possible risks for fundamental rights standards, especially privacy rights caused by surveillance technologies applied in the service of Coronavirus containment.

2 CORONAVIRUS „MADE IN CHINA“

China's old habits of putting secrecy and order ahead of openly confronting growing crisis is not a novelty. It is worth remembering that when SARS (which was also caused by a coronavirus) emerged in southern China in late 2002, the outbreak was covered up for more than a month before the Chinese authorities acknowledged the seriousness of the threat. Likewise, in the early days of the COVID-19 outbreak, police in Wuhan actually silenced medical professionals who tried to raise the alarm, and massive public gatherings were permitted well after the danger of the outbreak had become obvious (Wenliang, 2020). There is no doubt that because local negligence, ignorance, and censorship prevailed at the critical moment, the entire world is now paying an enormous price. What is more, even after it was obvious that COVID-19 would reach the level of a pandemic, China has managed to bar Taiwan from global discussions on how to respond (Rasmussen, 2020). Bearing that in mind, there exists an urgent need to establish a new global institution with the authority and capability to intervene as intrusively as necessary to prevent a contagious outbreak from spreading (Bildt, 2020). Reaching such an agreement would, however, not be politically easy what was already evidenced in conspicuously silent stance of the Security Council motivated by, according to diplomats, former U.N. officials and civil rights groups, a bitter standoff between two of its five veto-wielding permanent members – authoritarian China and democratic United States of America – over the origin of the pandemic.The former, avoiding responsibility in terms of punishing whistle blowers and suppressing information about the outbreak, hails the slowdown of the outbreak as a sign of the superiority of its authoritarian, top-down political system that gives officials nearly unchecked power (Kleinfeld, 2020). What is more, the ruling Communist Party initiated „donation diplomacy" that consists of medical supplies such as masks and protective equipment to countries in need. At the same time, however, Chinese government appears to be demanding public displays of gratitude from recipients of such assistance which is certainly not in the tradition of the best humanitarian relief efforts (Wong and Mozur, 2020); it rather demonstrates Chinese projection of „soft power". In such a way China has stepped into a role that the West once dominated in times of disaster or public health emergency and that President Trump has increasingly ceded in his „America First" retreat from international engagement. Indeed, his disdain for multilateral cooperation and embrace of disease denialism, shows that there's not been even a hint of an aspiration of American leadership/exceptionalism the special role the United States played for decades after World War II as the reach of its values and power made it a global leader and example to the world. Today it is leading in a different way: more than 1,094,800 people in the United States have been infected with coronavirus and at least 64,100 have died, more than anywhere else in the world; more than 1,000 additional deaths have been announced every day since April 2, 2020 (Coronavirus in the U.S., 2020). As the calamity unfolds, President Trump and state governors are not only arguing over what to do, but also over who has the authority to do it. In other words, world's American reference point has vanished. That is fundamentally new (Cohen, 2020). Especially, that in the past following president George W. Bush growing concern about preparedness for a pandemic after anthrax attacks and bird flu outbreak, in February

2007 the Centers for Disease Control and Prevention (CDC) made their approach – bureaucratically called Non-Pharmaceutical Interventions, or NPIs – official U.S. policy. In addition, it was then when the concept of social distancing made its way through the federal bureaucracy in 2006 and 2007, being viewed as impractical, unnecessary and politically infeasible. It is worth to mention in this context, that during Ebola crisis (2014-2016) it was the United States, not the WHO, that stepped in to prevent a wider disaster. Furthermore, following the NPIs five-year review by the Obama administration, the strategy was updated in a document published in 2017. As a result, in the circumstances of Coronavirus pandemic 2020, after postponed reaction to the crisis by American authorities led by president Donald Trump who played down the threat from COVID-19, the disease caused by the coronavirus, the Community Mitigation Guidelines to Prevent Pandemic Influenza (Community Mitigation Guidelines, 2017) was used to encourage the states to lock down as confirmed cases and deaths shot up. It is worth to emphasize in this context that according to recent studies compared to travel restrictions that might have been effective at the early stage, improved detection and isolation of cases as well as the social distancing which reduced contact with people who travelled from the epicenter of the epidemic and were encouraged to quarantine at home is likely to have been especially helpful in curbing the spread of an emerging pathogen to the wider community, and reduced the spread risk from asymptomatic or mild infections.

However, since Trump embodies the personal and societal collapse he is so skilled in exploiting. Insult the press. Discredit independent judges. Remove the checks. Upend the balances. Abolish truth. Pocket the system step by step, "the American patient", as depicted by the German magazine „Der Spiegel", is ripe for an authoritarian lurch. It is worth to mention in this context, that the pandemic, having potential to devastate the African continent and the populations in conflict zones in the Middle East and elsewhere, also emerged against the backdrop of rising authoritarianism and isolationism around the world, and the rejection of international cooperation among headstrong leaders, from Brazil and Philippines to Hungary and Poland. As regards the latter it symbolizes Europe's division between the prosperous north and the poorer south sharpened by the pandemic, and its fracture line between the democracies of Western Europe and the illiberal or authoritarian systems of Poland and Hungary (Erlanger, 2020). As Kenneth Roth recognized „a few weeks ago, the European Union underwent a fundamental change: it ceased being a bloc of exclusively democratic states" (Roth, 2020). It is worth to mention in this context, that the European Commission, which is the EU executive arm and guardian of the bloc's treaties, has already opened two infringement procedures against Poland, in mid-2017 and in mid-2018, over changes to retirement provisions for Polish ordinary and Supreme Court judges and their impact on their independence. In addition, in the recent judgment (2020) the EU Court ordered Poland to suspend Panel on Discipline of

Judges. As regards Hungary, paradoxically, it has been decided by the EU to provide this country with billions of dollars in aid through the Corona Response Investment Initiative on the very day (March 30) Orban asserted near-total autocratic power by beginning ruling by decree for an indefinite period. To conclude, there is no doubt that if the European Union does not stand up for liberal democratic values, those values will be orphaned in the menacing world of Trump, Putin and Xi Jinping who, having at their disposal in pandemic reality „Coronavirus digital surveillance" tools, would exert stricter social control, even turning security agency technologies on their own civilians. Hence, one may claim that these surveillance efforts may threaten to alter the precarious balance between public safety and personal privacy on a global scale.

3 EVOLUTION OF SURVEILLANCE TECHNOLOGIES

As countries around the world race to contain the pandemic, many are deploying digital surveillance tools traditionally applied to exert social control that are designed in these exceptional state of coronavirus pandemic to determine which people should be quarantined or permitted to enter public places. It is worth to recognize in this context, that already in the late 1980s the concept of dataveillance was coined to refer to the "systematic monitoring of people's actions or communications through the appli-cation of information technology". What dataveillance announced – the turning point of surveillance from the individual to the collective, from specific to indiscriminate data collection – the "new surveil-lance" confirms: a world where everything is collected, registered and processed. In addition, Marx emphasizes four points that distinguish new from old surveillance and are worth noting here; the traditional definition of surveillance presupposes there is someone to be especially placed under surveillance, be it a person or a group of persons. In the new surveillance, there is no need to focus especially on an individual: building access logs and credit card records, to mention just two examples, imply indiscriminate data processing. An individual does not have to be a suspect to have his or her name, photos and financial information collected and registered. Second, while in the traditional notion of surveillance there is a clear distinction between an organization conducting the surveillance and the object (person or group), in the new surveillance paradigm, this is not always the case – for example, when civilians photograph government officials in situations of abuse of power. Third, observation in the new surveillance is not necessarily close, as it is carried from remote places. Fourth, surveillance is executed not only through visualization, i.e., observation, but also through any means of data collection, for instance movement, sound and temperature detectionas it is a case during corona virus pandemic. In addition, the "new surveillance" exploits not only hard data – meaning data as collected and structured by administrations and related entities – but also soft data – collected and processed in an unstructured form from multiple sources such as social networks and localization systems (Costa, 2016) which is due to be analyzed in this paper. Finally, the “new surveillance” enabled by the technological endeavors is no longer just a means to detect potential threats but also potential opportunities such as in market analysis, human resources management and many other aspects of human beings’ existence, for instance health care system (Marx, 2002). This can be evidenced in the investi-gation of researchers at BenevolentAI, an artificial intelligence start-up in central London, which turned their attention to the coronavirus. Within two days, using technologies that can scour scientific literature related to the virus, they pinpointed a possible treatment with speed that surprised both the company that makes the drug and many doctors who had spent years exploring its effect on other viruses. Though many questions hang over its potential use as a coronavirus treatment, it will soon be tested in an accelerated clinical trial with the National Institutes of Health. It is also being studied in Canada, Italy and other countries hoping to accelerate efforts to understand how the coronavirus is spreading, treat people who have it and find a vaccine (Metz, 2020).

However, combating global health threat by means of putting in place a patchwork of digital surveillance measures in the interest of states’ authorities, with little international oversight (Singer and Sang-Hun, 2020) could permanently open the doors to more invasive forms of snooping later. It is a les-son Americans learned after the terrorist attacks of September 11, 2001. In this vein, one may recognize certain similarities between terrorism and pandemic; in the first place, both strike by surprise and in-vade individuals’ personal life; with terror ones worries about being in crowds and rallies and sport-ing events; similarly, with the virus – crowds spell danger.” Secondly, “the virus is something we don’t know, we can’t control, and so we’re afraid of it.” And for good reason – it has already killed more Americans than the nearly 3,000 who died on September 11, 2001, and it will kill many times more. In addition, part of what makes terrorism terrifying is its randomness; „terrorists count on it and in a sense this virus behaves the same way” (Erlanger, 2020). Concluding this comparison, in response to the 9/11 attacks the United State’s Patriot Act was passed; it gave the government broad surveillance powers with little oversight, including demanding customer data from telecoms without court appro-al. Twenty years later, it’s still around. Interestingly, in July 2015 in response to Charlie Hebdo attacks the French Intelligence Act, which resonated with the USA Patriot Act as far as uncontrolled surveillance is concerned, was passed by the National Assembly with 438 votes in favor and just 86 against. It introduced in France state of emergency and, as a result, enabled intelligence agencies to record any calls, text messages and internet activity using the so called “black boxes” (complex algo-rithms installed to detect a pattern of suspicious behavior online). Moreover, in a declared officially state of emergency authorities became capable of executing wireless phone taps, installing hidden cameras as well as using geolocation measures. What is more, on the October 3, 2017, under president Macron many of the above mentioned heightened security measures envisioned by the state of emergency, that have given local police and administrative authorities power to monitor, arrest or detain suspects without judicial oversight, were approved by the French Parliament in the frame-work of antiterrorism laws. Hence, in 2020 in the pandemic reality French known for sensitivity to freedom are even more cautious to use smartphone tracking application that would inform people if they come in contact with an infected person. By contrast, however, intrusive digital tracking applied by Asian democracies like South Korea has helped it avoid giving up fundamental freedom of move-ment by means of strict lockdowns experienced in Europe (Onishi and Méheut, 2020). Another example of using the pandemic to expand the power is provided by Britain, known for a long history of democracy and well-established democratic customs, where a coronavirus bill which was rushed through Parliament at a breakneck pace, affords government ministries the power to detain and isolate people indefinitely, ban public gatherings including protests, and shut down ports and airports, all with little oversight (Gebrekidan, 2020). What is more, as far as the British government's technologi-cal response to Coronavirus outbreak is concerned, the National Health Service is moving forward with an application to track the spread of the virus despite questions about the technology's effectiveness, privacy safeguards and compatibility with key iPhone and Android features. In Britain, which has a history of robust government surveillance to fight terrorism, officials argument that more can be learned about the virus by collecting lots of information in a centralized database that, as it is argued, guarantees more research capabilities to spot emerging hot spots and patterns of how the virus spreads. In addition, the British authorities said that the data would not include personally identifiable information, and that access would be limited to those working on the pandemic response. By contrast, Apple and Google are promoting a decentralized approach that would protect against invasions of privacy. It is worth to mention in this context that these Sillicon Valley Titans are supported by academics, security researchers and privacy groups devoted to restrict government data collection, by claiming that, whatever the safeguards, a centralized database creates too much potential for abuse (Satariano, 2020). What is more, Britain's top privacy regulator, Elizabeth Denham, said last month that a decentralized model should be a "starting point" for contact tracing (Denham, 2020).

4 EU AND U.S. APPLIANCE OF BIOMETRIC TECHNOLOGY

As numerous academic studies documented, the state surveillance led by the example of the United States of America has been applying biometrics, an information technology that allows for translation of such data as DNA, fingerprints, eye retinas and irisis, voice-, facial patterns and hand measure-ments into digitally processable data; in this way human body became „machine-redable".

Hence, these new technological endeavors in the field of migration policy such as databases, high-tech passports and visas inclusion of biometric data in documents and computer records has been on the rise. The Bush administration was a pioneer in launching the "Smart Borders" program, that was later copied by the European Union (Smart Borders Package was tabled by the European Commission in February 2013), designed to screen for terrorist incursions into the United States at air and land ports of entry; consequently, the system that tracked virtually all of the 35 million annual visitors to the United States was operable by 2005 (Schmitt, 2002). Using a variety of technologies, including surveillance, biometrics, and interlinked information technology (IT) databases, the stated goal was to identify problematic entrants either persons or cargo (e.g., terrorists and their weapons) while at the same time facilitating the quick entry of legitimate goods and travelers. In the wide sea of information flowing across globalized borders "secured through technology" utilizing tools to identify valuable knowledge about threats became priority. At the same time, the power of these technological solutions invoked questions of efficacy and democratic values. Crucial to note is the fact that in the "anti-terrorist crusade" scientific community was due to "... serve on the front lines of this war, by developing new technologies that would make America safer (Bush, 2002). In the first place, at the United States House subcommittee hearing in February 2002, a panel of commercial information technology experts and management consultants were asked to give technical advice on how the war on terror might be fought using risk profiling techniques. The hearing concluded that technologies designed to classify populations according to their degree of threat were long available in the private commercial sector and should be deployed at the service of border security. Indeed, the invited panel of experts stated clearly that 'our enemies were hiding in open and available information' and that, had surveil-lance and profiling techniques been in place, the events of 9/11 'could have been predicted and averted'.

As regards the European Union's approach towards technological innovations, it mirrored the strategy of its American ally. Technology has been embraced without much debate as a core compo-nent for the EU's Area of Freedom Security and Justice (AFSJ) policies. Furthermore, enormous pace at which large-scale IT systems proposals were tabled made it extremely difficult for stakeholders (European and national Parliaments, DPA's including EDPS as well as civil society) to have a full overview.So called ‚technology driven" approach was explicitly evidenced in the June 2008 report from the Future Group on European home affairs, which considered that "databases and new tech-nologies would play a central role in further developing Home Affairs policies [...] Even if technology can never completely replace the human factor, technological progress can provide the necessary means to optimise mobility, security and privacy simultaneously" (Report of the High Level Advisory Group on Future of European Home Affairs Policy, 2008). In this context, it is worth to mention that another EU institution, namely the European Parliament (EP) focused in its study on data protection challenges posed by the increased processing (ongoing or envisaged) of personal data for law-enforcement purposes. Among these were mentioned: 1) the tendency to generalise of data processing meaning the shift towards dataveillance, pro-activity and profiling; 2) putting limitation purpose referring to the „life of data" in EU data systems the key principle of data protection at risk by means of the proliferation of data-systems and, as a result, tendency to consider technology as one-size-fits-all solution (Bigo et al., 2011). The latter was also shared by the European Data Protection Supervisor (EDPS) who emphasized that „far reaching proposals regarding large-scale IT systems has been 'programme-driven' rather than 'evidence-driven" (Hustinx, 2008); in other words, the main stimulus originated from some Member States, the European Commission as well as private sector, rather then was caused by a demonstrated need.

5 Biometric technology

Answering to the terror-related challenges the European Union and the United States attempted to reinforce their knowledge about the cross-border movement of people by employment of scientific technologies and managerial expertise in the politics of border management. In this context, it is worth to mention about "Automated Target System" was applied by the US Department of Homeland Security (DHS) as a means of border control. According to the Privacy Impact Assessment (PIA) prduced by the DHS "the project involved conducting research to select the specific sensors that would capture video images, audio recordings, cardiovascular signals, pheromones, electrodermal activity, and respiratory measurements. For example, one potential measurement was heart rate. There was a number of technologies that a sensor could use to capture heart rate. One aspect of the research was to determine which specific sensor technology most accurately captures the desired measurement. Another aspect was reviewing the research records to determine if the measurement being captured is actually an indicator of the behavior being evaluated (i.e., did increased heart rate actually occur when the subject was intending to cause a disturbance)" (Privacy Impact Assessment 2008). Furthermore, more and more sophisticated technological tools, used for exercising of biopower such that the bodies of migrants and travelers themselves became sites of multiple encoded boundaries, consisted of: bone scanners, speech recognition utilities and last but not least biometrics (Liu, 2012). The latter derived from the Greek words bio (life) and metric (measure of) are referred to "technologies that measure and analyze physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person such as facial images or dactyloscopic data". What is more the use of biometric data refers back to the fourteenth century in China;Fingerprints were used by Chinese merchants to settle business transactions;

fingerprints and footprints were used by parents to differentiate children. Furthermore, physical/physiological characteristics are presented by fingerprint, finger vein, finger geometry, or wrinkles, palm print, odor, pores, bite marks, hand geometry, dental geometry, ear, facial geometry, facial thermogram, iris, skin patterns, smile, lips, DNA, etc. As far as the latter is concerned, it is crucial to note that DNA-based technologies do differ from standard biometrics in a number of ways: a) DNA requires an actual physical sample as opposed to an image, photograph or scan; b) DNA matching: a) is not done in a real time and, for the most part, is not automated; b) does not employ templates or feature extraction, but rather represents the comparison of actual samples. Behavior characteristics include dynamic grip recognition, handwriting, tapping, eye movement tracking, keystroke dynamics, gait, mouse dynamics, etc. (Liu, 2012). Despite these many types, the most common used, in terms of identification of individuals and identity verification, are facial, iris or finger recognition. In this context, it is worth to specify that identification (one-to-many) means an act of identifying a person, i.e. to establish that a passenger is a particular person. It is typically the process of comparing biometric data of an individual (acquired at the time of the identification) to a number of biometric templates stored in a database. For instance, it can be used where authorities aim to identify criminals or potential offenders among the passengers through comparison against a watch list. This means that biometric data are stored on a database. Identity verification (one-to-one), on the other hand, means that the identity of the person is compared to a claimed identity. It is typically the process of comparing the biometric data of an individual acquired at the time of the verification to a single biometric template stored in a device. Fur-thermore, the digital biometric data are algorithmically converted into what is called a template. It is defined although in a very broad way as the 'reference biometric feature set' and the 'set of stored biometric features comparable directly to probe biometric features'. The extracted reference biometric features (i.e. a template) can take many forms: a table or a (fixed-length) numerical (binary) string (e.g., 101010 representing a feature vector or not), differing in details and length. The templates will also vary for each of the characteristics. For example, for fingerprint, the minutiae features may be represented as an unordered set of tulles consisting of the minutiae's coordinates and local orientation. For hand geometry, the geometrical properties of the hand are represented by a fixed-length ordered vector of the lengths and widths of the fingers and/or palm. Iris is represented as fixed-length binary strings. A biometric sample can also be processed in several successive templates. The main idea, however, is that the template does not contain the full (biometric) information as contained in a sample, but only represents the particular features selected by the algorithm(s). Furthermore, these selected features, once extracted, are represented in a chosen specific (sometimes proprietary) format and are stored for later use. This processing is in most cases irreversible, which means that a 'raw' biometric data cannot be retrieved from the template. These templates are usually stored in a database that is contacted as soon as a face, eye, hand, finger or voice is presented to the system in a particular identification or verification procedure. Once this second biometric image has been subjected to the same algo-rithmic transformation, an identical template is searched for in the database, and, if found, the individual is recognized in the system. Another possibility is that the templates are not stored centrally, but on a chip card, in which case the user needs to show both the card and the required part of the body to 'prove' that he/she is the legitimate user of the card. Biometric data stored on a chip card do not need to be kept in a database by the organization concerned, and could be deleted without loss of functionality (van der Ploeg and Sprenkels, 2011).

Face, fingerprints, iris, retinas, hand geometry are widely used in biometrics systems biological characteristics. In the reality of the coronavirus pandemic where, according to the German Robert Koch Institute, almost 90% of people infected with COVID-19 in China have been diagnosed with fever, making fever screening by means of a new camera which measures body temperature with high accuracy and speed a valuable tool for virus transmission prevention (Burt, 2020). In addittion, the concept of on-the-fly biometrics suggests that the capture of biometric details (primarily in the form of fingerprints, face or iris recognition, but also vein or gait recognition) is executed automatically while the passenger is walking through the airport. The idea is that each one of the biometrics solutions should complement the others, so that the same biometric data and token can be used throughout the system. This should facilitate identity verification at several points in the infrastructure, enabling person-tracking capabilities. The expectation is that within the next 10 years, the majority of airports will trial single biometric travel tokens and 54% airlines plan to evaluate the technology. But today, although it has great potential, this technology is still being developed, with a number of challenges regarding performance (accuracy, speed) and operational requirements. Thus, further research and development is needed.

An image of the face can easily be captured, with or without the cooperation (and knowledge) of an individual, even from a distance. Facial scans are sometimes equipped with infrared illumination. The facial image can be analyzed in various ways. The analysis may focus on for example the geometric distinguishing features of the face, the relative distance between and directions of specific points, but also on skin texture. The distinctiveness of faces is, however, limited. As far as the facial recognition technology is concerned, the main idea is to collect face images of persons by Closed Circuit TV (CCTV) and compare them to existing biometric data stored in the form of high-resolution images, allowing to verify or identify a person. In general, facial recognition implies the use of the unique con-figuration of a person's facial features for identification and verification. A number of technologies are used, including 2D, 3D, infrared facial scans. The most systems work with two properties of the face: geometry – the configuration and placement of features, and the texture – colors, tones and condition. In Chinese city of Zhengzhou, for instance, a police officer wearing facial recognition glasses spotted a heroin smuggler at a train station. In Qingdao, a city famous for its German colonial heritage, cameras powered by artificial Intelligence helped the police snatch two dozen criminal suspects in the midst of a big annual festival. In Wuhu, a fugitive murder suspect was identified by a camera as he was buying food from a street vendor. Beijing is embracing technologies like facial recognition and AI to identify and track 1.4 billion people (Mozur, 2018). Consequently, in aviation security, facial recognition was initially developed in order to identify dangerous persons by comparing the live biometric input data – passenger's face image captured on CCTV – with the databases of known criminals or suspects. Such identification is still one of the main purposes of facial recognition technology at the airports. Accordingly, many states issue biometric passports, e.g. Russia and EU Member States (Commission's Decision, 2006), allowing comparison of input data with faces in travel documents at border control. Biometric passports have mainly been used in automated border control and/or Trusted Traveller Programs (TTP). In addition, the use of facial recognition for passenger verification grows rapidly. One of the reasons for this is the fact that the International Civil Aviation Organization (ICAO) selected face image as the primary biometric identifier for travel documents, with iris and fingerprints being optional (ICAO, 2015).

Fingertips contain ridges and valleys. The ridge flows form patterns such as arches, whorls and loops, three basic patterns recognized and used in the classification systems developed by Vucetich and Henry. Other biometric properties based on patterns are socalled cores and deltas. Specific points known as minutiae are used as well. Minutiae are discontinuities in the flow of the ridges and are mainly the ending or the bifurcation of the ridges. Minutiae and patterns are used in biometric fingerprint systems. Fingerprints, which are the prints left by the ridges of a finger due to secretions of sweat or ink use, are considered unique. Images of the fingerprint are collected by sensors. Cooperation of the data subject is in principle needed, but latent fingerprints, such as prints left on the sensor or prints found on objects at a crime scene, can also be used, with or without the knowledge of the data subject. The quality of the image is of high importance. Algorithms, proprietary to the vendor or the system developer(s), are used to reduce the 'noise' of the image and to enhance the ridges. Finger-print, which has been used in forensic applications for over hundred years, is now widely used in biometric systems in the private sector.

As far as the geometry of the hand is concerned, it was one of the first biometric characteristics used for automated verification against a stored reference. The shape and size of the hand palm, finger length, width and thickness of the fingers are measured, as well as curves and the relative locations of these features. In principle, only the geometric features are used for hand geometry and no surface details are recorded, ignoring fingerprints and ridges of the palm, lines, scars and color. Unlike fingerprint, the uniqueness of a human hand is limited. The individual hand geometry features therefore do not scale well for identification (in large-scale applications) and limits the use of hand geometry to mainly verification purposes and small-scale identification applications. Furthermore, the biometric method based upon this characteristic is vulnerable to changes of the hand geometry. Such changes may be caused by for example an injury (e.g., loss of one or more fingers or deformation of the hand), diseases (e.g., arthritis) and aging, but also by wearing jewelry. The print of the palm of one's hand is another distinctive biometric characteristic fit for use in biometric systems. A palm of the hand has patterns of ridges and valleys, similar to those of fingerprints, as well as lines and wrinkles. While the use of palm print shall be distinguished from the use of the geometry of one's hand as biometric characteristic as explained above, palm print systems may include hand geometry characteristics in their calculations. Because of their uniqueness, palms can be used for identification purposes.

Behavioral characteristics, such as typing or signature writing characteristics, are also used in biometric systems. They are based on behavior which is deemed to be unique or at least distinctive, universal and (more or less) persistent. Typing characteristics, in particular the way a person types or pushes on a key-board, such as the rhythm and error frequency, is distinctive and may be analyzed by software. The analysis detects the patterns of the typing and produces a digital measurement, which may be compared to previously stored patterns. The dynamic of someone writing a signature is anoth-er characteristic used in biometric systems. The way the signature is written with a 'smart pen' includ-ing sensors or on a pad is analyzed by software (e.g., the acceleration, pressure, and the direction of the signature strokes). Signatures have in general always been used as a method of verification, for examples in legal or commercial transactions, and the use of the socalled dynamic signature characteristics is therefore considered as being easily accepted.

Voice of an individual can be used for comparison in biometric systems as well. The charac-teristic depends on both one's biological and behavioral traits. Both systems based on text spoken by the individual and stored and those having no advance registration of one's speech are used. Coopera-tion of the individual is therefore in principle not required. Speaker recognition based upon voice can be used for identification (according to some with smaller databases) and verification. While being used until recently mainly in forensic applications, adoption in the private sector has been slow, but increased use may be expected.

The iris provides rich biometric data in the distinctly colored ring around the pupil. The random, detailed and unique structure is captured via a sensor to which the data subject in principle has to direct his or her eye and which illuminates the iris with near-infrared light. Occluding features such as eyelids, eyelashes, or reflections from glasses, must be detected and excluded from being encoded in the template. Latest technology, however, permits to capture iris information also at a distance and without specific cooperation of the individual. The analysis of the retina vascular patterns also pro-vides individual traits to be used in automated identification or verification processes. Retinal scanning analyses the layer of the blood vessels located at the back of the eyeball with special lighting. The scan uses infrared or near-infrared illumination and imaging. It has been adopted in various military applications because of good levels of accuracy when other biometric techniques were still developing. However, the retina is rather hard to measure and capturing its image requires a great degree of effort and cooperation of the data subjects. The use of the retina, however, com- pared with other biometric characteristics declined in popularity. Nowadays, its use is restricted to extremely demanding access control situations, such as in governmental or military settings, for example for access to nuclear weapon or research sites.

Most visible and at the same time most controversial airport security solutions according to both security professionals and civil rights advocates, are body scanners. It is noteworthy that at present, instead of the term "body scanner" or "whole-body scanner", more neutral and technical terms are used, like "security scanner" in the EU, "advanced imaging technology" (AIT) in the USA, "radio scan portal" in Russia. Clearly, this is done in order to present, via language, the scanning process as automatic, anonymized, universal, neutral, routine, and professional, downplaying the core essence – inspection of the naked body. Traditional measures for detecting hidden objects are metal detectors and hand search. Even if done in private, such searches require additional staff and cause delays for passengers, not to mention about privacy concerns related to prohibition of direct touching of private body areas as part of the search (Enerstvedt, 2002). In terms of relatively easy to hide dangerous items in sensitive body parts the scanner's advantages are quickness and no need of physical con-tact. The choice between hand search and body scanners is thus a trade-off between security effective-ness and privacy concerns (Neeman, 2015). The first body scanner was created by Steven W. Smith in the USA in 1992. It was an ultra-low-dose Secure 1000 backscatter X-ray scanner. It is believed that the first airport in the world to implement body scanners was the Schiphol in the Netherlands in 2006, but the trials of this technology started much earlier. According to some information, the USA started initial tests not later than in 2002, Russia – in the middle of 1990s. But the hour of body scanners came apparently after December 25, 2009, when the so-called "underwear bomber" attempted to detonate plastic explosives hidden in his undergarment. It was the moment when many other states became committed to have such devices at the disposal as well. The UK, for example, installed the machines immediately; Schiphol purchased additional units, etc. Detection performance lies in the scanner's ability to discern any prohibited object that the person screened may be carrying on the body or in the clothing. Several technologies are used in order to identify such hidden objects. They include those based on natural thermal radiation (heat from the body), but the most commercially available security scanners use the following technologies: backscatter X-ray, active millimeter wave (MMW), and X-ray transmission imaging technology. The early commonly used backscatter and MMW devices produced and showed to a human operator extremely detailed images of the screened persons as if they were naked. Thus, the reaction of the general public, privacy organizations and other interested persons and agencies was appropriate: protests and scandals. As a result, amend-ments were made to present images visible to operator in more privacy-friendly forms: blurring faces and intimate parts, using mannequin figures, etc.

Profiling, similar to biometrics, is not new and refers back to the Middle Ages, when the inquisitors tried to "profile" heretics (Enerstvedt, 2017). It is believed that the first "profile" for criminal purposes was created by British detectives in 1880s with regard to serial killer Jack the Ripper (Britannica, 2020). In terms of aviation security, in general, profiling is the practice of categorizing people according to particular characteristics, such as passenger's actual or perceived race, ethnicity, religion, nationality, age, gender, behavioral traits, separately or in combination, or together with other factors (Quinlan, 2015). The core idea is to create profiles or dossiers – a set of definite characteristics, associations, activities, etc. to predict behavior and more, and then search for individuals with a close fit to that set of distinctive features (Roger, 1993). For instance, the profile of the terrorist can be deduced by cross-indexing information from various databases, the population roll, the use of credit cards, movements detected through use of mobile phones, brand name discount cards, use of medications, etc. Furthermore, three types of profiling can be noted: manual performed by a human being, automated profiling performed by computers, and semi-manual, combining the first two. For any type of profiling, particular characteristics may serve as indicators of potentially dangerous behavior, assisting in determining whether to stop, search, or question a person. In aviation security, all types of profiling are used extensively and may refer to all the selected measures; with regard to body scanners, profil-ing can be relevant if passengers are selected to be scanned by security agents (manually) or automatically via a computer pre- screening system. For CCTV, behavior analysis can be conducted manually by a CCTV operator or automatically by algorithms of Video Analytics (Enerstvedt, 2017).

Concluding, the benefits of applying biometric technology, often referred to by expert circles, as big data analytics into the security domain are many; greater operational efficiency and speed, more precise risk analyses and the discovery of unexpected correlations, all of which feed into risk profiles, better targeted inspections and more efficient use of scarce resources (Broeders et al., 2017). However, it is crucial to note that biometrics – as a technique, as a concept and as a practice – is imprisoned in a number of paradoxes and dualities that make it unavoidably controversial. Biometric data is typically permanent and stays the same throughout lifetime. Not to mention about the fact that appliance of some of biometric data leaves traces (fingerprints, DNA) and thus increases the risk of unauthorized repetitive use (Belgian Privacy Commission, 2008). In other words, it is a unique identification instrument what may constitute the risk of identity theft. Furthermore, biometrics transforms the physical characteristics of a person into electronic data; in this process the distinction between – on the one hand – the ‚body itself' as a domain of bodily integrity – and – on the other – the information about the body that belongs to the domain of privacy is endangered. In this context, there appear a variety of dilemmas related to withholding respect for the body which constitutes at the same time a piece of digital information meaning that the digital body can be searched remotely in both time and place. In other words, without the person being present or knowing what is happening. Furthermore, practices such as searching databases, profiling and classifying target certain groups, which means that they are more vulnerable to social categorization, exclusion and automated decisions with all the risk that may be attached. Finally, no biometric system is infallible. All these currently in use have error margins expressed in 'false acceptance rates' (FAR): the system falsely recognizes someone as being the same person and in 'false rejection rates' (FRR): the opposite case in which the system falsely reports that it is not the same person. As has been evidenced by researchers the percentage of the above-mentioned errors increases when the biometric system tested at first in laboratory conditions with relatively homogeneous sample, is exposed to the outside world with all the variable conditions. Facial-recognition systems, in particular, are still scarcely useable because of this problem. Not to mention about the circumstances where fingerprints may be impossible to read, body parts may be missing or damaged. As regards young children, manual laborers and the elderly – their fingerprint ride pattern is either undeveloped or no longer clear enough to be properly registered by the scanners. To conclude, it is to be observed that a large number of physical and technical variables influence the performance of each biometric system that functions within the EU border and immigration data basis (van der Ploeg and Sprenkels 2011, p. 76).

6 TECHNOLOGICAL RESPONSE TO CORONAVIRUS PANDEMIC

In 2020 due to the coronavirus pandemic experienced in the United States, the White House officials spoke with Google, Facebook and other tech companies about potentially using aggregated location data captured from Americans' mobile phones for public health surveillance of the virus. Indeed the pandemic has created an opportunity but also a challenge for tech companies. As regards the former, in the frantic political and economic environment created by the outbreak their lobbying operations may be quietly push for long-held goals. Especially that tech services are increasingly in demand as millions of people work and socialize from home to avoid being infected by the coronavirus. Amazon orders have soared so much that the company has put a priority on shipping essential items like soap, food and toilet paper. Google has provided temporary free access to some of its remote work tools. And Facebook's traffic has surged. Tech lobbyists have nonetheless seized the moment. In the weeks before the virus swept the United States, groups representing Google, Facebook and Twitter already wanted the California attorney general, Xavier Becerra, to wait to enforce the state's new privacy rules until 2021. The law, known as the California Consumer Privacy Act, requires businesses to give people a copy of the data that has been collected about them, as well as the ability to delete it. Companies have complained that the rules would place too many obligations on businesses. The law went into effect this year, but California will not start enforcing it until July. Other companies with growing demand for their products have pushed for deregulation or other government action that would benefit them, arguing it would improve the response to the virus crisis. Trade associations representing drone makers like Amazon and the Alphabet subsidiary Wing have tried to expedite approval for airborne deliveries — or waive approvals altogether — and eliminate prohibitions on the circumstances under which the devices can be operated.

The challenge, on the other hand, consists of the necessity to reconfigure touch-based bio-metric authentication (fingerprint or hand scanners), that are currently potential vendors for the COVID-19 spread, to no-contact version. In addition, appliance of Information and Communication technologies aimed at curbing the spread of the virus has been recently legitimized by some expert circles by acknowledging that human surveillance and case reporting providing: a) information regarding the presence and epidemiology of influenza viruses in the community, b) determining appropriate interventions and targeting them, and c) generating current accurate information for public health officials, providers and the public, are efficacious and likely to be effective during any pandemic phase. At the same time, however, broad endorsement was qualified by concerns about resource con-straints, especially in a large outbreak, potential difficulties in cooperation between providers and governmental and non-governmental entities, the cost of scaling up capacity to report and investigate influenza-like illness, privacy rights and the right to informed consent (Aledort, Lurie and Wasserman, 2007).

Let us dwell in this section on particular examples of so called „coronavirus surveillance". In South Korea, government agencies were harnessing surveillance-camera footage, smartphone location data and credit card purchase records to help trace the recent movements of coronavirus patients and establish virus transmission chains. In addition, South Korean authorities began posting detailed location histories on each person who tested positive for the coronavirus. The site has included a wealth of information – such as details about when people left for work, whether they wore masks in the sub-way, the name of the stations where they changed trains, the massage parlors and karaoke bars they frequented and the names of the clinics where they were tested for the virus.

The above described South Korean's coronavirus crisis management mirrors the ever present dilemma in time of emergencies like pandemics of weighing privacy against other considerations, like saving lives. Simultaneously, however, one may claim that while companies and public authorities cooperate to enable proper response for the public good, governments as well as commercial business should limit the collection and use of data to only what is needed. This could be exemplified by unusual reac-tion of the South Korean authorities who announced that in order to balance the value of protecting individual human rights and privacy and the value of upholding public interest in preventing mass infections, data-sharing guidelines were due to be refined to minimize patient risk.

Undoubtedly, the highly technological reaction to the outbreak of the coronavirus pandemic relies heavily in South Korean's endeavors in the field of artificial intelligence exposed in reality of Songdo an Ambient Intelligence City being a synonym for convenience, purchasing power and comfort – something certainly arguable from an urbanist and environmental point of view – the name "Automated Target System", betrays itself, evoking traditional representations of the power of governments/corporations of the Leviathan or Big Brother style. Built from scratch its buildings and facilities are connected through Information and Communication Technology (ICT) not to mention public transportation that is more "intelligent" and "flexible"; by taking advantage of GPS and wireless technologies as well as Global Positioning System (GPS). As it turned out during the coronavirus pandemic location data are on demand; in Lombardy, Italy, the authorities analyzed this kind of data transmitted by citizens' mobile phones to determine how many people were obeying a government lockdown order and the typical distances they move every day. In Israel, the country's internal security agency was poised to start using a cache of mobile phone location data – originally intended for counterterrorism operations – to try to pinpoint citizens who may have been exposed to the virus. Similarly, in China, telecommunications companies helped the government track and contact people who had traveled through Hubei province during the early days of the virus. Location data was funneled to China's National Health Commission and other agencies, allowing them to recreate the steps of virus carriers and people that they may have encountered and issue warnings via social media.

Among countries that are using smartphone location data is Singapore; the TraceTogether application can identify people who have been within 2 meters of coronavirus patients for at least 30 minutes, using wireless Bluetooth technology which has to be turned on. In case a user get infected, the authorities will be able to quickly find out the other users he has been in close contact with, allowing for easier identification of potential cases and helping curb the spread of the virus. What is crucial, official contact tracers will provide a code that users can match with a corresponding verification code on their application. Once authenticated, users will get a PIN that allows data to be submitted. It is worth to emphasize in this context, that contact tracers will not ask for any personal details. Another example is provided by Iranian's government application; while its efficacy was low, given reports of asymptomatic carriers of the virus, the application saved location data of millions of Iranians. Furthermore, in Argentina those who are caught breaking quarantine are being forced to download the application that tracks their location. In Hong Kong, on the other hand, individuals arriving in the airport are given electronic tracking bracelets that must be synced to their home location through their smartphone's GPS signal (Gershgorn, 2020). To conclude, the use of smartphone location data that relies on tracking population-level movement down to enforcing individual quarantines is the most common form of surveillance implemented to battle the pandemic; raising concerns pervasive surveillance could be used as a new means of social control to restrict people's movements or stigmatize, isolate or even exile them later.

As regards the United States of America, its government agencies are putting in place or considering a range of tracking and surveillance technologies aimed at controlling the rapidly spreading coronavirus, but at the same time testing the limits of personal privacy. The technologies under con-sideration include everything from geolocation tracking that can monitor the locations of people through their phones, e.g. restaurants, parks, other public spaces that are still seeing heavy traffic despite shelter-in-place or stay at home orders, to facial-recognition systems that can analyze photos to determine who might have come into contact with individuals who later tested positive for the virus. While Google and Apple, two tech giants are working with public health authorities and university researchers to produce a set of tools that apps could use to notify users who come in close contact with a person who tested positive for COVID-19, the disease caused by the coronavirus, researchers at Washington University (Washington University, 2020) are working on the project that treat location data with more privacy in mind, not to mention about the Massachusetts Institute of Technology (MIT) which is working with partners around the world on „privacy preserving way of automated contact tracing" by using the Bluetooth signals that our cell phones send each other. These signals represent random strings of numbers, likened to "chirps" that other nearby smartphones can remember hearing. If a person tests positive, they can upload the list of chirps their phone has put out in the past 14 days to a database. Other people can then scan the database to see if any of those chirps match the ones picked up by their phones. If there's a match, a notification will inform that person that they may have been exposed to the virus, and will include information from public health authorities on next steps to take. Vitally, this entire process is done while maintaining the privacy of those who are COVID-19 positive and those wishing to check if they have been in contact with an infected person (MIT, 2020). To conclude, the issue of striking the right balance between privacy and safety is of paramount importance especially that according to the latest opinion poll conducted by the University of Maryland among major barriers to the above described endeavors is distrust of American society being at the same time also major source of skepticism about the infection-tracing apps of Google, Apple and tech companies generally, with a majority expressing doubts about whether they would protect the privacy of health data' (Timberg, Harwell and Safarpour, 2020). In addition, the University of Maryland's opinion poll uncovered also some other barriers to the above described endeavors; approximately 1 in 6 Americans do not have smartphones, which would be necessary for running any apps produced by the initiative. In addition, rates of smartphone ownership are much lower among seniors, who are particularly vulnerable to the ravages of Covid-19, with just over half of those aged 65 or older saying that they have a smartphone (53%). What is more, rates are even lower for those 75 and older, according to the poll. Furthermore, among the 82% of Americans who do have smartphones, willingness to use an infection-tracing app is split evenly, with 50% saying they definitely or probably would use such an app and an equal percentage saying they probably or definitely would not. Willingness runs highest among Democrats and people reporting they are worried about a COVID infection making them seriously ill. Resistance is higher among Republicans and people reporting a lower level of personal worry about getting the virus. It is crucial to emphasize here, that according to the opinion poll "a major source of skepticism about the infection-tracing apps is distrust of Google, Apple and tech companies generally, with a majority expressing doubts about whether they would protect the privacy of health data".

Apart from statistics, however, the Centers for Disease Control and Prevention (CDC) nation's health protection agency is working to model the virus outbreak with, among others, data-mining firm Palantir Inc., which was credited with helping to find Osama bin Laden. It is worth to mention that during the cholera outbreak in Haiti in 2010, the CDC used Palantir to "monitor the situa-tion and inform their response efforts," according to a white paper later published by Palantir. The company's technology allowed government analysts to "explore text messages" between Haitians and a text platform built by an outside technology company. Other companies that scrape public social media data have contracts in place with the agency and the National Institutes of Health. The coronavirus containment action is in part being coordinated by a task force working in conjunction with the White House, and includes startups as well as tech giants such as Alphabet Inc.'s Google unit, Apple, Facebook Inc. and Amazon.com Inc. (Grind, McMillan and Mathews, 2020). Other efforts are more grassroots, with tech companies pitching state agencies and governments. Hence, the U.S. authorities are considering ways to track hospital bed availability across the country using geolocation data, but also how the data could be aggregated so that personal information of cellphone users wouldn’t be shared. In addition, Facebook is already sharing disease-migration maps to help combat the spread of coronavirus. In a state of emergency such as coronavirus pandemic the U.S., the government has broader authority to request location data from telecom carriers or from Google, which has access to more-precise data belonging to its Android and Google Maps users. This information can’t typically be released without user consent or a court order. Furthermore, Camber Systems, a Washington, D.C., location-tracking startup founded by former government officials, says on its website that it leverages “data, machine learning and artificial intelligence” to help cities manage transportation and infrastructure that may sound like „Songdo reality”. Another firm called Clearview A.I. Inc., a facial-recognition startup that has sparked controversy among privacy advocates over its use by police departments, is in discussions with state agencies about using its technology to track patients infected by the coronavirus, according to people familiar with the matter. The technology has yet to be adopted by any agency, but the New York-based company hopes it will be helpful in what’s known as “contact tracing” – figuring out who else might have been with a person known to have the virus. Another example is provided by the New York-based K. Health Inc. which intends to provide the CDC with aggregated data that would help the agency map where patients in the U.S. are showing the symptoms most indicative of COVID-19, including shortness of breath, fever and cough. The company gathers such data because it offers a chat function powered by artificial intelligence to suggest potential diagnoses for consumers who enter symptoms and other information. What is more the company already offers a version of its map publicly.

In contrast, Massachusetts is the first state followed by California which is building its response around old-school, labour-intensive method; an ambitious contact tracing program, budgeting 44 million USD to hire 1,000 people who are due to make phone calls, text, track people, and ask them to come in for testing. It is to be acknowledged, however, that the human contact tracing, being applied also in Ireland (Wall, 2020), as compared to automation is expensive, can overlook contacts a subject may not recall, and, some argue, is too slow for a fast-moving virus (Barry, 2020).

7 Final remarks

To conclude, it is to be acknowledged that during current Coronavirus crisis tech and government officials are struggling to find a balance between deploying technology and keeping patients’ data – particularly medical information – safe. It is crucial in this respect that governments were transparent about the technology they are using and provide consumers with appropriate safeguards. At the same time, however, some privacy advocates worry that the crisis of the moment could create a new paradigm. That is why, it is of highest importance that adjustment of digital liberties to the emergency situation has to be temporary.

REFERENCES:

1. ALEDORT, J. E. et al. (2007): Non-pharmaceutical public health interventions for pandemic influenza: an evaluation of the evidence base. In: *BMC Public Health*, 2007, 208, 7, pp. 1-9.
2. ASSEMBLÉE NATIONALE (2017): French Anti-terrorism laws. [Online.] In: *Assamblée Nationale*, 2017. [Cited 01.05.2020.] Available online: <www.assemblee-nationale.fr/15/ta-pdf/0164-p.pdf>.
3. BARRY, E. (2020): An Army of Virus Tracers Takes Shape in Massachusetts. [Online.] In: *New York Times*, 2020. [Cited 01.05.2020.] Available online: <https//www.nytimes.com/2020/04/16/us/coronavirus-massachusetts-contact-tracing.html>.
4. Belgian Privacy Commission (2008): Opinion N°17/2008 biometric data.
5. BIGO, D. et al. (2011): Towards a New EU Legal Framework for Data Protection and Privacy Challenges, Principles and the Role of the European Parliament. In: *Report of the High Level Advisory Group on Future of European Home Affairs Policy,* 2011, pp. 40-48.
6. BILDT, C. (2020): Responsibility to report. [Online.] In: *Project Syndicate*, 2020. [Cited 01.05.2020.] Available online: <https://www.project-syndicate.org/commentary/responsibility-to-report-contagious-outbreaks-by-carl-bildt-2020-03>.
7. BROEDERS, D. et al. (2017): Big Data and security policies: Towards a framework for regulating the phases of analytics and use of Big Data. In: *Computer Law and Security Review*, 2017, 33, pp. 309-323.
8. BURT, Ch. (2020): Fever detection technology added to biometric hardware by Dermalog, Telpo, DFI, Hikvision and Kogniz. [Online.] In: *Biometric update*, 2020. [Cited 01.04.2020.] Available online: <https://www.biometricupdate.com/202004/fever-detection-technology-added-to-biometric-hardware-by-dermalog-telpo-dfi-hikvision-and-kogniz >.
9. BUSH, G. W. (2002): "Anti-Terrorism Technology Key to Homeland Security," Remarks at Argonne National Laboratory. [Online.] In: *White House Archive*, 2020. [Cited 20.01.2020.] Available online: <https://georgewbush-whitehouse.archives.gov/news/releases/2002/07/20020722-1.html>.
10. CDC (2020): Community Mitigation Guidelines to Prevent Pandemic Influenza. [Online.] In: *CDC*, 2020. [Cited 01.04.2020.] Available online: <https://stacks.cdc.gov/view/cdc/11425>.
11. CLARKE, R. (1993): Profiling: A hidden challenge to the regulation of data surveillance. In: *Journal of Law, Information and Science*, 1993, 4, 2, p. 403.

12. COHEN, R. (2020): Despotism and Democracy in the Age of the Virus. The battle for humanity and solidarity in the post-American world. [Online.] In: *New York Times*, 2020. [Cited 01.04.2020.] Available online: <https://www.nytimes.com/2020/04/24/opinion/coronavirus-democracy-europe.html>.
13. COSTA, L. (2016): *Virtuality and Capabilities in a World of Ambient Intelligence. New Challenges to Privacy and Data Protection*. Namur: Springer, 2016. 175 p. ISBN 978-3-319-39198-415.
14. DENHAM, E. (2020): Combatting COVID-19 through data: some considerations for privacy. [Online.] In: *ICO*, 2020. [Cited 01.05.2020.] Available online: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/04/combatting-covid-19-through-data-some-considerations-for-privacy/>.
15. ENCYCLOPEDIA BRITANNICA (n.a.): Jack the Ripper. [Online.] In: *Enceclopedia Britannica*, 2015. [Cited 01.09.2020.] Available online: <www.britannica.com/biography/Jack-the-Ripper>.
16. ENERSTVEDT, M. O. (2017): *Aviation Security, Privacy, Data Protection and Other Human Rights: Technologies and Legal Principles*. Springer, 2017. 213 p. ISBN 978-3-319-58139-218.
17. ERLANGER, S. (2020): The Coronavirus Inflicts Its Own Kind of Terror. [Online.] In: *New York Times*, 2020. [Cited 01.04.2020.] Available online: <https://www.nytimes.com/2020/04/06/world/europe/coronavirus-terrorism-threat-response.html>.
18. EUROPEAN COMMISSION (2006): Commission Decision of 28 June 2006 laying down the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States. [Online.] In: *European Commission*, 2006. [Cited 01.09.2020.] Available online: <https://ec.europa.eu/transparency/regdoc/rep/3/2006/DE/3-2006-2909-DE-F-0.Pdf>.
19. FOY, K. (2020): Bluetooth signals from your smartphone could automate Covid-19 contact tracing while preserving privacy. [Online.] In: *MIT News*, 2020. [Cited 01.05.2020.] Available online: <http://news.mit.edu/2020/bluetooth-covid-19-contact-tracing-0409>.
20. GEBREKIDAN, S. (2020): For Autocrats, and Others, Coronavirus Is a Chance to Grab Even More Power. [Online.] In: *New York Times*, 2020. [Cited 01.05.2020.] Available online: <https://www.nytimes.com/2020/03/30/world/europe/coronavirus-governments-power.html>.

21. GERSHGORN, D. (2020): We Mapped How the Coronavirus Is Driving New Surveillance Programs Around the World. [Online.] In: *OneZero*, 2020. [Cited 01.05.2020.] Available online: <https://onezero.medium.com/the-pandemic-is-a-trojan-horse-for-surveillance-programs-around-the-world-887fa6f12ec9>.
22. GOSTIN, L. (2006): Public health strategies for pandemic influenza: ethics and the law. In: *Jama*, 2006, 295, 14, pp. 1700-1704.
23. GRIND, K. – MCMILLAN, R. – MATHEWS, A. W. (2020): To Track Virus, Governments Weigh Surveillance Tools That Push Privacy Limits. [Online.] In: *Wall Street Journal*, 2020. [Cited 01.04.2020.] Available online: <https://www.wsj.com/articles/to-track-virus-governments-weigh-surveillance-tools-that-push-privacy-limits-11584479841>.
24. HUSTINX, P. (2008): *Liberty and Security in Integrated Management of EU Border*. Brussels, 2008.
25. ICAO (2015): Machine Readable Travel Document, Seventh Edition. available online: [Online.] In: *ICAO*, 2015. [Cited 01.05.2020.] Available online: <https://www.icao.int/publications/Documents/9303_p3_cons_en.pdf>.
26. KLEINFELD, R. (2020): Do Authoritarian or Democratic Countries Handle Pandemics Better? [Online.] In: *Carnegie Endowment*, 2020. [Cited 01.05.2020.] Available online: <https://carnegieendowment.org/2020/03/31/do-authoritarian-or-democratic-countries-handle-pandemics-better-pub-81404>.
27. LAI, S. et al. (2020): Effect of non-pharmaceutical interventions for containing the COVID-19 outbreak in China. [Online.] In: *Medrxiv*, 2020. [Cited 01.05.2020.] Available online: <http://www.medrxiv.org/content/10.1101/2020.03.03.20029843v3>.
28. LIU, N. Y. (2012): Bio-privacy. Privacy, Regulations and the Challenge of Biometrics. New York: Routledge, 2012, ISBN 9780203804087 32.
29. MARX, G. T. (1998): What's New About the „New Surveillance"?: Classifying for Change and Continuity. In: *Knowledge, technology and Policy*, 1998, 17, 1, pp. 18-37.
30. METZ, C. (2020): How A.I. Steered Doctors Toward a Possible Coronavirus Treatment. [Online.] In: *New York Times*, 2020. [Cited 01.04.2020.] Available online: <https://www.nytimes.com/2020/04/30/technology/coronavirus-treatment-benevolentai-baricitinib.html>.
31. MOZUR, P. (2020): Inside China's dystopian dreams: A.I., shame and lots of cameras. . [Online.] In: *New York Times*, 2020. [Cited 01.03.2020.] Available online: <https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html>.

32. NEEMAN, A. (2015): Radiation in passenger screening: busting the myths. In: *Aviation Security International*, 2015, 2, p. 13.
33. NEW YORK TIMES (2020): Coronavirus in the U.S.: Latest Map and Case Count. [Online.] In: *New York Times*, 2020. [Cited 01.04.2020.] Available online: <https://www.nytimes.com/interactive/2020/us/coronavirus-us-cases.html>.
34. NEW YORK TIMES (2020): Poland and Hungary Use Coronavirus to Punish Opposition. [Online.] In: *New York Times*, 2020. [Cited 01.05.2020.] Available online: <https://www.nytimes.com/2020/04/22/world/europe/poland-hungary-coronavirus.html>.
35. NORIMITSU, O. N. – MÉHEUT, C. (2020): France Weighs Its Love of Liberty in Fight Against Coronavirus. [Online.] In: *New York Times*, 2020. [Cited 01.04.2020.] Available online: <https://www.nytimes.com/2020/04/17/world/europe/coronavirus-france-digital-tracking.html>.
36. PLOEG van der, I. – SPRENKELS, I. (2011): Migration and Machine-Readable Body: Identification and Biometrics. In: *Migration and the New Technological Borders of Europe*. Palgrave Macmillan 2011, p. 75.
37. QUINLAN, T. (2015): Discrimination: the questionable effectiveness of screening based on race, religion, national origin or behaviour. In: *Aviation Security International*, 2015, 21, p. 36.
38. RASMUSSEN, A. (2020): Taiwan Has Been Shut Out of Global Health Discussions. Its Participation Could Have Saved Lives. [Online.] In: *The Time*, 2020. [Cited 01.05.2020.] Available online: <https://time.com/5805629/coronavirus-taiwan/>.
39. ROTH, K. (2020): Stopping the authoritarian rot in Europe. [Online.] In: *Euobserver*, 2020. [Cited 01.05.2020.] Available online: <https://euobserver.com/opinion/148147>.
40. SATARIANO, A. (2020): Eager to Corral the Coronavirus, U.K. Tests a Disputed Tracing App. [Online.] In: *New York Times*, 2020. [Cited 01.05.2020.] Available online: <https://www.nytimes.com/2020/05/07/world/europe/uk-coronavirus-contact-tracing.html>.
41. SCHMITT, E. (2020): Traces of Terror: Immigration, Ashcroft Proposes Rules for Foreign Visitors. [Online.] In: *New York Times*, 2002. [Cited 01.05.2020.] Available online: <https://www.nytimes.com/2002/06/06/us/traces-of-terror-immigration-ashcroft-proposes-rules-for-foreign-visitors.html>.

42. SINGER, N. – SANG-HUN, S. (2020): As Coronavirus Surveillance Escalates, Personal Privacy Plummets. [Online.] In: *New York Times*, 2020. [Cited 01.05.2020.] Available online: <https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html>.
43. United States Department of Homeland Security (2008): Privacy Impact Assessment for the Future Attribute Screening Technology (FAST) Project.
44. UNIVERSITY OF WASHINGTON (2020): Covidsafe Project at the Washington University: [Online.] In: *University of Washington*, 2020. [Cited 01.05.2020.] Available online: <https://covidsafe.cs.washington.edu/?mod=article_inline>.
45. WALL, M. (2020): Large number of public service staff to be redeployed to contact tracing. [Online.] In: *Irish Times*, 2020. [Cited 01.05.2020.] Available online: <https://www.irishtimes.com/news/health/large-number-of-public-service-staff-to-be-redeployed-to-contact-tracing-1.4212937>.
46. WENLIANG, L. (2020): He Warned of Coronavirus. Here's What He Told Us Before He Died. [Online.] In: *New York Times*, 2020. [Cited 01.05.2020.] Available online: <https://www.nytimes.com/2020/02/07/world/asia/Li-Wenliang-china-coronavirus.html>.
47. WONG, E. – MOZUR, P. (2020): China's 'Donation Diplomacy' Raises Tensions With U.S. [Online.] In: *New York Times*, 2020. [Cited 01.04.2020.] Available online: <https://www.nytimes.com/2020/04/14/us/politics/coronavirus-china-trump-donation.html>.
48. WU, J. – WATKINS, W. D. – GLANZ, J. (2020): How the virus got out. [Online.] In: *New York Times*, 2020. [Cited 01.04.2020.] Available online: <https://www.nytimes.com/interactive/2020/03/22/world/coronavirus-spread.html>.