Collection of Papers
from the International Academic Online Conference
22nd – 23rd of April 2021

TECHNOLOGIES IN TIMES OF CRISIS: THREAT OR OPPORTUNITY TO LAW?

BLF BRATISLAVA LEGAL FORUM 2021

Zborník príspevkov
z medzinárodnej vedeckej online konferencie
22. – 23. apríla 2021

BPF BRATISLAVSKÉ PRÁVNICKÉ FÓRUM 2021

SYMPOSIA, COLLOQUIA, CONFERENCES
SYMPÓZIÁ, KOLOKVIÁ, KONFERENCIE

TECHNOLOGIES IN TIMES OF CRISIS: THREAT OR OPPORTUNITY TO LAW?

BRATISLAVA LEGAL FORUM 2021

BRATISLAVSKÉ PRÁVNICKÉ FÓRUM 2021

Collection of Papers from the International Academic Online Conference
Bratislava Legal Forum 2021
organised by the Comenius University in Bratislava, Faculty of Law
on 22nd – 23rd of April 2021
under the auspices of the Alumni Club of Comenius University in Bratislava, Faculty of Law.

Zborník príspevkov z medzinárodnej vedeckej online konferencie
Bratislavské právnické fórum 2021
organizovanej Univerzitou Komenského v Bratislave, Právnickou fakultou
v dňoch 22. – 23. apríla 2021
pod záštitou
Alumni Klubu Univerzity Komenského v Bratislave, Právnickej fakulty.

UNIVERZITA KOMENSKÉHO
V BRATISLAVE
PRÁVNICKÁ FAKULTA
VYDAVATEĽSKÉ ODDELENIE

Univerzita Komenského v Bratislave
Právnická fakulta
2021

ISBN 978-80-7160-612-3
EAN 9788071606123

CONTENT / OBSAH

DATA GOVERNANCE IN CONNECTED AND AUTOMATED VEHICLES

Jozef Andraško

Comenius University in Bratislava, Faculty of Law

Abstract: The author deals with the issue of data governance in connected and automated vehicles. Firstly, the author defines technical solutions for the governance of vehicle generated data. Furthermore, the author focuses on different categories of vehicle generated data which can be transferred. Secondly, the author is dealing with the issue of access to vehicle generated data.

Keywords: data governance, connected vehicle, automated vehicles

1 INTRODUCTION

Fully automated vehicles when the vehicle does not have a steering wheel and pedals and no driver input is required are a matter of the future. However, connected and partially automated vehicles are a current legal issue due to their development and deployment.

The vehicle that is capable of communicating with other vehicles and other objects like infrastructure receive, produce, process and transmit a huge amount of data. These data are valuable for vehicle manufacturers, public authorities and entities who would like to provide services to users of the car. However, the access is limited to specific in-vehicle data and under some conditions.

The first part of the article introduces the concept of connected and automated vehicles. The second part of the article aims at analyzing data governance in connected and automated vehicles from the point of the current legal framework and related issues.

2 CONNECTED AND AUTOMATED VEHICLES

Connected vehicles can be described as vehicles that are equipped with wireless communication technologies that enable data transfer with other vehicles, infrastructure, or other networks.[1]

In cases when automated vehicles are equipped with communications technology that enables data transfer with other vehicles, infrastructure, or other networks we talk about **the connected and automated vehicle (hereinafter referred to as CAV)** [2]**.**[3]

Automated vehicles do not necessarily need to be connected and connected vehicles do not require automation. However, connectivity will be a major enabler for driverless vehicles.[4]

As stated in EU Communication: On the road to automated mobility: An EU strategy for mobility of the future: "*When vehicles become increasingly connected and automated, they will be able to coordinate their maneuvers, using active infrastructure support and enabling truly smart traffic management for the smoothest and safest traffic flows*."[5]

[1] BSI: Connected and automated vehicles – Vocabulary BSI Flex 1890 v3.0:2020-10, p. 3.

[2] BSI: Connected and automated vehicles – Vocabulary BSI Flex 1890 v3.0:2020-10, p. 3.

[3] For this article, we will use the term CAV or its plural (CAVs). If we want to highlight a fully autonomous vehicle, we will use the term autonomous vehicle.

[4]EU Commission: COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE, THE COMMITTEE OF THE REGIONS On the road to automated mobility: An EU strategy for mobility of the future. p.4.

[5] EU Commission: COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE, THE COMMITTEE OF THE REGIONS On the road to automated mobility: An EU strategy for mobility of the future. p.4. Studies have quantitatively shown that automation without connectivity could lead to a

CAVs rely on data that are created by their in-vehicle technologies, data that are sent from other vehicles or infrastructure, and traffic and infrastructure data sent from public authorities.

CAVs need proper functioning to observe their condition and surrounding environment. For these purposes, different types of **in-technologies** are used in CAVs. In general, there are three types:[6]

a) sensor technologies. Sensor technologies include RADAR (radio detection and ranging)[7], LIDAR (light detection and ranging)[8], VLC[9], infrared system[10] etc.

b) vision technologies. Vision technologies include HD cameras, Stereo Vision System (SVS)[11] etc.

c) positioning technologies. Positioning technologies include GPS, radar cruise control, and radar-based obstacle detections (RBOD).

The aforementioned technologies communicate with other internal components of vehicles like telematics and actuator by different networks. These networks include Flexray, Ethernet networks, Controller Area Network (CAN), etc.[12]

CAVs rely on data that is sent from **other vehicles, road infrastructure**s like C-ITS stations or traffic lights or signs, or other traffic participants (cyclists, pedestrians). CAVs can also use data from devices used inside the vehicle like smartphones, tablets, smartwatches, personal computers.

For these purposes, different types of communication technologies like short-range communication technologies that operate in the dedicated 5.9 GHz frequency band, as well as long-range technologies 3G, 4G, or 5G mobile networks can be used. In that regard, CAV is the connected entity that receives data from an external source and can share data that are recorded with a remote third party for various purposes. Based on the participants in the communication the notion of vehicle-to-everything includes:

- vehicle-to-vehicle (V2V),
- vehicle-to-infrastructure and vice-versa (V2I and I2V),
- vehicle-to-mobile network (V2N) and infrastructure-to-mobile network (I2N),
- vehicle-to-device (V2D),
- vehicle-to-persons (V2P).

Various **public authorities** responsible for road traffic and road infrastructure create and can provide access to these data under some requirements. Road traffic information and infrastructure data include dynamic speed limits, traffic rules, the location of stationary vehicles, road names, condition and availability of roads, length of roads, type of roads, road work warnings, number and position of traffic lights and signs, etc.

The automated vehicle can be described as a vehicle that is using driving automation systems or automated driving systems that can handle some or all dynamic driving tasks within its operational design domain. The driver must be promptly available to take control of the vehicle.

---

potential deterioration of traffic conditions: https://ec.europa.eu/jrc/en/publication/connected-and-automated-vehicles-freewayscenario-effect-traffic-congestion-and-network-capacity

[6] SKIHO, K - SHRESTHA, R. (2020). *Automotive Cyber Security Introduction, Challenges, and Standardization*. Springer Nature Singapore, p. 20.

[7] The RADAR rotates to give a 360-degrees scan of the world. The sensor operates by using radio waves.

[8] The LiDAR consists of GPS, scanner, and laser technology for the generation of 3D information in a specific area. LIDAR (Light Detection And Ranging), which uses light to scan the entire world and give depth to all nearby obstacles in 360 degrees.

[9] The VLC is a visible light-based system for transferring information from one location to another but with a small range of just about 50 m.

[10] Infrared systems provide visual information, as well as the two-dimensional shape of objects. See more LIM, H-Y-F. (2018) *Autonomous Vehicles and the Law: Technology, Algorithms, and Ethics*. Edward Elgar Publishing, p. 11.

[11] SVS using two cameras to see the same object. See more KALA, R. (2020). *On-Road Intelligent Vehicles. Motion Planning for Intelligent Transportation Systems*. Elsevier, p. 15.

[12] See more in SKIHO, K - SHRESTHA,R. (2020). *Automotive Cyber Security Introduction, Challenges, and Standardization*. Springer Nature Singapore, pp. 21-23.

Legal definitions of automated vehicle can be found in EU legislation. Regulation (EU) 2019/2144 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users (hereinafter referred as "**Regulation 2019/2144**")[13] defines an automated vehicle as: "*a motor vehicle designed and constructed to move autonomously for certain periods without continuous driver supervision but in respect of which driver intervention is still expected or required.*"[14]

The regulation in question mentions the concept of a **fully automated vehicle**. In this regard, a fully automated vehicle means: "*a motor vehicle that has been designed and constructed to move autonomously without any driver supervision.*"[15]

Furthermore, automated vehicles and fully automated vehicles have to comply with additional **specific technical specifications** set out in the Commission implementing act. The Commission implementing act will specify technical specification that relates to:[16]

a) systems to replace the driver's control of the vehicle, including signaling, steering, accelerating, and braking;

b) systems to provide the vehicle with real-time information on the state of the vehicle and the surrounding area;

c) driver availability monitoring systems;

d) event data recorders for automated vehicles;

e) harmonized format for the exchange of data for instance for multi-brand vehicle platooning;

f) systems to provide safety information to other road users.

However, those technical specifications relating to driver availability monitoring systems[17], will not apply to fully automated vehicles.[18]

3 DATA GOVERNANCE IN CAV

CAVs can receive, produce, process and transmit a huge amount of data. First of all, these data include in-vehicle data that are produced via sensor technologies, vision technologies, positioning technologies, and within vehicle control units. In-vehicle data include technical data about the vehicle (information about speed, acceleration, air temperature, fuel level, etc.), data about road traffic conditions, data about weather, data about driving behavior, data about the health status of the driver.[19]

In-vehicle data help to ensure the proper operation of the vehicle, checks its proper functioning and identifies and corrects errors, and refines and optimizes vehicle functions. This data can be used for different purposes such as repair and maintenance, road safety and traffic

[13] Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components, and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 (Text with EEA relevance)
PE/82/2019/REV/1

[14] Regulation 2019/2144, Art. 3 (21).

[15] Regulation 2019/2144, Art. 3 (22).

[16] Regulation 2019/2144, Art. 11 (1).

[17] Driver availability monitoring system is defined according to Art. 3 (23) of Regulation 2019/2144 as: "*a system to assess whether the driver is in a position to take over the driving function from an automated vehicle in particular situations, where appropriate.*"

[18] Regulation 2019/2144, Art. 11 (1).

[19] KERBER, W. – GILL, D. (2019). Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation, 10 (2019) *JIPITEC* 244 para 1. p. 247.

management, fleet management, quality management and product development, non-automotive usage (e.g car sharing, car rental, insurance).[20]

These data can be processed in the vehicle and under some circumstances exchanged via communication technologies with other vehicles, infrastructure, vehicle manufacturers.

Secondly, CAVs can receive **data from external sources** (e.g. roadside units, other vehicles).

Last but not least, **data imported** (e.g. phone contact list, destinations for navigation) and **produced** by driver and passengers (visited websites, online shopping preferences, etc.) are included.

The vehicle generated data and data produced by driver or passengers are valuable not only for vehicle manufacturers but also for public authorities (e.g. road traffic data) and entities who would like to provide services to users of the car (e.g. automotive aftermarket services, online shopping, insurance, etc.).[21]

CAVs data create new innovative services in the field of vehicle repair and maintenance (remote monitoring of the vehicle operation, remote diagnostics, remote and predictive maintenance, and repair services), navigation services, parking apps, online shopping, or insurance services. However, to provide these services, access to in-vehicle data and vehicle resources is necessary. In some cases, access to real-time vehicle data will be required.[22]

From the technical point of view, there are different concepts for access to in-vehicle data. First of all, **the extended vehicle concept** is widely used by many vehicle manufacturers. The extended vehicle concept allows accessing vehicle data via different types of interfaces depending on the purpose for which access is sought. Firstly, the concept in questions includes **OBD (on-board diagnostic)** interface where data for diagnosis and repair purposes can be accessed. Secondly, vehicle data can be accessed via **a web interface** for third-party services. In-vehicle generated data are transferred over a secure and encrypted communication channel (e.g. mobile telecom network) to a proprietary external server of the vehicle manufacturer. In this regard, vehicle manufacturers have exclusive, direct, full, and privileged control of data on their proprietary server and to whom access to data will be granted. Transferred data are usually in filtered and aggregated form. Vehicle manufacturers have also privileged, direct access to the driver´s dashboard (human-machine interface, HMI). Access to vehicle data and their use will require a B2B agreement between the service provider and vehicle manufacturer. Last but not least, the extended vehicle concept includes **an ad hoc communication interface** under the responsibility of the vehicle manufacturer (e.g. transfer of data for purposes of intelligent transport systems).[23]

Secondly, **the shared data server** concept is based on the idea that a neutral entity has control of the server and can grant non-discriminatory access to vehicle data. The data made available to the shared data server will be of the same quality as the data available on the vehicle manufacturer´s proprietary server. However, vehicle manufacturers will decide which data will be transferred from their proprietary server to the shared server. The vehicle manufacturer is privileged to directly display services to the consumer via the vehicle HMI.[24]

---

[20] ACEA position Paper (2016). Access to vehicle data for third-party services, p. 3.

[21] KERBER, W. – GILL, D. (2019). Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation, 10 (2019) *JIPITEC* 244 para 1. p. 248.

[22] Access to in-vehicle resources includes IT systems, sensors, telematics systems, and the human-machine interface (dashboard). In cases of remote diagnostics, remote and predictive maintenance and repair services not only reading (downloading data) but especially writing data for updating or reconfiguring of software is necessary. See more KERBER, W. – GILL, D. (2019). Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation, 10 (2019) *JIPITEC* 244 para 1. p. 248. KERBER, W. (2018). Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data, 9 (2018) *JIPITEC* 310 para 1.

[23] ACEA position Paper (2016). Access to vehicle data for third-party services, pp. 3-5. Commission´s final report on Access to In-vehicle Data and Resources, 2016, p. 45.

[24] ACEA position Paper (2016). Access to vehicle data for third-party services, pp. 3-5. Commission´s final report on Access to In-vehicle Data and Resources, 2016, p. 6. Commission´s final report on Access to In-vehicle Data and Resources, 2016, p. 205.

Thirdly, **on-board application platform.** In this technical solution, the vehicle is considered as a platform where data are stored in the vehicle. The car owner will decide to whom to grant access to in-vehicle data and who is allowed to provide services directly to car users. This platform should support different functionalities directly from the HMI.[25]

Vehicle manufacturers are strictly against the onboard application platform because of security and safety issues that could be created by giving any third-party uncontrolled access to vehicle data and resources. In this regard, vehicle manufacturers are willing to grant access to specific vehicle data to third parties based on B2B contract when strict requirements for data security and product safety will be met.[26]

At the EU level, access and use of in-vehicle data are heavily discussed, especially as a part of a cooperative intelligent transport system platform. Commission´s final report on Access to In-vehicle Data and Resources defined five guiding principles that should apply to access to in-vehicle data and resources. According to one of these principles' vehicle user (data subject) decides if data can be provided and to whom, including the concrete purpose for the use of the data. Another principle states that all service providers should be in an equal, fair, reasonable, and non-discriminatory position to offer services to the vehicle user.[27]

Current EU legal regulation of access to vehicle generated data[28] deals with access to vehicle OBD information[29] and vehicle repair and maintenance information[30] rather than general access to vehicle-generated data or data produced by vehicle users. Vehicle manufacturers are obliged to provide to independent operators[31] unrestricted, standardized, and non-discriminatory access to vehicle OBD information and vehicle repair and maintenance information. Non-discriminatory access

[25] KERBER, W. (2018). Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data, 9 (2018) *JIPITEC* 310 para 1, p. 2018.

[26] ACEA position Paper (2016). Access to vehicle data for third-party services, pp. 3-5. Commission´s final report on Access to In-vehicle Data and Resources, 2016, pp. 5-7.

[27] Commission´s final report on Access to In-vehicle Data and Resources, 2016, p. 150. Other principles deal with compliance with data privacy and data protection, tamper-proof access and liability, and standardized access and interoperability.

[28] Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components, and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC (hereinafter referred to as the "Vehicle type approval regulation").

[29] According to Art. 3 (49) of the Vehicle type approval regulation is vehicle OBD information defined: "as *the information generated by a system that is on board a vehicle or that is connected to an engine, and that is capable of detecting a malfunction, and, where applicable, is capable of signaling its occurrence by means of an alert system, is capable of identifying the likely area of malfunction by means of information stored in computer memory, and is capable of communicating that information off-board."*

[30] Under Art. 3 (48) of the Vehicle type approval regulation vehicle repair and maintenance information: "*means all information, including all subsequent amendments and supplements thereto, that is required for diagnosing, servicing, and inspecting a vehicle, preparing it for roadworthiness testing, repairing, re-programming, or re-initializing of a vehicle, or that is required for the remote diagnostic support of a vehicle or the fitting on a vehicle of parts and equipment, and that is provided by the manufacturer to his authorized partners, dealers, and repairers or is used by the manufacturer for the repair and maintenance purposes."*

[31] Under Art. 3 (45) of the Vehicle type approval regulation is independent operator: "*a natural or legal person, other than an authorized dealer or repairer, who is directly or indirectly involved in the repair and maintenance of vehicles, and include repairers, manufacturers, or distributors of repair equipment, tools or spare parts, as well as publishers of technical information, automobile clubs, roadside assistance operators, operators offering inspection and testing services, operators offering training for installers, manufacturers and repairers of equipment for alternative-fuel vehicles; it also means authorized repairers, dealers, and distributors within the distribution system of a given vehicle manufacturer to the extent that they provide repair and maintenance services for vehicles in respect of which they are not members of the vehicle manufacturer's distribution system;"*

also applies to remote diagnosis services used by vehicle manufacturers and authorized dealers and repairers. However, it has to be interpreted in the way that independent operators do not have remote access to in-vehicle data and resources but rather have access to the results of the diagnostic services. Thus, independent operators are not allowed to provide their repair and maintenance services. Additionally, information will be presented in an easily accessible manner in the form of machine-readable and electronically processable datasets. [32]

4 CONCLUSIONS

Fully automated vehicles are a matter of the future, however, connected and partially automated vehicles are a current legal issue due to their development and deployment. EU aims to provide the CAVs manufacturers sound legal environment and become the leader in regulatory innovations and attract economic stimulations.

In-vehicle data include technical data about the vehicle, data about road traffic conditions, data about weather, data about driving behavior, data about the health status of the driver. In-vehicle data help to ensure the proper operation of the vehicle, checks its proper functioning and identifies and corrects errors, and refines and optimizes vehicle functions. Furthermore, this data can be used for different purposes such as repair and maintenance, road safety and traffic management, fleet management, quality management and product development, non-automotive usage (e.g car sharing, car rental, insurance).

Processing of data and related data governance is fundamental to the development and use of CAV. As discussed in the article, manufacturers of CAVs are quite reluctant to allow access to data for third parties. The current legislation provisions ensure access only to maintenance and repair data for independent operators.

Current EU legal regulation of access to vehicle generated data deals with access to vehicle OBD information and vehicle repair and maintenance information rather than general access to vehicle-generated data or data produced by vehicle users.

In order to achieve the goal of full automation, it will be necessary to provide easier access to in-vehicle data. In this regard, it will be necessary to define categories of data that can be made available. Furthermore, purpose for which it is used and if these data are used for public interest or commercial interest have to be taken into account.

Bibliography:

ACEA position Paper (2016). Access to vehicle data for third-party services Commission´s final report on Access to In-vehicle Data and Resources, 2016.

BSI: Connected and automated vehicles – Vocabulary BSI Flex 1890 v3.0:2020-10.

KERBER, W. – GILL, D. (2019). Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation, 10 (2019) *JIPITEC* 244.

KERBER, W. (2018). Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data, 9 (2018) *JIPITEC* 310.

SKIHO, K - SHRESTHA, R. (2020). *Automotive Cyber Security Introduction, Challenges, and Standardization*. Springer Nature Singapore.

LIM, H-Y-F. (2018) *Autonomous Vehicles and the Law: Technology, Algorithms, and Ethics*. Edward Elgar Publishing.

Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components, and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC.

[32] Vehicle type approval regulation, Art. 61 (1).

Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components, and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users.

EU Commission: COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE, THE COMMITTEE OF THE REGIONS On the road to automated mobility: An EU strategy for mobility of the future.

Commission´s final report on Access to In-vehicle Data and Resources, 2016.

Contact:
JUDr. Jozef Andraško, PhD.
jozef.andrasko@flaw.uniba.sk
Comenius University in Bratislava, Faculty of Law
Šafárikovo nám. č. 6
P. O. Box 313
810 00 Bratislava
Slovak Republic

RULE OF LAW IN THE LIGHT OF NEW TECHNOLOGY - IN TIME OF CRISIS

Mgr. Zoltán Gyurász

Univerzita Komenského v Bratislave, Právnická fakulta

Abstract: Our world is facing an unprecedented crisis. At its core with global public health emergency on a scale not seen for centuries. But in this connected world, innovation is happening continuously playing an important role in responding to the challenges posed by the pandemic. Through the last decade, work with data has increased the potential of technology dramatically, and now new technologies are able to play a crucial role during the time of crisis and disasters. But how will the use of new technology cope in the light of the concept of "rule of law"

Abstrakt: Náš svet čelí bezprecedentnej kríze. Globálna pandemická situácia akú náš svet nevidel po celé storočia. V tomto prepojenom svete však neustále prebiehajú inovácie, ktoré zohrávajú dôležitú úlohu pri reakcii na výzvy, ktoré predstavuje pandémia. Počas posledného desaťročia práca s dátami dramaticky zvýšila technologický potenciál nových technológií, ktoré tak môžu v čase krízy a katastrof teraz hrať rozhodujúcu úlohu. Ako sa však vysporiada s používaním nových technológií vo svetle idey právneho štátu.

Key words: Rule of law, Technology, Crisis

Kľúčové slová: Právny štát, Technológie, Kríza

1. INTRODUCTION

Plato is credited for coining the phrase "*Necessity is the mother of invention*," and often a crisis acts as the forcing mechanism to compel expeditious innovation, leading to rapid advances in technology, policy, and/or procedures. But not to stop at one quote, President John F. Kennedy in his 1959 speech[1] famously said: "*When written in Chinese, the word 'crisis' is composed of two characters one represents danger and one represents opportunity*." Although today it is widely recognized that this is not the correct interpretation of the Chinese characters, President Kennedy's point about a crisis yielding unique opportunities may be more important than ever.

Crises are generally viewed as dangerous, expensive, and detracting from other important agendas and priorities. However, a brief look back in history illustrates that crises and extreme threats can be useful for directing individuals, a country, and even the world to a solution. As President Kennedy suggested, out of crises can emerge new and incredible opportunities, particularly if traditional approaches and paradigms are questioned and challenged. During a crisis, incentives, and motivations change, potentially leading to new behaviors. Crises can get the collective adrenaline flowing, focusing minds to solve the problem at hand.[2] As mentioned earlier, a brief look back in history quickly reveals numerous ways that crises have offered unexpected benefits for societies, countries, and humanity. The measures taken to survive and eventually end a crisis often make the society stronger and more resilient for future events. Large scale crises that challenge multiple interests and equities have a way of pulling together diverse allies and rivals alike to solve the crisis. Sometimes

[1] Remarks of Senator John F. Kennedy, Convocation of the united negro college fund, INDIANAPOLIS, INDIANA, APRIL 12, (1959). Available at: https://www.jfklibrary.org/archives/other-resources/john-f-kennedy-speeches/indianapolis-in-19590412.

[2] From the Deep-Water Horizon collapse to the Fukushima meltdown, look closer in LANGEN-RIEKHOF, M – AVANNI, A – JANETTI, A.: Sometimes the world needs a crisis: Turning challenges into opportunities, (2017).

the fear generated from a crisis and corresponding public outcry enables and even forces leaders to make bold and often difficult policy moves, even in countries not involved in or affected by the crisis.[3]

2. RULE OF LAW

If we would ask any lawyer they will tell you that the "Rule of Law" is not only one of the basic values of the European Union, but also one of the fundamental principles of the member states' legal system, and a part of what the European Court of Justice sees as the "European constitutional heritage".[4] They might generally concur that the "Rule of Law" should be approached within the notion of a ruling, that is, a relationship between ruler and ruled, the stuff of constitutional history.

There is belief that a society blessed with the prevalence of the "Rule of Law" stand free from three tyrannies. Firstly, the tyranny of fear, which means that no individual may be arbitrarily treated, punished nor imprisoned by the State, nor by the powerful. Secondly, the tyranny of the few, which means that no King, Minister, nor wealthy men is above the law. Lastly, and the tyranny of the majority, which means that no minority group may be persecuted with impunity, just because there is a majority that whishes so. Throughout centuries of struggle and contestation, European countries have fine-tuned the specific ramifications of such social ideals, as well as they believe, "exported" it to the rest of the world. As a result, the "Rule of Law" is considered to be a core pillar of the European Union and by implication a core benchmark for accession by candidate countries.[5]

Yet, despite the importance of these rationales, the concept "Rule of Law" does not seem to prevail today within its own jurisdiction. Some would argue that this is true of older member states, thus reducing their ability to promote the "Rule of Law" without being accused of hypocrisy.[6]

3. RULE OF LAW IN TIME OF CRISIS

The world is facing an unprecedented crisis. At its core is a global public health emergency on a scale not seen for a century, requiring a global response with far-reaching consequences for our economic, social, and political lives. The priority is to save lives. In view of the exceptional situation and to preserve life, countries have no choice but to adopt extraordinary measures[7]. Extensive lockdowns, adopted to slow transmission of the virus, restrict by necessity freedom of movement and, in the process, freedom to enjoy many other human rights. Such measures can inadvertently affect people's livelihoods and security, their access to health care (not only for COVID-19), to food, water and sanitation, work, education – as well as to leisure. Measures need to be taken to mitigate any such unintended consequences. State authorities are having to deploy maximum resources to combat the spread of the disease and protect lives. Decisions are being made at speed and, even though well-intended, some can inadvertently have adverse consequences. Responses must be proportionate to the pandemic to preserve the trust that needs to exist between people and their government, especially during a crisis.

Observing the crisis and its impact through the lens of rule of law puts a focus on how it is affecting people on the ground, particularly the most vulnerable among us, and what can be done about it now, and in the long term. The public health crisis is fast becoming an economic and social crisis and a protection and human rights crisis rolled into one. In some, ongoing crises, especially armed conflict, put human rights and other international legal protections under extra pressure. The COVID-19 crisis has exacerbated the vulnerability of the least protected in society. It is highlighting deep economic and social inequalities and inadequate health and social protection systems that

[3] Ibid.

[4] NICOLAIDIS, K. – KLEINFELD, R.: Rethinking Europe's « Rule of Law » and Enlargement Agenda: The Fundamental Dilemma, SIGMA Papers, (2012).

[5] Look closer, LYSINA, P.: PRÁVNY ŠTÁT AKO SPOLOČNÁ HODNOTA ČLENSKÝCH ŠTÁTOV EURÓPSKEJ ÚNIE? Zborník z medzinárodnej vedeckej konferencie Bratislavské právnické fórum (2020).

[6] NICOLAIDIS, K. – KLEINFELD, R.: Rethinking Europe's « Rule of Law » and Enlargement Agenda: The Fundamental Dilemma, SIGMA Papers, (2012).

[7] For the national measures look closer, Koronavírus a Slovensko: Všetky dôležité a aktuálne informácie o ochorení COVID−19 a o opatreniach, ktoré Slovensko prijíma v boji proti nemu. (2021) Available at: https://korona.gov.sk.

require urgent attention as part of the public health response.[8] This is not a time to neglect human rights, it is a time when, more than ever, human rights are needed to navigate this crisis in a way that will allow us, as soon as possible, to focus again on achieving equitable sustainable development and sustaining peace. The pandemic has led to countries imposing emergency and security measures. While in most cases these are needed to fight the virus, they can also be politically driven and may be easily abused. The pandemic could provide a pretext to undermine democratic institutions, quash legitimate dissent or disfavored people or groups, with far-reaching consequences that we will live with far beyond the immediate crisis.

Although coercive measures may be justified in certain situations, they can backfire if applied in a heavy-handed, disproportionate way, undermining the whole pandemic response itself.[9] The type of instability created by this public health emergency requires peace and stability to be maintained. Fairness, justice, and respect for the rule of law are needed to strengthen and support the national effort on the public health front.[10]

4. RULE OF LAW IN LIGHT OF NEW TECHNOLOGY - IN TIME OF CRISIS

The digital revolution at the end of the 20th century brought information to our fingertips, enabling us to make faster, better, and more efficient decisions than ever before in our history. Today, in the era of new technology our lives are becoming more and more intertwined with intelligent devices, and our society is only slowly getting used to this "new normal". Through the last decade, work with data[11] has increased the potential of new technology dramatically. This has been made possible by everything being connected and accessible online through digital devices and sensors. Today we have data from possibly every source and in every form.[12] Nevertheless, with the pandemic, the world we live in is changing dramatically again and there are significant adjustments to be made. New technologies offer enormous potential to help with the fight against COVID-19, including finding a cure or vaccine and analyzing the spread of the disease[13]. Positioning technologies play a crucial role during the time of crisis and disasters. Government agencies and first responders require precise positions to accurately assess the situation, pinpoint the riskiest areas, and carry out tasks accordingly.[14] However, use of technologies, including artificial intelligence and big data, to enforce emergency and security restrictions or for surveillance and tracking of impacted populations raise concerns.[15]

The potential for abuse of new technology in time of crisis is high[16]. What's even worse, is the idea that what is justified during an emergency now may become normalized once the crisis has

[8] Look closer, Human Rights Dimensions of COVID-19 Response, (2020). Available at: https://www.hrw.org/news/2020/03/19/human-rights-dimensions-covid-19-response.

[9] In most of the countries across the globe, people protested against the measures such as lockdowns and masks. Look closer, Mapping coronavirus anti-lockdown protests around the world, (2021) Available at: https://www.aljazeera.com/news/2021/2/2/mapping-coronavirus-anti-lockdown-protests-around-the-world.

[10] Human Rights Dimensions of COVID-19 Response, (2020) Available at: https://www.hrw.org/news/2020/03/19/human-rights-dimensions-covid-19-response.

[11] Look closer: ANDRAŠKO, MESARČÍK: Právne aspekty otvorených údajov (2020) C. H. Beck SK, ISBN 9788089603794

[12] KRASADAKIS, G: Technology Innovation — Trends and Opportunities (2017) Available https://medium.com/innovation-machine/2018-innovation-trends-and-opportunities-8a5d642fd661

[13] Look closer, KHAN, S: Predicting the coronavirus outbreak: How AI connects the dots to warn about disease threats, (2020) available: https://theconversation.com/predicting-the-coronavirus-outbreak-how-ai-connects-the-dots-to-warn-about-disease-threats-130772.

[14] CHATURVEDI, A: The China way: Use of technology to combat Covid-19 (2020) Available: https://www.geospatialworld.net/article/the-sino-approach-use-of-technology-to-combat-covid-19/.

[15] Look closer, MESARČÍK, M. – GYURÁSZ, Z.: Umelá inteligencia a právna úprava zdravotníctva v Slovenskej republike. 1. vydanie. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2020.

[16] Look closer, GYURÁSZ, Z.: Technology: the great divider, Crisis as a challenge for human rights [elektronický dokument]-:1. vyd. ISBN 978-80-7160-551-5. - Bratislava: Univerzita Komenského v Bratislave, 2020. - S. 463-478 [online], (2020). Available at:

passed. Without adequate safeguards, these powerful technologies may cause discrimination, be intrusive and infringe on privacy, or may be deployed against people or groups for purposes going far beyond the pandemic response. The pandemic is impacting every country, but some countries face existing peace and security challenges that make their response even more difficult. Combined with existing instability, the pandemic poses a real threat to peace and security, can undermine peacebuilding gains, and heighten conflict risks over time. Other actors may seek to take advantage of the crisis for political ends.[17]

Therefore, all measures must incorporate meaningful data protection safeguards, and just as always be lawful, necessary, and proportionate, time-bound and justified by legitimate public health objectives.[18] The COVID-19 pandemic has brought many challenges for our society. We believe that modern technologies are an essential tool for solving many practical issues in a more efficient way, that we have encountered recently. Nevertheless, there are still significant legal limitations of the use of some of these new technologies, we cannot forget that as with any new filed which must be regulated, it will take time and effort to come to a satisfying end.

5. CONCLUSION

Our world is facing an unprecedented crisis. In view of the exceptional situation and to preserve life, countries have no choice but to adopt extraordinary measures. Extensive lockdowns adopted to slow transmission of the virus, restrict by necessity freedom of movement, and, in the process, freedom to enjoy many other human rights. Although coercive measures may be justified in certain situations, they can backfire if applied in a heavy-handed, disproportionate way, undermining the whole pandemic response itself.

The type of instability created by this public health emergency requires peace and stability to be maintained. Fairness, justice, and respect for the rule of law are needed to strengthen and support the national effort on the public health front. The concept of Rule of Law is not only one of the basic values of the European Union, but also one of the fundamental principles of the member states' legal system, and a part of what the European Union sees as the "European constitutional heritage" Therefore, all measures must incorporate meaningful data protection safeguards, be lawful, necessary, and proportionate, time-bound and justified by legitimate public health objectives. The COVID-19 pandemic has brought many challenges for our society.

We believe that modern technologies are an essential tool for solving many practical issues in a more efficient way, than we have encountered recently. Nevertheless, there are still significant legal limitations of the use of some of these new technologies, we cannot forget that as with any new field which must be regulated, it will take time and effort to come to a satisfying end.

REFERENCES

ANDRAŠKO, J. a kol. Právo informačných a komunikačných technológií 2. Bratislava: TINCT, 2021, s. 328

ANDRAŠKO, MESARČÍK: Právne aspekty otvorených údajov (2020) C. H. Beck SK, ISBN 9788089603794

ANTONIO, R.: LEGAL KNOWLEDGE & INFORMATION SYSTEMS, 2017 IOS Press; 1 edition

APC: Supporting human rights online in times of crisis: A collection of useful resources, 2020 Available at: https://www.apc.org/en/news/supporting-human-rights-online-times-crisis-collection-useful-resources

CHATURVEDI, A: The China way: Use of technology to combat Covid-19 (2020) Available: https://www.geospatialworld.net/article/the-sino-approach-use-of-technology-to-combat-covid-19/

FÁBRY, B. - KASINEC, R. - TURČAN, M.: TEÓRIA PRÁVA. Bratislava: Wolters Kluwer, 2019

https://www.flaw.uniba.sk/fileadmin/praf/Veda/Zborniky/Crisis_as_a_challenge_for_human_rights.pdf

[17] Human Rights Dimensions of COVID-19 Response, (2020) Available at: https://www.hrw.org/news/2020/03/19/human-rights-dimensions-covid-19-response.

[18] NICOLAIDIS, K. – KLEINFELD, R.: Rethinking Europe's « Rule of Law » and Enlargement Agenda: The Fundamental Dilemma, SIGMA Papers, (2012).

Human Rights Dimensions of COVID-19 Response, 2020 Available at: https://www.hrw.org/news/2020/03/19/human-rights-dimensions-covid-19-response
GYURÁSZ, Z.: Technology: the great divider, Crisis as a challenge for human rights [elektronický dokument]. - : 1. vyd. ISBN 978-80-7160-551-5. - Bratislava : Univerzita Komenského v Bratislave, 2020. - S. 463-478 [online], 2020. Available at: https://www.flaw.uniba.sk/fileadmin/praf/Veda/Zborniky/Crisis_as_a_challenge_for_human_rights.pdf
HUSOVEC, M. - MESARČÍK, M. - ANDRAŠKO, J.: Právo informačných a komunikačných technológií 1. Bratislava: TINCT, 2020. 262 s.

KHAN, S: Predicting the coronavirus outbreak: How AI connects the dots to warn about disease threats, (2020) available: https://theconversation.com/predicting-the-coronavirus-outbreak-how-ai-connects-the-dots-to-warn-about-disease-threats-130772
KRASADAKIS, G: Technology Innovation — Trends and Opportunities(2017) Available https://medium.com/innovation-machine/2018-innovation-trends-and-opportunities-8a5d642fd661
LANGEN-RIEKHOF, M – AVANNI, A – JANETTI, A.: Sometimes the world needs a crisis: Turning challenges into opportunities, 2017 Available at: https://www.brookings.edu/research/sometimes-the-world-needs-a-crisis-turning-challenges-into-opportunities/
LUDOW, K. - BOWMAN, M.D. - GAFOT, J. - BENNETT, G. M.: Regulating Emerging and Future Technologies in the Present, Springer, 2015.
LYSINA, P.: PRÁVNY ŠTÁT AKO SPOLOČNÁ HODNOTA ČLENSKÝCH ŠTÁTOV EURÓPSKEJ ÚNIE? Zborník z medzinárodnej vedeckej konferencie Bratislavské právnické fórum 2020
Mapping coronavirus anti-lockdown protests around the world, 2021 Available at: https://www.aljazeera.com/news/2021/2/2/mapping-coronavirus-anti-lockdown-protests-around-the-world
MESARČÍK, M. – GYURÁSZ, Z.: Umelá inteligencia a právna úprava zdravotníctva v Slovenskej republike. 1. vydanie. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2020.
NICOLAIDIS, K. – KLEINFELD, R.: Rethinking Europe's « Rule of Law » and Enlargement Agenda: The Fundamental Dilemma, SIGMA Papers, 2012

Contact information:

Mgr. Zoltán Gyurász
zoltan.gyurasz@flaw.uniba.sk
Univerzita Komenského v Bratislave
Právnická fakulta
Šafárikovo námestie 6,
810 00
Bratislava

DIGITAL COVID PASS WITHIN THE EIDAS REGULATION AND SLOVAK E-GOVERNMENT

Kristian Hodossy

Comenius University Bratislava, Faculty of Law

Abstract
The pandemic has been bringing up many legal matters which have to be considered unsolved, and yet it is possible to detect and experience legislation in a super fast legislative process. The pace of the legislation that is having an attitude to reinstate the basic principles of the functioning of European Union has to cause legal uncertainties and legal issues within the impementation in member states. The topic of covid pass is such a case. The case of covid pass entitles the public to expect a „light at the end of the tunnel" in getting back to normal lives. The legal expertise including academics have to outline the legal risks and questions which are closely related.

Key words: Identification. Authentification.Covid. Passport. Digital.

1. Introduction

The pandemic situation is lasting since the beginning of 2020, which therefore causes initiatives that would otherwise not be significant and absolutely unnecessary for the functioning of the society. To ensure and restore some of the basicn freedoms and principles of European union, the issue of covid pass or green covid pass is brought up by the European commission (hereinafter referred to as „***EC***"). The iniciative is considered to be a „ice breaker", but the necessary caution is definitively welcome.

The proposed regulation governing the basic principles and condition of the green covid pass will be drafted and submitted to the EC and after being agreed upon and confirmed by the EC transferred to the European parliament. Hence do I believe that the necessity to have an identifier for the purposes of the covid era and for the purpose of protection of public health is outweighing the possible risks, the legal aspects shall be identified and subjected to a legal scrutiny.

The article will be subject to legal matters of the green covid pass. I will evaluate the possible identification and authtentification aspects of the so called unique identifier. Apart from the way of identifying and authentifying the holder of the covid pass, the EC must definitely focus on the legal issues which are to be in place in relation to the way of having a common repositary for the purposes of what IT token can be cosindered a covid pass, way of integrating the information sytems of the member states as soon as the data will be accessed by designated officials.

Other then the e-government processing legal issues, the article must evaluate the data accessibility position of the member states. The processing of personal data espacially sensitive data must be scrutinised to the extent, that no personal data breach will be committed. Identification and authentification considering the legal specifics of each member states will be evaluated from the prospective of Slovak e-government.

After taken into consideration the complexity and timeliness of the topic the hypothesis of the article is „***digital covid pass is causing legal disruption in the process of identification and authentification and in the process of sensitive personal data protection***".

This article was drafted with the support from a grant awarded by the Slovak Research and Development Agency No. APVV – 17 – 0403 Effects of Mutual Recognition of Electronic Identification Means on Electronic Services of Public Administration and is included in a research task.

2. Green covid pass – basic principles

To comply with the measures to limit the spread of the coronavirus, travellers in the EU have been asked to provide various documents, such as medical certificates, test results, or declarations. The absence of standardised formats has resulted in travellers experiencing problems when moving within the EU. There have also been reports of fraudulent or forged documents. Therefore the era of a green covid pass is being lived by EU citizens willing to travel across the border of EU.

The right of EU citizens to move and to reside freely within the European Union is one of the EU's most cherished achievements, and an important driver of its economy. Pursuant to Article 21 of the Treaty on the Functioning of the European Union (hereinafter referred to as „***TFEU***"), every EU citizen has the right to move and reside freely within the territory of the member states, subject to the limitations and conditions laid down in the Treaties and by the measures adopted to give them effect. However, some of the restrictions adopted by the member states in order to limit the spread of severe acute respiratory syndrome coronavirus 2 ('SARS-CoV2'), which causes covid 19, have had an impact on citizens' right to free movement. These measures often consisted of restrictions on entry or other specific requirements applicable to cross-border travellers, such as to undergo quarantine or self-isolation or to be tested covid infection prior to and/or after arrival.

The green covid pass whcih is in fact a digital certificate (hereinafter referred to as „***green covid pass***" will be considered a proof that a person has been vaccinated against COVID-19, received a negative test result or recovered from COVID-19. The green covid pass will be an accapted and preferred solution of providing and enabling EÚ citizens their most affected and EÚ fundamental principle incorporated in the right to freely move inside the EU borders. It will be available, free of charge, in digital or paper format. It will include a QR code to ensure security and authenticity of the certificate. The EC will construct some kind of a gateway, which shall be created in such a way that it ensures all certificates can be verified across the EU, and support member states of EÚ in the technical implementation of certificates. Member states will be in line with the green covid pass responsible for implementing the the forthcoming legislation. EU member must remain responsible to decide which public health restrictions can be waived for travellers but will have to apply such waivers in the same way to travellers holding a green covid pass.

It has been publicly announce by EÚ representatives : *"The Digital Green Certificate offers an EU-wide solution to ensure that EU citizens benefit from a harmonised digital tool to support free movement in the EU. This is a good message in support of recovery. Our key objectives are to offer an easy to use, non-discriminatory and secure tool that fully respects data protection. And we continue working towards international convergence with other partners."*[1]

Key elements of the proposed EC regulation are the following:

a) Accessible and secure certificates for all EU citizens:

- ***The green covid pass (it means a certificate will cover three types of certificates****)– vaccination certificates, test certificates, and certificates for persons who have recovered from vocid.*
- ***The certificates will be issued in a digital form or on paper.*** *Both will have a QR code that contains necessary key information as well as a digital signature to make sure the certificate is authentic.*
- ***The EC will build a gateway*** *and support member states to develop software that authorities can use to verify all certificate signatures across the EU. No personal data of the certificate holders passes through the gateway, or is retained by the verifying Member State.*
- ***The certificates will be available free of charg****e and in the official language or languages of the issuing Member State and English.*[2]

[1] Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1181 (28.04.2021)

[2] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination,

b) Non-discrimination:

- **All EU citizens – vaccinated and non-vaccinated – should benefit from a green covid pass** when travelling in the EU. To prevent discrimination against individuals who are not vaccinated, the Commission proposes to create not only an interoperable vaccination certificate, but also test certificates and certificates for persons who have recovered from covid.
- **Same right for travellers with the green covid pass** –member states will accept proof of vaccination to waive certain public health restrictions such as testing or quarantine, they would be required to accept, under the same conditions, vaccination certificates issued under the gree covid pass certification system. This obligation would be limited to vaccines that have received EU authorisation, which means EU official controlling process must have been processed in relation to the vaccines. The regulation is morover providing space for certain exceptions, which are based on the decision of Member States. In other words, member states are allowed to provide exceptions to EU citizens which have chosen a non authorised vaccine by the EU officials.
- **Notification of other measures** – if a member state continues to require holders of a green covid pass further obligation prior to entering the country such as quarantine or test, a notofication process will be conducted and EC will evalute it.

c) Only essential information and secure personal data:

- **The certificates will include a limited set of information** such as name, date of birth, date of issuance, relevant information about vaccine/test/recovery and a unique identifier of the certificate. This data can be checked only to confirm and verify the authenticity and validity of certificates.

In parallel, Member States must implement the **trust framework** and technical standards, agreed in the eHealth network, to ensure timely implementation of the Digital Green Certificate, their interoperability and full compliance with personal data protection. To ensure a well-coordinated, predictable and transparent approach to the adoption of restrictions on freedom of movement, the Council adopted, on 13 October 2020, Council Recommendation (EU) 2020/1475 on a coordinated approach to the restriction of free movement in response to the COVID-19. The Council Recommendation established a coordinated approach on the following key points:
a) the application of common criteria and thresholds when deciding whether to introduce restrictions to free movement,
b) mapping of the risk of COVID-19 transmission, published by the European Centre for Disease Prevention and Control (ECDC)2 , based on an agreed colour code, and
c) coordinated approach as to the measures, if any, which may appropriately be applied to persons moving between areas, depending on the level of risk of transmission in those areas.

Part of the whole green covid pass preparation proces is the trust framework, which is being worked on by the commission and member states in the eHealth Network, a voluntary network connecting national authorities responsible for eHealth, on preparing the interoperability of vaccination certificates.

The eHealth Network adopted adopted Guidelines on proof of vaccination for medical purposes, which it updated on 12 March 20216 . These guidelines define the central interoperability elements, namely a minimum dataset for vaccination certificates, and a unique identifier. The eHealth Network and the Health Security Committee have also been working on a common standardised set of data for COVID-

testing and recovery to facilitate free movement during the COVID-19 pandemic (Digital Green Certificate).

19 test result certificates, guidelines on recovery certificates and respective datasets, and an outline on the interoperability of health certificates. [3] The guidelines on proof of vaccination for medical purposes is designed to follow the principle:

a) simplcity,
b) flexibility,
c) rigorous protection of personal data
d) step wise approach.

2.1 Trust framework

Pursuant to the Proposal for a regulation of the european parliament and of the council on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID-19 pandemic (Digital Green Certificate) (hereinafter referred to as „***proposal for regulation***“) the trust framework designed by the green covid pass scheme is described as follows: "*trust framework" means the rules, policies, specifications, protocols, data formats and digital infrastructure regulating and allowing for the reliable and secure issuance and verification of certificates to guarantee the certificates' trustworthiness by confirming their authenticity, validity and integrity, including by the possible use of electronic seals.*[4]

According to article 8 proposal for regulation the trust framework is defined as follows: „*To ensure uniform conditions for implementation of the trust framework established by this Regulation, the Commission shall adopt implementing acts containing the technical specifications and rules to:*
a)securely issue and verify the certificates referred to Article 3;
b) ensure the security of the personal data, taking into account the nature of the data;
c) populate the certificates referred to Article 3, including the coding system and any other relevant elements;
d) lay down the common structure of the unique certificate identifier;
e) issue a valid, secure and interoperable barcode;
f) ensure interoperability with international standards and/or technological systems;
g) allocate responsibilities amongst controllers and as regards processors.“

The guidelines[5] adopted by the eHealth Network[6] are based on thre pillar:

a) minimmum data set,
b) standard unique ideintifier for such proffs and
c) **trust framework which provides the basic for establishing the certificates autehenticity, integrity and validity**.

The green covid pass is a certificate rliying on a minimum dataset including a unique vaccination certificate, which shall be used as a connection between the data and the issueing authority and the registry.

The verifier of a certificate should be able to recognise that:

[3] Available at: https://ec.europa.eu/health/sites/default/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf (25.04.2021)
[4] Proposal for a regulation of the european parliament and of the council on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID-19 pandemic (Digital Green Certificate).
[5] eHealth Network guidelines on proof of vaccination for medical purposes - basic interoperability elements, adopted and published on 27 January 2021.
[6] the eHealth Network is a voluntary network created under article 14 of Directive 2011/24/EU on the application of patients' rights in cross-border healthcare. It provides a platform for Member States' competent authorities responsible for eHealth.

- The certificate has been issued by an authorised entity;
- The information presented on the certificate is authentic, valid, and has not been altered;
- The certificate can be linked to the holder of the certificate.

The trust framework outlines the basis for discussion with member states on the implementation of interoperable certificates as green covid passes. It defines the rules, policies, protocols, formats and standards needed to ensure that green covid passes (certficates) are issued in such a way that their authenticity and integrity can be verified and trusted. The trust framework shall be flexible enough to encompass different use cases. It defines provisions that allow both digital and analogue, off-line and on-line versions of the covid green passes, as well as the associated verification. The trust framework can be and must be considered as a trust service that is built and provided upon framework. The framework is building the principles to be followed by member states in admitting the EU citizens their freedom of movement.

It is more importantly fundamental in the trust framework scheme that, in fact there will be a communication between entities from different EU member states, but a central service will be provided by the EU having a gateway platform for verifing validity and authencity of the green covid pass. Until the gateaway is implemented trust verification mechanism in communicating member states will be relevantly answering all the electronic requests for identification and authentification.

The design of the trust framework relies on key design principles listed below. The list is not prioritised. Instead, the trust framework that is specified later in the document attempts to optimise as many of the key design principles as possible.

a) *Cross-border interoperability. National implementations of certificates that comply with the specifications of the trust framework should be interoperable. This means that if Countries A and B implement the specifications, it should be possible for a verifier in Country B to verify a digital vaccination certificate that has been issued in Country A.*
b) *Data protection (including data minimisation, purpose limitation, etc.). The trust framework should protect the data of the involved individual stakeholders (most importantly, certificate holders). This covers several data protection dimensions catered by the General Data Protection Regulation, including purpose limitation and data minimisation.* [7]
c) Data security and privacy by design and by default. Abuse of data by actors (especially, the certificate verifiers and holders) and forgery should be prevented by any reasonable means. The trust framework should by design and default ensure the security and the privacy of data in the compliant implementations of digital vaccination certificate systems, ensuring both security and privacy.
d) Inclusiveness (especially medium-neutrality). The trust framework should be inclusive both towards member states' approaches and the individual citizen ('no citizen left behind'). The design of the trust framework should attempt to maximize its support for diverse contexts (e.g., high resource vs low resource contexts).
e) Simplicity and user-friendliness. It is very important that the trust framework is designed with simplicity and user-friendliness of the possible implementation of digital certificate systems in mind.
f) Implementation flexibility. The trust framework specifications should provide implementers with a variety of options when developing green covid pass systems according to the trust framework specifications.
g) Modularity and scalability. This is strongly linked with the previous key design principle. The trust framework architecture should be modular and easily scalable, for instance, to additional usage scenarios, use cases and types of certificates.
h) Open standards. The trust framework should rely for its implementations on open standards, to the extent that this is possible. This will greatly contribute to the interoperability of the resulting

[7] Interoperability of health certificates – trust framework. V.1.0.

implementations, in addition combined with open governance and open source implementations, it will instil trust in the involved stakeholders.

The trust framework must be in compliance with the regulation set up by the GDPR that states strict obligations on controllers (entities determining the purposes and means of processing of personal data, here e.g. organisations issuing and verifying vaccination certificates), such as to have a legal basis for their processing operations, document them, implement appropriate security measures, and to inform data subjects (natural persons data relating to whom are processed).

Trust framework in the case of green covid pass shall be compared in the world of electronic identity, authenticity as a form of temporary trust service having the necessary format and providing a so called „freedom of movement service". The important point, which may bring up questions is whether the necessity of data protection, data processing or interoperability of various health registries of member states is met at the highest possible level.

3. Legal aspects of green covid pass

TFEU in article 21 (2) confers on EU citizens the right to move and reside freely within the territory of the Member States. Article 21(2) provides for the possibility for the EU to act and to adopt provisions with a view to facilitating the right to move and reside freely within the territory of the Member States if action to attain this objective is necessary to facilitate the exercise of this right.

The proposal for regulation aims to ensure that restrictions of free movement currently in place to limit the spread of COVID-19 can be lifted in a coordinated manner as more scientific evidence becomes available. The objectives of the proposal for regulation, namely to facilitate the free movement within the EU by establishing secure and interoperable green covid pass on the holder's vaccination, testing and recovery status. The proposal for regulation aims to create a legal and social area, that cannot be sufficiently achieved by the member states independently but rather at EU level. Action at EU level is thus necessary.

Absence to act at EU level would likely result in member states adopting different systems, resulting in citizens exercising their free movement rights experiencing problems in the acceptance of their documents in other Member States. In particular, it is necessary to agree on the technical standards incorporaetd in the „trust framework" to be used to ensure interoperability, security and verifiability of the certificates being issued. EU action can add considerable value in addressing the challenges identified above and is the only way by which a single, streamlined and accepted framework can be achieved and maintained. The adoption of unilateral or uncoordinated measures regarding green covid pass is likely to lead to restrictions on free movement that are inconsistent and fragmented, resulting in uncertainty for EU citizens when exercising their EU rights. **The proposal limits the processing of personal data to the minimum necessary**, by only including a limited set of personal data on the certificates to be issued, by setting out that the data obtained when verifying the certificates should not be retained, and by establishing a framework that does not require the setting up and maintenance of a central database.

Green covid pass a eldas regulation

According to recital number (21) Regulation of (EU) No. 910/2014 OF THE European Parliament and of the the council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/E (hereinafter referred to as „***eIDAS regulation***"): „*Regulation should also establish a general legal framework for the use of trust services. However, it should not create a general obligation to use them or to install an access point*

for all existing trust services. In particular, it should not cover the provision of services used exclusively within closed systems between a defined set of participants, which have no effect on third parties. For example, systems set up in businesses or public administrations to manage internal procedures making use of trust services should not be subject to the requirements of this Regulation. Only trust services provided to the public having effects on third parties should meet the requirements laid down in the Regulation. Neither should this Regulation cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form laid down by national or Union law. In addition, it should not affect national form requirements pertaining to public registers, in particular commercial and land registers."

The eidas regulation further enacts the basic principles and rules for the functioning of trust services,which must be therefore accepted and recognise by European union (hereinafter referred to as „***EÚ***"). For the purposes of eidas regulation i tis necessary to note that followign definitions. Article (1) of eidas regulation states: „electronic identification' means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person; electronic identification means' means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service;

Article 5 of the eidas regulatuion describes 'authentication' as means of an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed. Most importantly this regulation defines the so called 'trust service', which means an electronic service normally provided for remuneration which consists of:

(a) **the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services**, or
(b) the creation, verification and validation of certificates for website authentication; or
(c) the preservation of electronic signatures, seals or certificates related to those services;

Additionally the article 17 describes 'qualified trust service' means a trust service that meets the applicable requirements laid down in this Regulation. In the context of the pandemic and in the context of the green covid pass, it shall be monitored if the use of a digital tool, that is readable in various different ways meets all the necessary criteria of the eidas regulation. So far the legislators are calculating with the green covid pass something similar as an identificator (e.g. ID card, passport, driving lincese or others). In the authors opininon, this approach if will be realied, in a maximally minimalistic way.

The eIdas regulation and its fundamental definitions as identificaiton, authentification which are mostly the basic of this regulation were implemented in the act no. 305/2013 Coll. On e-government (hereinafter referred to as „***Act on e-government***"). The article 19, 20 and 21 of Act on e-government defines the exact process of identification and authentification in the legal system of Slovak republic. It has to be understood, that this process is much more sophisticated and is bound to a certain degree of services, but considering green covid pass an identifier, which will be evaluated by different means (systems, persons and other) we have to evaluate the adequacy of the proposed legislation. The process of entering other member state of an EU citizen shall be verified be based on a green covid pass. More importantly the green covid pass seem to lead to an authentification process behind, that will enable the citizen to perform certain activities.

Green covid pass and GDPR

The personal data contained in the green covid pass certificates issued in accordance with the proposal for regulation shall be processed for the purpose of accessing and verifying the information included in the certificate in order to facilitate the exercise of the right of free movement within the EU. The personal data included in the certificates shall be processed by the competent authorities of the member state of destination, or by the cross-border passenger transport services operators required by national law to implement certain public health measures to confirm and verify the holder's vaccination, testing or recovery status. For this purpose, the personal data shall be limited to what is strictly necessary. **The personal data accessed pursuant to this paragraph shall not be retained longer than is necessary for its purpose and in no case longer than the period for which the certificates may be used to exercise the right to free movement**.

The Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**General Data Protection Regulation**), strictily defines the basic principles of processing personal data and outlines what are the measures taken into account when specific data are being processed. From the possible data misuse or data breach prospective it tis necessary to verifiy the purpose of processing data from the green covid pass as well as the necessity of processing the data. The security issue shall be conducted in some way by the EU gateaway and the security measures taken by meber states to protect their data centres. Once the above mentioned measures taken by the member states are met, the GDPR principles should be applied.

Conlusion

Discussing the eHealth Network's outline, security and privacy researcher Dr Lukasz Olejnik — who has also written about the privacy risks and wider ramifications of vaccine passports — said the document raises some questions such as who will be the source of trust and whether there's a risk of function creep related to the proposed design."*This technical document confirms that the user's ID will be bound to the certificate. This may mean that the passport would mediate a proof of ID," he told TechCrunch. "Considering today's proposal of a regulation it is pertinent to wonder whether a function-creep-like expansion couldn't lead to these passports becoming actual proofs of identity in the future.*[8]

Considering the structure of the green covid pass scheme, taking into considerations that minimum data safety issues arise, the biggest legal issue is what will be the relevance of the green covid pass in the process of identification and authentification. In my opinion the GDPR issues will be on a zero level once the gateaway of the EU will be created. Other than that GDPR already pushes legislators to a high level of data protection especially in case specific data are processed. In case of data security the green covid pass mechanism provides a double degre safety check. We still have to admit that the risk from an outside attack is a possibility.

The trust framework being a temporary trust service in my opinion without having fulfilled the necessary eIDAS obligations, may bring difficulties in the wrold of electronic identification and authentification. The exercise of the right to freedom of movement has been mentioned as the reason for the proposal for regulation, but since technical framework is being drafted preperly, the eIDAS aspects and relations of the green covid pass have been omitted until this moment.

[8] Available at: https://techcrunch.com/2021/03/17/europes-rush-for-a-covid-19-digital-pass-stirs-concerns (01.05.2021)

Bibliography:

1) CChabra, S., Muneesh K.:Integrating e- business models for government solutions. Hershey- New York. Information science reference. 2009. 296s. ISBN: 9781605662404.
2) Compagnucci, M.C.: Big Data, Databases, Ownership rights in the cloud (perspectives in Law, Business and Innovation). Kyushu. Springer. 2019. 492s.
3) Lloyd Ian J.: Information technology law. Oxford. Oxford University press. 2014. 541 s. ISBN:978-0-19-870230-0.
4) Millard, Ch.: Cloud Computing Law.Oxford. Oxford University Press. 1st edition. 2013. 500s. 978-019967168. 500s.
5) Rowland, D., Kohl U., Charlesworth A.:Information technology law – fourth edition. Oxon. Routledge. 2012. 521s ISBN:978-0-415-48227-1.

Legislation

1) Interoperability of health certificates – trust framework. V.1.0.
2) eHealth Network guidelines on proof of vaccination for medical purposes.
3) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID-19 pandemic (Digital Green Certificate).

Contact:
Mgr. Kristian Hodossy
Hodossy1@uniba.sk
Univerzita Komenského,
Právnická fakulta Šafárikovo námestie 6, P.O.BOX 313
811 00
Bratislava Slovenská republika

COPYRIGHT REGULATIONS IN THE FIELDS OF IMAGING AND TECHNOLOGY IN TIMES OF CRISIS

Ewa Lewandowska, PhD

University of Warmia and Mazury in Olsztyn

Abstract: Identifying the problem discussed in this paper, it shall be noticed that new technologies and their common application introduced by the covid pandemic create great opportunities for image fixing and then its dissemination. Another phenomenon is situations where permission for the fixing and dissemination of an image is a condition for obtaining a service or gaining admission to a conference or seminar. In view of such behavior, the envisaged legal protection often has a reatroactive and insufficient application. This work discusses the issues of image protection from the point of view of copyright regulation. The binding provisions have been assessed, and it was considered whether it currently stands at the height of imagine protection. The literature on the subject was reviewed in terms of the definition of an image in the context of new technologies. Next, attention was paid to the category of "a commonly known person" and the interpretation of the phrase "detail of a whole". In conclusion, the interpretation of binding provisions (or the direction of desirable amendments) shall be more demanding in details, for example according to the requirement to precisely specify the scope of the permission granted for disseminating the image.
Keywords: copyright, image, dissemination

1. INTRODUCTION

Many years ago, images were not widely discussed in the legal forum, in part because there were no appropriate tools to record it and, as a result, there were no violations[1]. The first regulations appeared in connection with the development of photography, whereas photography was initially protected as a creative[2]. But regulations have evolved to take on their current well-established shape. For example, the Polish Copyright Act[3] includes image protection in art. 81[4]. Hereby, people (societies), we can even say with confidence — the world — has reached the year 2021, when most business meetings, national and international conferences, as well as other meetings of various types are held online using available applications. In recent years the world has witnessed scientific and technological developments, which translates, inter alia, on such image-recording tools as digital cameras. Recently it is promoted sharing and broad licenses, for example its very popular social media platforms, and what is worth mentioning most is that society follows this trend. In all this, it is forgotten that consolidating an image causes it to lose its fleeting character and becomes permanent. This problem is worsened because most users fail to read or understand the platforms' terms of service or the rules/conditions for participating in an online meeting. Another danger comes when permission to disseminate an image as a condition *sine qua non* to participate in an event is not allowed (a take-it-or-leave-it construction)[5].

[1] GIESEN, B., O naturze prawa do wizerunku – uwagi na tle rozważań historycznych oraz prawnoporównawczych, in: Qui Bene Dubitat, Bene Sciet. Księga jubileuszowa dedykowana Profesor Ewie Nowińskiej, Warsaw: Wolters Kluwer, 2018, p. 135, SHNIKAT, M.M., The Civil Legal Protection of One's Image Right: A Comparative Study between Jordan, France, and Egypt, In: Journal of Law, Policy and Globalization 2019, 82, p. 132.

[2] Wider: BARBAS, S., The Laws of Image, In: New England Law Review 2012, 47, no. 1, p. 23-92.

[3] Act of 4 February 1994 on Copyright and Related Rights, (consolided text, Journal of Law of 2019, item 1231, as amended), hereinafter: the Copyright Act.

[4] Compare: OLTEANU, E.G., The Copyright and Its Relationship with the Image Right, In: Revista de Stiinte Juridice 2016, no. 2, p. 34.

[5] See: PATTON, M., How to Protect Users' Copyright Rights in the Age of Social Media Platforms and Their Unread Terms of Service, In: University of San Francisco Law Review 2019, 53, no. 3, p. 463-488.

Due to the restrictions introduced by the Covid pandemic, we are witnesses of a new stage. We can observe that in the conditions of a Covid pandemic and in the aftermath of online meetings, recording the meeting seems natural and accessible, and brings only benefits. But is this really so? It is worth considering the risks. In the literature on the subject, many authors point out significant concern from the copyright point of view, which relies on technology, digitalization and the internet, and their ease, speed, and low cost combined with the permanence of posts and effortlessness of online distribution that allow for access, storage, manipulation, reproduction, and distribution of any content[6].

The main reason to write this paper was the statute (document with general conditions) of one scientific conference[7]. In this document the conference organizers stipulated that "by participating in the conference, the participant permits to the use and dissemination of the image for advertising, promotional and marketing purposes. The consent is not limited in time or territory and covers all forms of publication, in particular advertising posters, leaflets, printed promotional materials, TV spots, advertising in newspapers and magazines and on the Internet, etc. The participant hereby waives all (existing and future) claims, including for remuneration, for the use of his image"[8]. The most unfair in this stipulation is the very broad scope of the permission in addition to the potential participant having no choice and no negotiating power. She/He is namely either to agree to the proposed/imposed terms or not to take part in the conference. Such a casuistic example is not an exception[9]. This justifies in-depth considerations, which in this study will cover the issue of image in relation to copyright.

In this paper, in order to identify the problem it is necessary to start with the presentation of definition and characteristics of an image. Next, the assessment of the biding regulation about image will be made. It seems to be very important to consider whether it stands at the height of image protection in current realities. Finally, the direction of changes, postulates, and conclusions will be presented.

2. IMAGE DEFINITION

2.1. IMAGE IN THE MULTITUDE OF LEGAL ACTS

Image is the object of analysis in different areas of law, as it is regulated in many legal acts, starting with the Constitution[10] (under the right to privacy), in the Civil Code[11], Press Law[12], the Copyright and Neighbouring Rights Law[13], Sport Law[14], and the Law of Penal Proceedings[15]. Moreover, acts of international rank include image (as a part of the right to respect private life), for example it is protected under the European Convention on Human Rights and Fundamental Freedoms of 4.11.1950[16], Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April

[6] McMAHON, K., The Current State of Digitized Images Necessitates Congressional Action to Protect Authors and Content Providers from Online Infringement, In: Suffolk University Law Review 2016, 49, no. 4, p. 487.

[7] By the way, it is worth noting that the organizer of the conference - admittedly a scientific one - was a private entity, to which the scientific unit most likely commissioned this organization.

[8] Due to the critical assessment of the cited stipulation, the Author, as a representative of science and a participant in scientific conferences, decides not to reveal the source.

[9] For example, see: PATTON, M., op.cit., p. 473.

[10] Art. 47 of the Constitution of the Republic of Poland of April 2, 1997, (Journal of Laws of 1997 No. 78 item 483 with the subsequent amendments), hereinafter: Constitution.

[11] Art. 23 of the Act of April 23, 1964 The Civil Code (consolidated text, Journal of Laws of 2020, item. 1740), further: the Civil Code.

[12] Art. 13 of the Act of January 26, 1984 The Press Law (consolidated text, Journal of Laws of 2018, item 1914).

[13] Art. 81 of the Act of February 4, 1994 Law on Copyright and Neighbouring Rights (consolided text, Journal of Laws of 2019, item 1231), further Copyright Act.

[14] Art. 14 of the Act of June 25, 2010 the Sport Law (consolidated text, Journal of Laws of 2020, item 1133), see as well: BLACKSHAW, I., Protecting Sports Image Rights in Europe, In: Business Law International 2005, 6, no. 2, p. 270-285.

[15] Art. 173 of the Act of June 6, 1997 Code of Penal Proceedings (consolidated text, Journal of Laws of 2021, item 534).

[16] Art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms drawn in Rome on November 4, 1950 later amended by Protocol No. 3, 5 and 8 and supplemented by Protocol

2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)[17]. The above confirms that the image is not something new. On the contrary, it is a commonly known and understood element. However, image issues are not uniform or harmonised throughout Europe[18].

Due to the multi-faceted nature of image regulation, it is not legally defined. This has its pros and cons, as it enables the adjudicating bodies to use specific leeway in making their decisions, and consequently to allow for the actual social conditions when evaluating factual circumstances, but as well it causes the threat or inconvenience of various legal qualifications of image itself and the corresponding rights[19]. Therefore, in the literature on the subject, much space is devoted to considerations aimed at determining the scope of the concept of image.

Article 81 of the Copyright Act, which is the subject of this paper, specifies regulations of the Civil Code, showing how to use and protect image[20]. Therefore, the considerations cannot take place without signaling the issue of image as a personal right[21]. The concept of personal rights is treated very differently in literature and jurisprudence and there is no single, commonly accepted definition of these goods. Without going into the theoretical and legal analysis of the concept of personal rights, it can be assumed that it is the value recognized by legal systems in almost every country. It is said that the legislator protects the world of psychological experiences and human feelings because of certain values[22]. It can be concluded that these values were shaped (and are still being shaped) in the course of the development of social life[23]. The catalog of personal rights includes the image (cf. Art. 23 of the Act of April 23, 1964 The Civil Code[24]). In this sense, the personal right is the psychological comfort of a specific person related to the concretization of his physical image consisting in the preparation or dissemination of the image[25]. The dominant opinion is that image is connected with the right to private life[26].

2.2. MEANING OF IMAGE IN COPYRIGHT

The Copyright Act is one of the legal Acts that striclty refer to image and its protection. In the literature on the subject it is mentioned that copyright regulation is very important due to the social

No. 2, (Journal of Laws 1993 No. 61 item 284); available at https://www.echr.coe.int/documents/convention_eng.pdf on 5 of April 2021.

[17] Art. 4, number 14) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (Official Journal of the European Union 2016, L 119/1), available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=PL on 5 of April 2021

[18] SYNODINOU, T., Image Right and Copyright Law in Europe: Divergence and Convergences, In: Laws 2014, 3, no. 2, p. 183 and following.

[19] BIENIEK, E., KAWAŁEK, P., Right to publicity in the age of globalisation; In: Human rights, Spiritual values and global economy, B. SITEK, J.J. SZCZERBOWSKI, A.W. BAUKNECHT, G. DAMMACCO (eds.), South Jordan: ecko House Publishing, 2011, ISBN (13): 978-1-4276-5324-6, p. 181.

[20] ZAREMBA, M., Prawo prasowe – ujęcie praktyczne, Warsaw: Difin, 2007, p. 252, see also: OLTEANU, E.G., op.cit., p. 34-37.

[21] Image is a personal right, which is confirmed by the literature on the subject, for example: SHNIKAT, M.M., p. 132-158.

[22] ŚLĘZAK, P., Commentary to art. 81 Copyright Act, In: Ustawa o prawie autorskim i prawach pokrewnych. Komentarz, 2017, Warsaw: C.H. Beck, p. 563.

[23] SOKOŁOWSKI, T., Commentary to art. 23 of PCC, In: Kodeks cywilny. Komentarz. Tom I. Część ogólna, A., KIDYBA (ed.), 2012, Warsaw: Wolters Kluwer Polska, LEX Legal Information System.

[24] Act of April 23, 1964 The Civil Code (consolidated text, Journal of Laws of 2020, item 1740, as amended), hereinafter: PCC.

[25] ŚLĘZAK, P., op.cit. p. 563.

[26] BALAN, E., The Right to One's Own Image, In: Romanian Journal of Intellectual Property Law 2006, no. 3, p. 50-56.

media and the development of other internet platforms[27]. The current, widely commented issue is, *inter alia*, the right of publicity (recognized mainly in the United States)[28]. The image can be used for promotion and advertising, and therefore it is also valuable in terms of commercial use.

The definitions of image presented in literature are similar in their understanding. In general, image is defined as a visual representation of something or someone[29]. As a rule, the definition refers to the physical characteristics of a person that allow for his or her identification, such as personal appearance[30]. It is even possible to talked about physical image (appearance) that shows "perceptible features of a man, creating his or her appearance and enabling to identify a person among other people"[31]. For example, the Supreme Court pointed out that the elements of an image are, among others, facial features or silhouettes that enable individualization and identification of a person, creating his or her sense of identity and uniqueness[32].

In fact, however, the concept of imagine is much broader. According to J. Barta and R. Markiewicz, as an image, not only natural human features should be included, but also other added features, such as makeup, clothing or props (e.g., glasses). After all, these may be important gadgets in identifying the person for whom they are characteristic[33]. For example, elements of an image such as movement, gestures, dress, or nicknames can also help recognize a given person[34]. An important defining element of the image is also the ability to fixate by technical means (e.g., photography) and its dissemination[35]. In this place it should be emphasized that the carrier (material substrate) on which an image is recorded, for example a painted portrait, a photograph, a drawing, or a caricature, is a physical media of the immaterial (intangible) right (namely image).

3. INTERPRETATION OF BINDING REGULATION

Art. 81 of the Copyright Act states: 1. The dissemination of an image shall require the permission of the person presented in it. Unless there is a clear reservation, such permission shall not be required if such a person has received the agreed price for posing. 2. The permission shall not be required for dissemination of the image: 1) of a commonly known person, if such an image has been made in connection with his/her performance of public functions and, in particular, political, social or professional functions; 2) of a person constituting only a detail of a whole, such as a meeting, a landscape, or a public event[36]. In the further part of this paper, reference was made to the interpretation of the above-mentioned provision, paying particular attention to the current situation resulting from the covid pandemic and, consequently, the prevalence of online meetings and the

[27] WAGNER, M., Set Your Settings on Private: Copyright in Era of Social Media Usage, In: Cybaris: An Intellectual Property Law Review 2018, 9, no. 1, p. 57-79.
[28] Wider: KING, Y.M., The Right-of-Publicity Challenges for Tattoo Copyrights, Nevada Law Journal, 2016, 16, no. 2, p. 450 and following, SYNODINOU, T., op.cit., p. 193 and following.
[29] SHNIKAT, M.M., op.cit., p. 134.
[30] WOJNICKA, E., Prawo do wizerunku w ustawodawstwie polskim, In: ZNUJ 1990, 56, p. 107, about image of legal person see: ŚLĘZAK, P., op.cit., 562, SOKOŁOWSKI, T., op.cit., LEX Legal Information System, Judgment of Court of Appeal in Warsaw, from November 7, 2012, I ACa 612/12 Legalis, CIRCA, A., Reflections on the Right to Image, In: Romanian Journal of Intellectual Property Law 2012, no. 1, p. 137-151.
[31] WOJNICKA, E., op.cit., p.. 101 and the following.
[32] Judgment of the Supreme Court ruled on March 7, 2003, File no. I CKN 100/01, LEX Legal Information System no. 83833.
[33] BARTA J., MARKIEWICZ, R., Wokół prawa do wizerunku, In: ZNUJ. Zagadnienia prawa własności intelektualnej. Profesorowi Stefanowi grzybowskiemu pracownicy Instytutu Wynalazczości i Ochrony Własności intelektualnej w darze, 2002, 2 p. 12, and cited here judgment of the Court of Appeal in Cracow from February 7, 1995 r., I ACr 697/94, LEX Legal Information System no 62626, this shares: KALUS, S., Commentary to art. 23 of PCC, In: Kodeks cywilny. Komentarz. Tom I. Część ogólna (art. 1-125), M. FRAS, M. HABDAS (eds.), Warsaw: Wolters Kluwer Polska, 2018, LEX Legal Information System.
[34] KALUS, S., op.cit., Lex Legal Information System.
[35] BARTA J., MARKIEWICZ, R., op.cit., p. 11 and following, ŚLĘZAK, P., op.cit., p. 555.
[36] Compare: PEPTAN, R., The Right to Own Image, In: Annals of the Constantin Brancusi University of Targu Jiu Juridical Sciences Series 2016, no. 4, p. 51-58.

possibility of preserving and disseminating the image. The analysis of the provision will concern a specific case (it will therefore be casuistic), i.e., the provision from the statute referred to in the introduction part in the regulations presented by the organizer of the scientific conference.

Art. 81 of the Copyright Act is an instrument for controlling the use of your image by other people[37]. When analyzing the content of this provision, one should first refer to the permission that may be granted by a person to disseminate his or her image. The legislator determines the possibility of using and disseminating the image of a person from this permission. It is therefore the most important element in assessing the legality of disseminating an image. There is a need to resolve the legal nature of permission and its form and scope of granting (how to define the boundaries of the permission?). Secondly, however, it should be considered whether, in connection with the analyzed problem, there are any circumstances allowing for the dissemination of a person's image without their permission, as given in art. 81 of the Copyright Act.

3.1. PERMISSION TO DISSEMINATE AN IMAGE

3.1.1. LEGAL CHARACTER OF PERMISSION

The purpose and the essence of permission is to grant its addressee the right (authorization) to the procedure specified in the permission[38], in this case dissemination of an image. Permission as a carrier of a right must be treated as a civil law event, and since it is always a manifestation of the will of the person granting it, it is conceptually the closest to a declaration of intent. Theoretically, permission may be a declaration of intent, a unilateral legal act or simply a legal action similar to a declaration of intent[39]. Because the legal consequences of granting permission are far-reaching, in order to meet the condition of permission to disseminate an image it is not enough to know that the image will be disseminated. It is necessary to actively accept the terms and legal consequences of granting it. The problem arises when the permission to disseminate an image is only one of many provisions of the statute, which the person accepts with a so-called "one click". It seems that statistically few people are familiar with these statute contents. As a result, few people realize what they agreed to (they may be shocked to discover the risks that they are agreeing to take).

Since permission to disseminate an image is similar in legal nature to a declaration of intent, it should be a separate/individual element and not part of another document. The internet carries numerous risks, including the case study in this paper. It should be postulated that only such an interpretation of consent, i.e., as an individual declaration, would sufficiently protect the entity granting it.

3.1.2. PERMISSION FORM

In the wording of Art. 81 Copyright of Act, the legislator does not indicate the form of permission. It should be concluded that granting permission to disseminate an image does not require any special form. However, taking into account the legal consequences that result from the fact of granting the permission in question, it should at least be in written form. However, such a conclusion results from the practice of applying the provision, and not from its content.

3.2.3. THE PERMISSION SCOPE

The legislator does not determine the scope (content) of the permission granted pursuant to Art. 81 of Copyright Act. It can even be said that, apart from the possibility of granting it, it does not refer in any way broadly to the permission in question.

In the literature on the subject, in connection with the content of Art. 81 of Copyright Act indicates that the rightholder, when giving permission, should indicate the scope of actions that may be taken by the person obtaining the permission[40]. When granting permission, the entitled person (the

[37] ŚLĘZAK, P., op.cit., p. 566.

[38] BANASZCZYK, Z., Stosunek cywilnoprawny, In: System Prawa Prywatnego, t. 1, Prawo cywilne - część ogólna, M. SAFJAN (ed.), Warsaw: C.H. Beck, 2007, p. 887.

[39] Wider: GRZESZAK, T., Prawo do wizerunku i prawo adresata korespondencji, In: System Prawa Prywatnego, Prawo autorskie, T. 13, J. BARTA (ed.), Warsaw: C.H. Beck, 2013, p. 690 – 696.

[40] ŚLĘZAK, P., op.cit., p. 568, FERENC-SZYDEŁKO, E., Commentary to art. 81 of Copyright Act, In: Ustawa o prawie autorskim i prawach pokrewnych. Komentarz, Waraw: C. H. Beck, 2011, p. 561-562.

one who grants permission) should be fully aware of the circumstances of disseminating the image[41]. The content of the permission cannot be general[42]. The point is that the person granting permission should be aware of such circumstances as: the manner of presenting his image, place of publication, time of publication, comparison with a specific text, and advertising use of the image[43]. It should be assumed that the granted permission, to the extent that the person granting it was not aware of what he/she actually permitted (disseminating the image in any way or in any context), should be considered invalid, e.g., on the basis of a general regulation of the lack of awareness (see Art. 82 of the PCC).

The cited theses are important from the point of view of the problem presented at the beginning of this paper. The image of natural persons should be determined for a specific purpose. Therefore, the question arises, to what extent should the scope of the permission be defined? Can such permission have an undefined scope of the circumstances of disseminating the image of a person (closer to the so-called blank consent)?

Although the doctrinal postulates should be considered correct, the fact is that the legislator confines itself to stating that disseminating an image requires the permission of the person presented in it. At this point, deep reflection is required in connection between technological advances and dissemination of image. The aim should be to break the middle ground between the advocates for online-free access and the copyright holders, in particular image protection. These times, the way people do their job, makes one forget about respecting values such as privacy, which includes images. As a *de lege ferenda* postulate, it should be indicated that it is desirable to expand and specify the scope of permission (as to its content). A certain reference may be the shape of the regulation of Art. 41 section 2 of the Copyright Act, in which the legislator imposes an obligation on the parties to the contract for the transfer of copyright to explicitly mention the fields of exploitation in the contract. However, this is not an ideal solution, as shown by the practice of use[44].

3.1.3. PERMISSION AS A PREREQUISITE FOR PARTICIPATION IN AN EVENT

By sharing the image on platforms such as Facebook, Twitter, and Instagram, we agree to its further dissemination, which results from the platforms' policies. If the use of these platforms is an addition or a whim, or is fulfilling a desire to be "noticed" on socia media[45], then permission to disseminate the image does not raise any major doubts. By assumption, these types of platforms are geared towards broadly sharing content in order to attract a larger following and reach a greater audience[46]. However, reservations are raised when the condition for participation in an event such as a scientific conference or business meeting includes permission to disseminate images. At the same time, it is necessary to distinguish from a situation where a meeting participant has the opportunity to participate in said meeting, simultaneously turning off his camera, which means that he does not share his image.

The condition of participation in the event from the absolute permission to use the image without any restrictions seems to go beyond the broadly understood principles of social coexistence. Providing the image and permitting its dissemination should be voluntary and not a condition for participation in the event. The admissibility of such solutions is a manifestation of discrimination and inequality. Moreover, it violates constitutionally guaranteed freedoms and rights (cf. Art. 31, 32 of the the Constitution). In such situations, it is desirable that the event organizer leaves the choice of participants to permission.

[41] ŚLĘZAK, P., op.cit., p. 569.
[42] Compare: FERENC-SZYDEŁKO, E., op.cit., p. 561-562.
[43] ŚLĘZAK, P., p. 569.
[44] The parties to the contract for the transfer of economic copyrights in the content of the contract indicate, *inter alia*, on the basis of Art. 50 Copyright Act, containing an open catalog of fields of exploitation.
[45] WAGNER, M., Set Your Settings on Private: Copyright in Era of Social Media Usage, In: Cybaris: An Intellectual Property Law Review 2018, 9, no. 1, p. 75.
[46] WAGNER., M., op.cit., p. 75.

3.2. LEGALLY DISSEMINATING A PERSON'S IMAGE WITHOUT HIS/HER PERMISSION

Based on the content of art. 81 of the Copyright Act, the legislator provides for exceptions to the principle of obtaining permission to disseminate an image. These include situations where the person: 1) received the agreed payment for posing, 2) is a commonly known person, if such an image has been made in connection with his/her performance of public functions and, in particular, political, social or professional function, or 3) is only a detail of a whole, such as a happening (meeting), landscape, or public event.

3.2.1. PAYMENT FOR POSING

In fact, this circumstance in connection with the case indicated in the introduction of this paper can be omitted. Currently, the rule is that a representative of science participating (active) in a conference, seminar, workshop, or other scientific meeting (including online) does not receive any remuneration for his/her consent.

3.2.2. COMMONLY KNOWN PERSON

The second circumstance, which is an exception to the rule of obtaining permission to disseminate an image, concerns a commonly known person. The statutory concept of a "commonly known person" in practice raises a number of controversies due to the lack of a normative definition. The interpretation of this concept is important, because the limits of the privacy sphere of an average person are different from the limits of the privacy of an actor, politician, or writer, and, finally, people of public interest, who through their actions have become historical figures treated on an equal footing with public figures[47]. Intuitively, a commonly known person should be considered as a popular person, recognized in a given environment, e.g., an athlete, actor, journalist, or influencer (as of the present times). One can also come across the thesis that determining whether the internet may serve this circumstance, e.g., with a presence on Wikipedia, the number of pages with the name or image of a given person found on the web[48]. However, bearing in mind that when discussing the image, we mean a sensitive element, therefore the statistics themselves should not be decisive[49].

It should be noted that as a criterion for the legality of disseminating the image of a commonly known person, the legislator reserved the condition of performing this image "in connection" with the performance of public functions by that person, in particular political and social and professional ones. The representatives of the doctrine indicate that in this sense it may also involve activities related to literary, artistic, musical, acting, and scientific works[50]. A classic example of using the image of a person commonly known in connection with her public function is the image of the president during a meeting with the head of a foreign country or the image of a member of a popular music group during a concert. These are not in doubt. On the other hand, the participation of a scientist in a scientific conference seems to require deeper reflection. It seems that if the dissemination of an image is related to an event (in a narrow scope, e.g., a report from that event), it can be approved that the image of a person has been disseminated due to the person's behavior in the public sphere he/she is connected with. Therefore, the circumstances of dissemination are not without significance. Limiting the right to the image (i.e., the possibility of its dissemination without the permission of the person shown on it) of commonly known persons applies only to the dissemination of the image in connection with the function performed, and not for commercial purposes, for example[51].

3.2.3. A PERSON CONSTITUING ONLY A DETAIL OF A WHOLE

The third circumstance established by the legislator as an exception to the rule of granting permission to disseminate an image is a situation where a person is only a detail of the whole. It

1.1 [47] Judgment of the Court of Appeal in Lodz from February 18, 1998, I ACa 38/98, LEX nr 62559.

[48] FERENC-SZYDEŁKO, E., op.cit., p. 565.

[49] GRZESZAK, T., op.cit., p. 698.

[50] FERENC-SZYDEŁKO, E., op.cit., p. 565.

[51] GRZESZAK, T., op.cit., p. 707.

should be pointed out that in this case, the decision should boil down to establishing the relationship between the image of the person seeking protection and other elements of its content[52].

A special case in this context is recording an online meeting. In such circumstances, is the image only a fragment of a specific whole? In terms of online meetings, we are basically dealing with the framing of individuals. Therefore, it can be concluded that an element of, for example, a photo is no longer a general view, and individualized people become, which means that the exclusion of image protection does not work. A portrait of a specific person captured during a public event does not fall within the scope of Art. 81 section 2 of Copyright Act. It should be emphasized that disseminating the image does not require a permit if the image is only an incidental or accessory element of the presented whole where if the image is removed, the subject and nature of the representation would not change, e.g., class photography[53].

4. CONCLUSIONS

Due to the increased activity of society (especially representatives of science) in online events (meetings), there is the risk that binding provisions do not provide an effective legal framework for protecting an image. Emphasizing that the law is reactive, it is worth making changes to the regulations now. This justifies the discussion on the applicable copyright law in the field of image protection.

In summary, it should be pointed out that copyright regulations that provide for the permission of a person to disseminate his image in the present form carry a high risk of unknowingly permitting the dissemination of the image, so in the current implementation they are incapable of providing an effective legal framework for protection. It is desirable that the permission to disseminate an image shall be a separate document, not part of a larger one, containing the general provisions. Moreover, due to the availability of various means that can be used for infringing this right (the wide scope of methods to disseminate an image), it is also necessary to precisely indicate the scope of permission to disseminate the image. Finally, permitting the recording and dissemination of the image (especially in an unlimited scope) cannot be a condition for participation in an event.

In conclusion, one should also refer to situations in which the legislator allows the dissemination of the image of a person without his permission. It seems that the scope of the term for a commonly known person will require redefinition by taking into account, for example, the working environment. Also required is a new perception of “a detail of a whole” (in terms of new and commonly used applications).

It should be emphasized that copyright has always caused difficulties in interpretation, in the sense that some support narrow copyright protection, and others a broader view. “Our society expects everything online for free, and to some extent, unrestricted content is vital to flourishing cultural commons; however, a balance is necessary”[54]. The legislator’s task is to find a solution to the measure so as to sufficiently protect certain entities while allowing others to operate effectively. Let this paper to be a voice in the discussion toward possible changes to the applicable regulations.

LEGAL ACTS:

Act of 4 February 1994 on Copyright and Related Rights, (consolided text, Journal of Law of 2019, item 1231, as amended), hereinafter: the Copyright Act.
Act of April 23, 1964 The Civil Code (consolidated text, Journal of Laws of 2020, item. 1740), further: the Civil Code.
Act of January 26, 1984 The Press Law (consolidated text, Journal of Laws of 2018, item 1914).
Act of June 25, 2010 the Sport Law (consolidated text, Journal of Laws of 2020, item 1133)
Act of June 6, 1997 Code of Penal Proceedings (consolidated text, Journal of Laws of 2021, item 534).
Art. 47 of the Constitution of the Republic of Poland of April 2, 1997, (Journal of Laws of 1997 No. 78 item 483 with the subsequent amendments).
Convention for the Protection of Human Rights and Fundamental Freedoms drawn in Rome on November 4, 1950 later amended by Protocol No. 3, 5 and 8 and supplemented by Protocol No. 2,

[52] ŚLĘZAK, P., op.cit., p. 574.
[53] Ibidem.
[54] McMAHON, K., op.cit., p. 493.

(Journal of Laws 1993 No. 61 item 284); available at https://www.echr.coe.int/documents/convention_eng.pdf on 5 of April 2021.
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (Official Journal of the European Union 2016, L 119/1), available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=PL on 5 of April 2021.

JUDGMENTS:

Judgment of the Court of Appeal in Cracow from February 7, 1995 r., I ACr 697/94, LEX Legal Information System no 62626.
Judgment of the Court of Appeal in Lodz from February 18, 1998, I ACa 38/98, LEX Legal Information System no 62559.
Judgment of the Supreme Court ruled on March 7, 2003, I CKN 100/01, LEX Legal Information System no. 83833.
Judgment of Court of Appeal in Warsaw from November 7, 2012, I ACa 612/12 Legalis.

BIBLIOGRAPHY:

BALAN, E., The Right to One's Own Image, In: Romanian Journal of Intellectual Property Law 2006, no. 3, p. 50-56.
BANASZCZYK, Z., Stosunek cywilnoprawny, In: System Prawa Prywatnego, t. 1, Prawo cywilne - część ogólna, M. SAFJAN (ed.), Warsaw: C.H. Beck, 2007, 1283 pages, ISBN: 978-83-7483-342-4.
BARBAS, S., The Laws of Image, In: New England Law Review 2012, 47, no. 1, p. 23-92.
BARTA J., MARKIEWICZ, R., Wokół prawa do wizerunku, In: ZNUJ. Zagadnienia prawa własności intelektualnej. Profesorowi Stefanowi grzybowskiemu pracownicy Instytutu Wynalazczości i Ochrony Własności intelektualnej w darze, 2002, 2 p. 11-32.
BIENIEK, E., KAWAŁEK, P., Right to publicity in the age of globalisation; In: Human rights, Spiritual values and global economy, B. SITEK, J.J. SZCZERBOWSKI, A.W. BAUKNECHT, G. DAMMACCO (eds.), South Jordan: ecko House Publishing, 2011, 599 pages, ISBN (13): 978-1-4276-5324-6.
BLACKSHAW, I., Protecting Sports Image Rights in Europe, In: Business Law International 2005, 6, no. 2, p. 270-285.
CIRCA, A., Reflections on the Right to Image, In: Romanian Journal of Intellectual Property Law 2012, no. 1, p. 137-151.
FERENC-SZYDEŁKO, E., Commentary to art. 81 of Copyright Act, In: Ustawa o prawie autorskim i prawach pokrewnych. Komentarz, Waraw: C. H. Beck, 2011, 803 pages, ISBN:987-83-255-2319-0.
GIESEN, B., O naturze prawa do wizerunku – uwagi na tle rozważań historycznych oraz prawnoporównawczych, in: Qui Bene Dubitat, Bene Sciet. Księga jubileuszowa dedykowana Profesor Ewie Nowińskiej, Warsaw: Wolters Kluwer, 2018, 984 pages, ISBN: 978-83-8124-412-1.
GRZESZAK, T., Prawo do wizerunku i prawo adresata korespondencji, In: System Prawa Prywatnego, Prawo autorskie, T. 13, J. BARTA (ed.), Warsaw: C.H. Beck, 2013, 1137 pages, ISBN: 978-83-255-5068-4.
KALUS, S., Commentary to art. 23 of PCC, In: Kodeks cywilny. Komentarz. Tom I. Część ogólna (art. 1-125), M. FRAS, M. HABDAS (eds.), Warsaw: Wolters Kluwer Polska, 2018, LEX Legal Information System.
KING, Y.M., The Right-of-Publicity Challenges for Tattoo Copyrights, In: Nevada Law Journal, 2016, 16, no. 2, p. 441-466.
McMAHON, K., The Current State of Digitized Images Necessitates Congressional Action to Protect Authors and Content Providers from Online Infringement, In: Suffolk University Law Review 2016, 49, no. 4, p. 469-494.
OLTEANU, E.G., The Copyright and Its Relationship with the Image Right, In: Revista de Stiinte Juridice 2016, no. 2, p. 34-37.
PATTON, M., How to Protect Users' Copyright Rights in the Age of Social Media Platforms and Their Unread Terms of Service, In: University of San Francisco Law Review 2019, 53, no. 3, p. 463-488.
PEPTAN, R., The Right to Own Image, In: Annals of the Constantin Brancusi University of Targu Jiu Juridical Sciences Series 2016, no. 4, p. 51-58.

SHNIKAT, M.M., The Civil Legal Protection of One's Image Right: A Comparative Study between Jordan, France, and Egypt, In: Journal of Law, Policy and Globalization 2019, 82, p. 132-158.
SOKOŁOWSKI, T., Commentary to art. 23 of PCC, In: Kodeks cywilny. Komentarz. Tom I. Część ogólna, A., KIDYBA (ed.), 2012, Warsaw: Wolters Kluwer Polska, LEX Legal Information System.
SYNODINOU, T., Image Right and Copyright Law in Europe: Divergence and Convergences, In: Laws 2014, 3, no. 2, p. 181–207.
ŚLĘZAK, P., Commentary to art. 81 Copyright Act, In: Ustawa o prawie autorskim i prawach pokrewnych. Komentarz, 2017, Warsaw: C.H. Beck, 919, pages, ISBN: 978-83-255-8839-7.
WAGNER, M., Set Your Settings on Private: Copyright in Era of Social Media Usage, In: Cybaris: An Intellectual Property Law Review 2018, 9, no. 1, p. 57-79.
WOJNICKA, E., Prawo do wizerunku w ustawodawstwie polskim, In: ZNUJ 1990, 56, p. 101-124.
ZAREMBA, M., Prawo prasowe – ujęcie praktyczne, Warsaw: Difin, 2007, 392 pages, ISBN: 9788372518170.

Contact information:
Ewa Lewandowska, PhD
e.lewandowska@uwm.edu.pl
Department of Civil Law and Private International Law
Faculty of Law and Administration
University of Warmia and Mazury in Olsztyn
Oczapowskiego 2
10-719 Olsztyn
Poland

THE DOCTRINE OF „FAIR USE" AS ANALYSED BY THE SUPREME COURT OF THE UNITED STATES

Viera Petrášová

Comenius University in Bratislava, Faculty of Law

Abstract: The paper aims the analysis of the most recent decision of the Supreme Court of the United States in case of alleged software copying and its procedural aspects of Google LLC v. ORACLE AMERICA, INC from 5th of April 2021. The proportionality test of a fair use in terms in copying a computer program may have been analysed in terms of a competition restriction but the Supreme Court was convinced of strictly restricted and limited interface usage by Google.

Key words: software protection, copyright, dominant position, restriction of a competition

Doktrína „spravodlivého použitia" analyzovaná Najvyšším súdom Spojených štátov amerických

Abstrakt: Príspevok má za cieľ analyzovať najnovšie rozhodnutie Najvyššieho súdu Spojených štátov amerických v prípade údajného kopírovania počítačového programu a jeho procesných aspektov vo veci Google LLC proti ORACLE AMERICA, INC z 5. apríla 2021. Test proporcionality týkajúci sa spravodlivého použitia z titulu kopírovania počítačového programu mal byť analyzovaný vo vzťahu k obmedzeniu hospodárskej súťaže avšak najvyšší súd bol presvedčený o tom, že spoločnosť Google na vytvorenie platformy použila len nevyhnutné časti počítačového programu.

Kľúčové slová: ochrana počítačového programu, autorské právo, dominantné postavenie, obmedzenie hospodárskej súťaže

INTRODUCTION:

The International Organization for the Protection of Intellectual Property Rights has responded to the hypothesis that any computer program is created by using the intellectual and creative human aspects and as such, it adopted the WIPO Copyright Treaty (WTC) in its territory and stipulated that computer programs are protected as a literary work under Art.2 of the Berne Convention. At the same time, the International Convention stipulated that such protection would apply to computer programs, regardless of the manner or form of their expression. As the result, the only legal way to acquire a computer program is by its license, take-over the undertaking that possess such computer program or to hire software engineers to perform this task on behalf of that undertaking. Any other acquisition of a software program is the subject of the copyright protection and shall be fully compliant with legal restrictions.

The case responds to perceived hypothesis outlined by various academics: 'In recent years, United States courts have grappled with significant issues in copyright law, including copyrightability of useful articles, fair use, contracts and licensing, the meaning of 'substantial similarity', contributory liability, and how works become public domain. New technologies for creating and distributing content and international commerce have been prime influences in shaping United States copyright law.'[1]

The case of Google LLC v. ORACLE AMERICA, INC is about the copyright of so called an Application Programming Interface (API) programmed in JAVA programming language. It implicated two of the

[1] Campbell Dennis. Copyright infringement. Alphen aan den Rijn, The Netherlands: Wolters Kluwer, [2018]. 1 online resource (xv, 266 pages). ISBN 9789403500843 (e-book).

limits in the current US Copyright Act. First, the Act provides that copyright protection cannot extend to "*any idea, procedure, process, system, method of operation, concept, principle, or discovery . . .* ." 17 U. S. C. §102(b). Second, the Act provides that a copyright holder may not prevent another person from making a "*fair use*" of a copyrighted work. Under the Google's petition, the company asked the Court to apply both provisions to the copying at issue. Courts just found as necessary to resolve the case, for argument's sake that the copied lines can be copyrighted and focused on whether Google's use of those lines was a "*fair use*." The case itself started in 2005 and it took almost 15 years to decide on merits. If we would compare the facts analysed by courts we may find out that the legal analysis and assumptions of law itself correspond to the literal analysis of functioning and operation of the Application Programming Interface (API).

Should we compare the so called legitimacy to bring the action on the copyright protection: 'the United States system establishes that only i) the person that holds ownership of a valid copyright; as well as it concerns ii) activity by the defendant that violates any of the copyright owner's exclusive rights respecting the work.'[2] While for instance, the copyright dispute under the Slovak national law includes 'any dispute concerning i) the work under the definition of the copyright, ii) persons entitled under the Copyright Act e.g. author, inherited rights holders, persons entitled under the license, organizations of a collective rights management or an employer should the work satisfy requirements for a copyright protection, iii) the infringement or threatening of a copyright'[3].

A FAIR USE

As we may conclude by analysing the case, the presumption that the programme was indeed copyrighted and the analysis on background and conceptual work has been carried out. Moreover, courts analysed a marketing strategy because one of four reasons for a fair use is the effect on relevant market. The decision thus confirmed the previous decision-making of the US courts that no human creativity skills are required to be proved[4]. As the Supreme Court quotes: Art. 1 § 8 cl. 8 ,,Copyright encourages the production of works that others might cheaply reproduce by granting the author an exclusive right to produce the work for a period of time". The US explanation of a fair use is a mixed question of fact and law. The US Supreme Court refers to the innovation and technology as,, de novo" principle that should better address the disruptive technologies that just turn into the factual existence without a proper legal regulation and standardisation that may be presumed by law. What is different are facts that are to be assumed by the jury while in continental Europe courts in general try to evaluate and examine facts (such as the comparison of work carried by individuals). As the result, fair use shall be examined from four aspects:

---

[2] Feist Publications vs. Rural Telephone Service Co., 499 U.S. 340, at p. 361(1991). The word ''copying" is „shorthand" for the various activities that may infringe a copyright owner's exclusive rights. Range Rd. Music, Inc. vs. E. Coast Foods, Inc., 668 F.3d 1148, at pp. 1153 and 1154 (9th Cir., 2012).

[3] JUDr. Tatiana Mičudová, Copyright disputes in civil proceedings, Bulletin SAK - 7-8/2017

[4] 'The Ninth Circuit's rule overlooks the key distinction between the use of technical experts to analyze substantial similarity as opposed to enabling lay judges and jurors to perceive the underlying works. Just as it would be absurd to ask a lay jury with no familiarity with Kanji characters to assess whether a translation of HARRY POTTER AND THE PHILOSOPHER'S STONE into Japanese infringed the English original without the aid of a bilingual translator, it makes no sense to ask a non-technical jury to compare computer source codes written in different assembly languages to determine substantial similarity without expert assistance. We contend, consistent with the views of every court outside of the Ninth Circuit that has addressed the issue, that courtsshould permit the use of technical experts to enable lay judges and juries to perceive the meaning of computer languages and computer code.' The Use of Technical Experts in Software Copzright Cases> Rectifzing the Ninth Circuit's ,,Nutty: Rule, 2020 Shyamkrishna Balganesh & Peter S. Menell., 35 Berkeley Technology Law Journal 663 (2021), 54 p.

1. the purpose and character of the use,including whether such use is of a commercial nature or is for non-profit educational purposes,
2. the nature of the copyrighted work,
3. the amount and substantiality of the portion used in relation to the copyrighted work as a whole,
4. the effect of the use upon the potential market for or value of the copyrighted work.

As mentioned above, the main characteristics of a fair use shall be analysed individually by separate judicial justification on facts in this case previously judged by a jury[5]. The nature of a fair use reads in the way other software engineers may interact with the copyrighted interface. The case analysed that while the interface is a separate system that may be accessible to other software engineers by simple commands and its nature does not involve instructions to computer to execute a task. The US court also examined the overall functioning of a final software product that is by a large part created by other software engineers that create a separate computer application compatible with Google interface. The question for the purpose and character is then analysed towards a transformation and addition of something new with a further purpose or different character[6]. While the court file shows and it was not a question during the trial, Google copied only what was necessary to enable other software engineers and programmers to perform the creation of other application interfaces. Since Google did not interfere with other the creative freedom of other programmers, the purpose and character were not held to be contrary of a fair use of computer programme copyright protection. The substantiality factor was analysed as the difference and the relationship of the computer programme that was copyrighted towards the entire group of computer programs that works as the interface. As such, since only 0,4% of the entire system has been copyrighted, no substantiality was against a fair use doctrine. The fourth argument in favour of a fair use is that of the effect on trade or in US court wording on market for or value of the copyrighted work. As it was evidenced in the court file 'In 2005, Google acquired Android, Inc., startup firm that hoped to become involved in smartphone software. Google sought, through Android, to develop a software platform for mobile devices like smartphones.'[7]and since no market uptake happen, the court found the doctrine of fair use as not distorted.

The main decision of the Supreme Court is noticeably short, stating five main reasons why they decided that the infringement of the copyright by Google LLC. is not of such nature as to restrict the competition. As dissenting opinions follow, the analysis of main decisive aspects is shown.

[5] Fair use is a legal doctrine that permits the unlicensed use of copyright-protected works in certain circumstances. Section 107 of the Copyright Act provides the statutory framework for determining whether something is a fair use and identifies certain types of limited and „transformative" uses, such as criticism, comment, news reporting, teaching, scholarship, and research, as examples of activities that may qualify as fair use., 17 United States Code, Section 107; United States Copyright Office Fair Use Index, More information on Fair Use, see https://www.copyright.gov./fair-use/more-info.html. The Fair Use Index provides searchable summaries of major fair use decisions.

[6] The inquiry in to the "the purpose and character" of the use turns in large measure on whether the copying at issue was "transformative," i.e., whether it "adds something new, with a further purpose or different character." Campbell, 510 U. S., at 579.

[7] A platform provides the necessary infrastructure for computer programmers to develop new programs and applications. One might think of a software platform as a kind of factory floor where computer programmers (analogous to autoworkers, designers, or manufacturers) might come, use sets of tools found there, and create new applications for use in, say, smartphones. (For visual explanations of "platforms" and other somewhat specialized computer-related terms, you might want to look at the material in Appendix A, infra.)

PROPORTIONALITY PRINCIPLE

Justice Breyer opinion analysed the objective of creating the Application Programming Platform in accordance with its marketing strategy[8]and the current copyright regulation as quoted in four main provisions:

- First, a definitional provision sets forth three basic conditions for obtaining a copyright. There must be a "wor[k] of authorship," that work must be "original," and the work must be "fixed in any tangible medium of expression." 17 U. S. C. §102(a); see also Feist Publications, Inc. v. Rural Telephone Service Co., 499 U. S. 340, 345 (1991) (explaining that copyright requires some original "creative spark" and therefore does not reach the facts that a particular expression describes),
- Second, the statute lists certain kinds of works that copyright can protect. They include "literary," "musical," "dramatic," "motion pictur[e]," "architectural," and certain other works. §102(a). In 1980, Congress expanded the reach of the Copyright Act to include computer programs. And it defined "computer program" as "'a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result.'" §10, 94 Stat. 3028 (codified at 17 U. S. C. §101),
- Third, the statute sets forth limitations on the works that can be copyrighted, including works that the definitional provisions might otherwise include. It says, for example, that copyright protection cannot be extended to "any idea, procedure, process, system, method of operation, concept,principle, or discovery . . . ." §102(b). These limitations, along with the need to "fix" a work in a "tangible medium of expression," have often led courts to say, in shorthand form, that, unlike patents, which protect novel and useful ideas, copyrights protect "expression" but not the "ideas" that lie behind it. See Sheldon v. Metro-Goldwyn Pictures Corp., 81 F. 2d 49, 54 (CA2 1936) (Hand, J.); B. Kaplan, An Unhurried View of Copyright 46–52 (1967),
- Fourth, Congress, together with the courts, has imposed limitations upon the scope of copyright protection even in respect to works that are entitled to a copyright. For example, the Copyright Act limits an author's exclusive rights in performances and displays, §110, or to performances of sound recordings, §114. And directly relevant here, a copy- right holder cannot prevent another person from making a "fair use" of copyrighted material.

As the justice points out:,,Here Google's use of the Sun Java API seeks to create new products. It seeks to expand the use and usefulness of Android-based smartphones. Its new product offers programmers a highly creative and innovative tool for a smartphone environment. To the extent that Google used parts of the Sun Java API to create a new platform that could be readily used by programmers, its use was consistent with that creative "progress" that is the basic constitutional objective of copyright itself. Cf. Feist, 499 U. S., at 349–350 ("The primary objective of copyright is not to re- ward the labor of authors, but '[t]o promote the Progress of Science and useful Arts'" (quoting U. S. Const., Art. I, §8, cl. 8))."

Justice Thomas and Justice Alito have also commented on facts of the case as they find that Google did not use a copyright on fair terms contrary to the majority opinion of the US Supreme Court senate. ,,Computer code occupies a unique space in intellectual property. Copyright law generally protects works of authorship. Patent law generally protects inventions or discoveries. A library of code straddles these two categories. It is highly functional like an invention; yet as a writing, it is also a work of authorship. Faced with something that could fit in either space, Congress chose copyright, and it

[8] Its idea was that more and more developers using its Android platform would develop ever more Android-based applications, all of which would makeGoogle's Android-based smartphones more attractive to ultimate consumers. Consumers would then buy and use ever more of those phones. Oracle America, Inc. v. Google Inc., 872 F. Supp. 2d 974, 978 (ND Cal. 2012); App. 111, 464. That vision required attracting a sizeable number of skilled programmers.

included declaring code in that protection." And ,,Hence, Congress rejected any categorical distinction between declaring and implementing code. Implementing code orders a computer operation directly. Declaring code does so indirectly by incorporating implementing code. When faced with general language barring protection for "methods of operation" and specific language protecting declaring code, the "'specific governs the general.'" RadLAX Gateway Hotel, LLC v. Amalgamated Bank, 566 U. S. 639, 645 (2012).This context makes clear that the phrase "method of operation" in §102(b) of US Copyright Act does not remove protection from declaring code simply because it is functional. That interpretation does not, however, render "method of operation" meaningless. It is "given more precise content by the neigh- boring words with which it is associated." United States v. Williams, 553 U. S. 285, 294 (2008). Other terms in the same subsection such as "idea," "principle," and "concept" suggest that "method of operation" covers the functions andideas implemented by computer code— such as math functions, accounting methods, or the idea of declaring code— not the specific expression Oracle created. Oracle cannot copyright the idea of using declaring code, but it can copy- right the specific expression of that idea found in its library."

Its strategy was to release Android to device manufacturers for free and then use Android as a vehicle to collect data on consumers and deliver behavioral ads. With a free product available that included much of Oracle's code (and thus with similar programming potential), device manufacturers no longer saw much reason to pay to embed the Java platform.For example, before Google released Android, Amazon paid for a license to embed the Java platform in Kindle devices. But after Google released Android, Amazon used the cost-free availability of Android to negotiate a 97.5% dis- count on its license fee with Oracle. Evidence at trial similarly showed that right after Google released Android, Samsung's contract with Oracle dropped from $40 million to about $1 million. Google contests none of this except to say that Amazon used a different Java platform, Java Micro Edition instead of Java Standard Edition. That difference is inconsequential because the former was simply a smaller subset of the latter. Google copied code found in both plat- forms. The majority does not dispute—or even mention— this enormous harm.

DURATION AND APPLICABILITY OF COMPUTER PROGRAMS PROTECTION IN THE SLOVAK REPUBLIC

The nature of litigation under the Civil Procedure Code, which is currently of fundamental importance for the development of the digital society and software engineering in Slovakia, requires a teleological interpretation. According to § 1 of Act no.35/1965 Coll.on Literary, Scientific and Artistic Works (Copyright Act) as amended: "*The purpose of this Act is to regulate the relations arising in connection with the creation and social application of literary, scientific and artistic works so as to protect the interests of authors and to ensure favorableconditions for the development of literary, scientific and artistic creation."*The legal assessment of computer programs is therefore based on three alternatives in the fact-finding, which is already envisaged by the last adopted Act No. 185/2015 Coll. Copyright Act as amended. According to the explanatory memorandum to the law: "*Within the exceptions and limitations of property rights, the authorized user may, without the consent of the author of the computer program, modify the computer program to the extent necessary for its proper use, making a backup copy or examining, studying or testing the functionality of the computer program. Another restriction of the property rights of the author of a computer program is the so-called decompilation, resp. back-translation of a computer program from machine code into the source code (text) of a programming language, for the purpose of obtaining information used to achieve interoperability of computer programs*." The information obtained by decompiling a computer program may not be used for other purposes and other than defined by law. ,,*If the use of computer programs beyond the above activities is unauthorized use*." As such, under the computer programs copyright protection, we may observe following situations that should be analysed during the fact finding of the litigation itself.

i) software engineers had access to the source code (§ 89 paragraph 3 letter c) of Act No. 185/2015 Coll. Copyright law ,,*The right of the author of a computer program does not*

interfere with an authorized user or licensee of a computer program who makes a copy of the source code or machine code of a computer program or part thereof or translates the source code or machine code of a computer program or part thereof without the consent of the author of the computer program. to the extent necessary to obtain the information necessary to achieve interoperability between the computer program and other independently created computer programs where that information was not previously commonly available. The information obtained under the first sentence may not be used to (c) ensure the development, production or marketing of a computer program similar in its expression, or any other activity which would infringe the rights of the author of the computer program. "

ii) software engineers had access only to the background and conceptual material (89 (2) (c) of Law No. 185/2015 Coll. Copyright law ,,*The right of the author of a computer program is not infringed by an authorized user if, without the consent of the author of the computer program, he examines, studies or tests the functionality of the computer program to determine the idea or principles underlying any part of the computer program during recording, display, transmission, verifying the functionality and storing a computer program in the computer's memory.*"

iii) software engineers need to link the original computer program with a new computer program in violation of the principles of fair trade (§ 89 paragraph 3, first sentence of Act No. 185/2015 Coll. Copyright Act), or translate the source code or machine code of the computer program or its parts to the extent necessary to obtain the information necessary for the interoperability of the computer program with other independently created computer programs, if that information was not previously commonly available).[9]

Historically, the substantive law on the protection of a computer program according to substantive law as a subjective absolute copyright is regulated by Act No. 35/1965 Coll. on literary, scientific and artistic works (copyright law). The literary form (literary work) of the computer program was agreed within the World Intellectual Property Organization (WIPO / OMPI) and subsequently implemented by Act no. 35/1965 Coll. on literary, scientific and artistic works (copyright law) as well as Section 5(18) and Section 6(1)point(a) of Act no. 383/1997 Coll. Copyright Act as amended. Council Directive 91/250 /EEC, which was effective at the time of Slovakia's accession to the EU, provided in Article 9(2): ,,*The provisions of this Directive shall also apply to programs established before 1 January 1993, without prejudice to acts which took place before that date and to rights acquired before that date.*" The accession of the Slovak Republic to the European Union means de jure that the legal regulation of computer programs was not substantially changed, the legal regulation was harmonized only for those Member States that did not specifically ratify the Berne Convention on Literary Works and the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). Directive 2009/24/EC, which took over the temporal provision of Directive 91/250 /EEC in its Article 1(4):,, The *provisions of this Directive shall apply also to programs created before 1 January 1993, without prejudice to any acts concluded and rights acquired before that date*".

[9] 'Unauthorized reproduction, translation, modification or alteration of the code in which the copy of the computer program was delivered threatens the exclusive rights of the author. Under certain circumstances, copies of the code and translation of its form are necessary to obtain the information necessary to achieve the operational capability of the independently created program with other programs. It is therefore necessary to provide that only in these limited circumstances is the reproduction and translation by a person entitled to use or on behalf of the copy of the program justified and compliant and therefore does not require the permission of the rights holder. One of the objectives of this exception is to enable the interconnection of all elements of a computer system, including those created by different manufacturers, so that they can work together. Such an exception to the author's exclusive rights may not be used to prejudice the legitimate interests of the rights holder or to jeopardize the normal use of the program.' Dr. et JUDr. Libor Klimek, PhD., Legal protection of computer programs in the European Union, Justičná revue 2015 / JR - 11/2015

In practice and in the framework of international scientific cooperation, as well as in attracting investors to companies engaged in research and development, it has been overly complicated for specific companies with such facts to convince third parties of the significance of their scientific research results. The protection of facts not subject to copyright or other protection therefore consisted only in the conclusion of specific confidentiality agreements, for which it was difficult to determine the safeguard in case of breach of contractual obligations and to present the way of functioning and operation of any innovative solution. If the work is not expressed, and there is no doubt that a particular person uses an almost identical technological solution, protection against the breach of trade secrets is possible. In accordance with the provisions of Section 17(1)of the Commercial Code, it is sufficient that the preparatory conceptual material has an intangible value, it is not a commonly available result of scientific research, the scientist or innovator did everything to keep this preparatory conceptual material confidential and ensure its confidentiality accordingly. The difference with such regulation is, however, that the legal regulation of trade secrets does not allow the claimant to claim rights from the originator but his employer, who should meet the definition of a company in the sense of Section 5 of the Commercial Code and also carries out business activities.

In addition to expert characteristics of creativity, an interesting characteristic from prof. Švidroň on creativity aspects of background will be described (Fundamentals of Intellectual Property Law, 2000). He characterizes creativity as an outpouring of the creative personality determined by his motivational (personality) horizon and this is given mainly by his education, life experience, development of his talent, sympathy for certain means of authorial expression, etc. From this point of view, the author's work is ontologically connected with its creator. Creativity does not distinguish between higher or lower creativity and there is no exact line between,, creative *and non-creative*". And this is where the stimuli from the spheres that are practically most affected by these issues are missing. When asked whether a result of intellectual activity corresponds to the postulated criterion of creativity, we often rely entirely on the relevant scientific or artistic disciplines of creation, their professional expression and expert evidence. According to Švidroň (2000), the author's personality traits include education, life experience, talent development, etc.

THE EUROPEAN UNION METHODOLOGY

The copyright protection of software was largely discussed from 2002 when the European Commission has proposed a Directive on the patentability of computer-implemented inventions. The proposal was discussed while the Council adopted a common position but the European Parliament has proposed a different approach and stressed out the importance of the interoperability of a computer programme with other programmes. As follows from the report, ,,*Unlimited patent protection for software could make it illegal under patent law to engage in reverse engineering practices employed by software developers to achieve interoperability as currently permitted under the exceptions in the Software Copyright Directive. Therefore future EU legislation related to software patents must include an explicit exception to patent rights in order to ensure that developers of software can continue to engage in the same acts to achieve interoperability under patent law as they are allowed to today within the limits of copyright law.*"[1011]

[10] https://www.europarl.europa.eu/sides/getDoc.do?reference=A5-2003-0238&type=REPORT&language=EN&redirect

[11] What constitutes an abuse under Article 102 must be judged by norms. Competition on the merits is the principal norm for exclusionary conduct, and as developed below, fairness is the principal norm for exploitative conduct. Application of the fairness norm has been the subject of remarkably little commentary, perhaps because economists and lawyers specializing in competition have little to say on fairness. Scholarly literature on exploitative abuse has not focused on when conduct infringes Article 102, but rather on when competition agencies should act against infringing conduct. Gregory J. Werden (2021) Exploitative abuse of a dominant position: a bad idea that now should be abandoned, European Competition Journal, 17:3, 682-713, DOI: 10.1080/17441056.2021.1930451

Case of Google LLC v. ORACLE AMERICA, INC was well followed in the United States of America[12], while in the European Union, the effect on trade was deeply analysed by the European commission in 2018 that imposed to Google LLC. a fine of 4,34 billion EUR because Google[13] imposed illegal restrictions on Android device manufacturers and mobile network operators to cement its dominant position in general internet search.[14] As the European Commission quotes: ,,*In 2005, Google bought the original developer of the Android mobile operating system and has continued to develop Android ever since. Today, about 80% of smart mobile devices in Europe, and worldwide, run on Android.*" When Google develops a new version of Android it publishes the source code online. This in principle allows third parties to download and modify this code to create Android forks. The openly accessible Android source code covers basic features of a smart mobile operating system but not Google's proprietary Android apps and services. Device manufacturers who wish to obtain Google's proprietary Android apps and services need to enter into contracts with Google, as part of which Google imposes a number of restrictions. Google also entered into contracts and applied some of these restrictions to certain large mobile network operators, who can also determine which apps and services are installed on devices sold to end users.

The breach of Antitrust rules lies than on three following actions:

1. Illegal tying of Google's search and browser apps.First, the tying of the Google Search app. As a result, Google has ensured that its Google Search app is pre-installed on practically all Android devices sold in the EEA. Search apps represent an important entry point for search queries on mobile devices. The Commission has found this tying conduct to be illegal as of 2011, which is the date Google became dominant in the market for app stores for the Android mobile operating system. Second, the tying of the Google Chrome browser. As a result, Google has ensured that its mobile browser is pre-installed on practically all Android devices sold in the EEA. Browsers also represent an important entry point for search queries on mobile devices and Google Search is the default search engine on Google Chrome. The Commission found this tying conduct to be illegal as of 2012, which is the date from which Google has included the Chrome browser in its app bundle.
2. Illegal payments conditional on exclusive pre-installation of Google Search. The Commission's investigation showed that a rival search engine would have been unable to compensate a device manufacturer or mobile network operator for the loss of the revenue

[12] By the European Competition Journal: 'The US Amex case also raises critical questions about the nature of optimal interaction between economics and law. As an organic discipline law borrows insights from multiple streams including economics. It is still, however, not clear as to the standards that an economic theory must conform to before it starts informing (at times shaping) the legal enforcement.' Vikas Kathuria (2019) Platform competition and market definition in the US Amex case: lessons for economics and law, European Competition Journal, 15:2-3, 254-280, DOI: 10.1080/17441056.2019.1644578

[13] 'In sum, we believe that the ad tech sector comprises at least the following markets: (i) a market for intermediation in online advertising (comprising ad exchanges and ad networks); and (ii) a market for ad serving technologies, which should be further segmented between ad servers for publishers and ad servers for advertisers. This does not exclude that further markets may have to be defined to account for additional ad tech products.' Damien Geradin & Dimitrios Katsifis (2019) An EU competition law analysis of online display advertising in the programmatic age, European Competition Journal, 15:1, 55-96, DOI: 10.1080/17441056.2019.1574440

[14] 'How we approach market definition in cases of multi-sided platforms essentially reflects upon our understanding of how platforms compete in the marketplace. At a time when our understanding of platform competition is still developing, it is too early to propose pre-defined criteria that run the risk of leading to an erroneous conclusion about the state of competition in the relevant market.' Vikas Kathuria (2019) Platform competition and market definition in the US Amex case: lessons for economics and law, European Competition Journal, 15:2-3, 254-280, DOI: 10.1080/17441056.2019.1644578

share payments from Google and still make profits. That is because, even if the rival search engine was pre-installed on only some devices, they would have to compensate the device manufacturer or mobile network operator for a loss of revenue share from Google across all devices.

3. Illegal obstruction of development and distribution of competing Android operating systems. Google has prevented device manufacturers from using any alternative version of Android that was not approved by Google (Android forks). In order to be able to pre-install on their devices Google's proprietary apps, including the Play Store and Google Search, manufacturers had to commit not to develop or sell even a single device running on an Android fork. In doing so, Google has also closed off an important channel for competitors to introduce apps and services, in particular general search services, which could be pre-installed on Android forks. Therefore, Google's conduct has had a direct impact on users, denying them access to further innovation and smart mobile devices based on alternative versions of the Android operating system. In other words, as a result of this practice, it was Google – and not users, app developers and the market – that effectively determined which operating systems could prosper.

CONCLUSION

To quote the European Parliament on the proposal for Directive on patentability of computer programmes from 2005: ,,*The controversy is how software should be protected: only by copyright or also by patent. A workable distinction is that a patent protects the practical application of knowledge, ideas or know-how, whereas copyright is not concerned with practical effects, but rather protects the expression of works (in the case of software, the code, in whatever form) against unauthorised reproduction or commercial exploitation. But there is a feeling that "copyright protects too little and patents risk protecting too much". Copyright protection is considered to have limitations as a means of protecting more than the actual coding of a computer program and there are misgivings lest patent protection should lead to patents being granted for inventions which do not satisfy the traditional criteria. The proposal for a directive as amended by the rapporteur resolves this dilemma reasonably and subtly.*" While in 2021, we may assume that computers programmes in its nature and its flexibility especially in order to interact with other programmes may not be subject of a strict regulation or a concrete temporary contractual mechanism. A fair use doctrine does not seem to be contradictory to principles of fair trade relations as laid down by the Commercial Code. The Slovak Republic Supreme Court quotes: ,,*It is expected that in its relations with other entrepreneurs it will promote its interest, use the opportunities provided by the legislation and strive to achieve the highest possible profit and improve its market position. On the other hand, the trader may not exceed the limits that result from the principles of fair trade in the promotion of his interests, he must not abuse the rights that he has acquired under the law. The application of the principle of fair trade is intended to protect contractual partners from bullying tendencies and practices in trading. Bullying would be the case if the enforcement of the law were clearly directed only to manifest harm to other entities.*"[15]

[15] Judgment of the Supreme Court of the Slovak Republic, file no. zn. 3 Obdo / 11/2008 of 18 June 2009

Legal acts:

US SupremeCourtjudgement in Google LLC v. ORACLE AMERICA, INC from 5th of April 2021

Feist Publications vs. Rural Telephone Service Co., 499 U.S. 340, at p. 361(1991). The word ''copying" is „shorthand" for the various activities that may infringe a copyright owner's exclusive rights. Range Rd. Music, Inc. vs. E. Coast Foods, Inc., 668 F.3d 1148, at pp. 1153 and 1154 (9th Cir., 2012).

Report of theEuropeanParliament on theproposalfor a directive of theEuropeanParliament and of theCouncil on thepatentability of computer-implementedinventions (COM(2002) 92 – C5-0082/2002 – 2002/0047(COD))

Summary of Commission Decision of 18 July 2018 relating to a proceeding under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the EEA Agreement (Case AT.40099 — Google Android) (notified under document C(2018) 4761)

Directive 2004/48/EC of 29 April 2004 on the enforcement of intellectual property rights

Directive 2009/24/EC of 23 April 2009 on the legal protection of computer programs

Code of Civil Procedure: Code of Civil Procedure, Act No 160/2015 as amended

Act No 84/2007 on the amendment of Act on copyright and rights related to copyright (copyright) and on the amendment of other acts as amended

Act No 40/1964 Civil Code as amended

Act No 513/1991 Commercial Code as amended

Act No 618/2003 on copyright on copyright and related rights (Copyright Act)

Act No 146/2000 on legal protection of topographies of semiconductor products

Judgment of the Supreme Court of the Slovak Republic, file no. zn. 3 Obdo / 11/2008 of 18 June 2009

Bibliography:

1. HUGHES, Anton,. The patentability of software: software as mathematics [elektronický zdroj]. New York, NY: Routledge, 2019. 1 online resource. ISBN 9781315283197.
2. Campbell Dennis. Copyright infringement. Alphen aan den Rijn, The Netherlands: Wolters Kluwer, [2018]. 1 online resource (xv, 266 pages). ISBN 9789403500843 (e-book).
3. Gregory J. Werden (2021) Exploitative abuse of a dominant position: a bad idea that now should be abandoned, European Competition Journal, 17:3, 682-713, DOI: 10.1080/17441056.2021.1930451
4. The Use of Technical Experts in Software Copzright Cases> Rectifzing the Ninth Circuit's ,,Nutty: Rule, 2020 Shyamkrishna Balganesh & Peter S. Menell., 35 Berkeley Technology Law Journal 663 (2021), 54 p.
5. JUDr. Tatiana Mičudová, Copyright disputes in civil proceedings, Bulletin SAK - 7-8/2017
6. SHEMTOV, Noam,. Beyond the code: protection of non-textual features of software [elektronický zdroj]. First edition. Oxford: Oxford University Press, 2017. 1 online resource. ISBN 9780191026171.
7. ȘTRENC, Alexandru Cristian,. European software directives and European software patents [elektronický zdroj]. Alphen aan den Rijn: Kluwer Law International, 2017. 1 online resource (145 pages). ISBN 9789041187734.
8. Campbell Dennis. Copyright infringement. Alphen aan den Rijn, The Netherlands: Wolters Kluwer, [2018]. 1 online resource (xv, 266 pages). ISBN 9789403500843 (e-book).
9. Vikas Kathuria (2019) Platform competition and market definition in the US Amex case: lessons for economics and law, European Competition Journal, 15:2-3, 254-280, DOI: 10.1080/17441056.2019.1644578
10. Damien Geradin & Dimitrios Katsifis (2019) An EU competition law analysis of online display advertising in the programmatic age, European Competition Journal, 15:1, 55-96, DOI: 10.1080/17441056.2019.1574440
11. United States Code, Section 107; United States Copyright Office Fair Use Index, More information on Fair Use, see https://www.copyright.gov./fair-use/more-info.html. The Fair Use Index provides searchable summaries of major fair use decisions.
12. Dr. et JUDr. Libor Klimek, PhD., Legal protection of computer programs in the European Union, Justičná revue 2015 / JR - 11/2015
13. MAREK, K. – LEŠKA, R. Spolupráce vysokých škol a ponikatelské sféry. In *Štát a právo* [online]. 2021, vol. 8, no. 1, pp. 44-60 [cit. dátum citovania]. ISSN 2644-643X. Available at: https://doi.org/10.24040/sap.2021.8.1.44-60
14. CRAIG, P., DE BÚRCA G., EU LAW, Third Edition, Oxford University Press, p. 115, ISBN 0-19-924943-1
15. FAIRHURST, J., Law of the European Union, p. 771, ISBN 978-1-4058-4688-2
16. TRITTON, G., Intellectual Property in Europe, p. 779, ISBN 0-421-54230-6

Kontaktné údaje:

JUDr. Viera Petrášová
vierapetrasova@gmail.com
Univerzita Komenského v Bratislave,
Právnická fakulta
Šafárikovo námestie 6
814 99 Bratislava 1

INTELLECTUAL PROPERTY IN TIMES OF CRISIS

Albert Priehoda

Comenius University in Bratislava, Faculty of Law

Abstract: The pandemic crisis induced by the Covis-19 virus has had significant consequences for the health and lives of people around the world. It caused a significant downturn in national economies. A solution offered by healthcare professionals is a vaccine effective against this virus. Vaccine development is time consuming, and efforts to accelerate it have been accompanied by billions in investment in research and development. The intellectual property aspect ensures the willingness of investors to invest considerable funds in the development of vaccines and enables the return on these investments. Intellectual property is also of legitimate importance as one of the tools for economic recovery and the faster return of companies to economic prosperity.

Abstrakt: Pandemická kríza vyvolaná vírusom Covis-19 spôsobila nemalé následky na zdraví a životoch obyvateľstva na celom svete. Spôsobila významný prepad národných ekonomík. Odborníkmi v oblasti zdravotníctva ponúkaným riešením je vakcína účinná proti tomuto vírusu. Vývoj vakcín je časovo náročný a snahu o jeho urýchlenie sprevádzali miliardové investície do vývoja a výskumu. Aspekt duševného vlastníctva zabezpečuje ochotu investorov investovať nemalé finančné prostriedky do vývoja vakcín a umožňuje návratnosť týchto investícií. Duševné vlastníctvo má svoj opodstatnený význam aj ako jeden z nástrojov pre oživenie ekonomík a rýchly návrat podnikov k ekonomickej prosperite.

Key words: Intellectual property, pandemic crisis, Covid-19, impact, economy, vaccine, health and economic consequences, global public goods.

Kľúčové slová: Duševné vlastníctvo, pandemická kríza, Covid-19, dopad, ekonomika, vakcína, zdravotné a ekonomické dôsledky, globálne verejné statky.

1 INTRODUCTION

In the long run, it was expected in some circles, but it was still a surprise for almost everyone. Not only because it came, but also with its scope and impact on the life of the whole society. Although the Covid-19 pandemic brought opportunities for some areas of the economy, it had a disproportionately negative impact on the development of economies around the whole world, causing declines in sales and corporate bankruptcies, declining incomes and the loss of employment of hundreds of thousands of employees. It made us change our lifestyle. In many cases, the necessary social distancing has led to the isolation of some groups of the population. It has claimed the lives of millions of people.

Immediately after identifying the virus as the cause of the problems, measures were introduced to reduce its human-to-human transmission. Face masks for respiratory protection, increased hand hygiene, social distancing, even lockdowns. Their implementation led to the suspension of production, the closure of sales outlets, the disruption of social events, the relocation of work to home office and much more. The measures were followed or not. And so was their effect. Somewhere bigger, elsewhere smaller. It was the right time to think again about the health condition and try to improve one's own immunity. No other solution was available.

According to experts, very generally according to health professionals, despite various risks and opponents, the most effective solution is vaccination. Antibiotics are effective against bacteria, but the treatment of viral diseases is still difficult and ineffective. The best solution seems to be vaccination, which reduces the probability of the outbreak of the disease and improves its course, as well as the consequences after its overcome. It significantly reduces the mortality of patients with these diseases.

However, the vaccine was not available at the beginning of the pandemic, it did not exist even more than a year after. It took an extreme effort, and a huge amount of money, to come up with a solution in the form of functional vaccines in such an unusually short time. Investment in the development and size of vaccines is estimated at billions of dollars invested by individual governments as well as private investors. According to Healthline media[1], the U.S. federal government only has put billions of dollars into the development of vaccines.

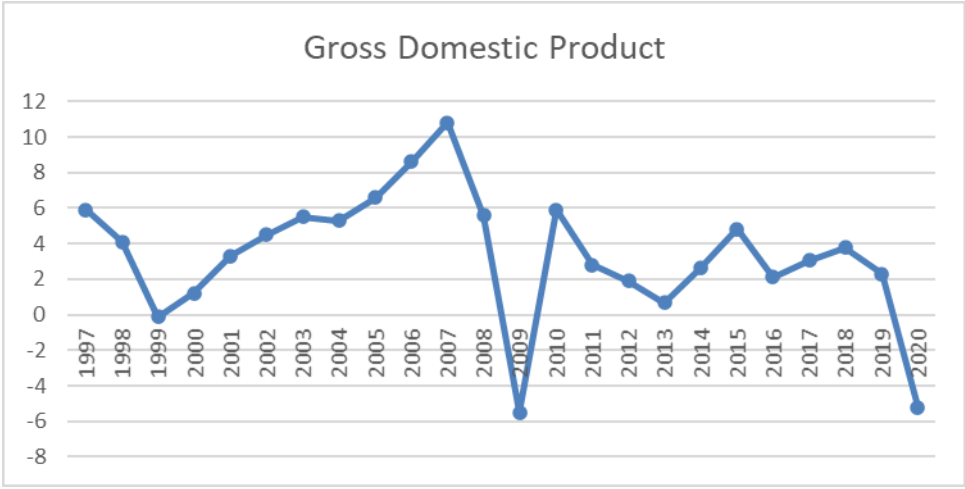
2 INTELLECTUAL PROPERTY IN TIMES OF CRISIS

The role of the vaccine is to save lives. The role of intellectual property, in this case, is to protect those who invest their resources in research and the production of such a vaccine.

The protection of intellectual property has a key role in ensuring the financial return on the energy and financial resources spent on development of Covid-19 vaccine. Intellectual property is also one of the aspects influencing how quickly national economies and individual businesses will recover from the economic crisis caused by this pandemic.

2.1 Impact on economy

The pandemic crisis in 2020 was an important parameter influencing macroeconomic development in the Slovak Republic. Based on data published by the National Bank of Slovakia[2], gross domestic product decreased by 4.8% year-on-year. During the period of existence of the Slovak Republic, it is the most significant decline in domestic production after the period of the financial crisis of 2009.

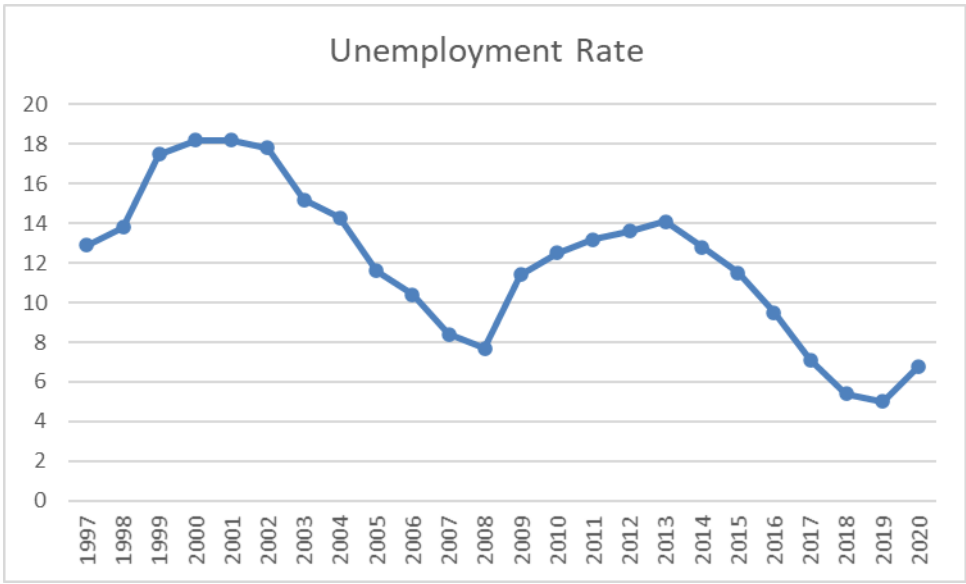


Graph 1: Gross domestic product development in the Slovak Republic, year-on-year change in % by the National Bank of Slovakia (own interpretation).

The negative effects of the pandemic crisis on Slovak economy were manifested in several areas. After a period of six years of the registered unemployment rate decline, unemployment rate rose from 5,0% in 2019 to 6.8% in 2020. In December 2020, compared to December 2019, the available number of jobseekers registered by the Labour, social affairs and family Office of the Slovak Republic increased by 71,667 to 207,184 jobseekers. This has led to a reduction in the disposable income of households, affected by job loss and a change in purchasing behaviour due to fears of job loss across the society.

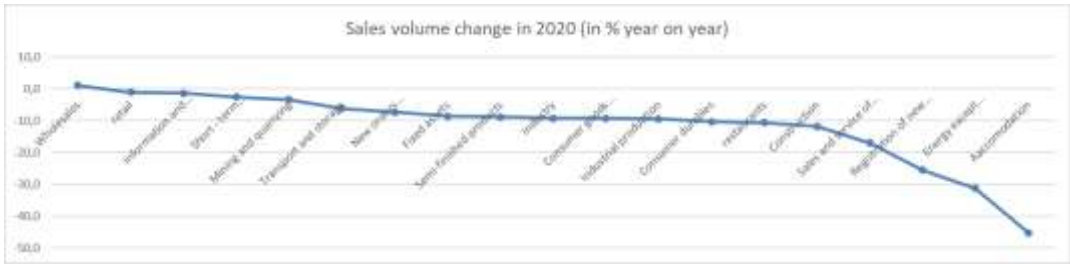
[1] How Much Will It Cost to Get a COVID-19 Vaccine? Online: https://www.healthline.com/health-news/how-much-will-it-cost-to-get-a-covid-19-vaccine.

[2] National Bank of Slovakia: Selected economic and monetary indicators of the Slovak Republic. Online: https://www.nbs.sk/_img/Documents/_Publikacie/OstatnePublik/ukazovatele.pdf.



Graph 2: Unemployment rate in the Slovak republic, year-on-year change in % by the National Bank of Slovakia (own interpretation).

Looking at the individual areas of the Slovak economy, the areas most affected by the anti-pandemic measures were accommodation services. In addition to some areas in the energy sector, a significant decline was recorded by registration of new passenger cars, sales and service of vehicles. Once again, it was confirmed that the construction sector is one of the first to show a decline during economic decline of the national economy. Restaurant services are the sixth area with a significant negative impact on revenues. There was also a significant decrease in the number of employees in this segment.[3]



Graph 3: Sales development in the Slovak Republic in 2020, year-on-year change in % by the National Bank of Slovakia (own interpretation).

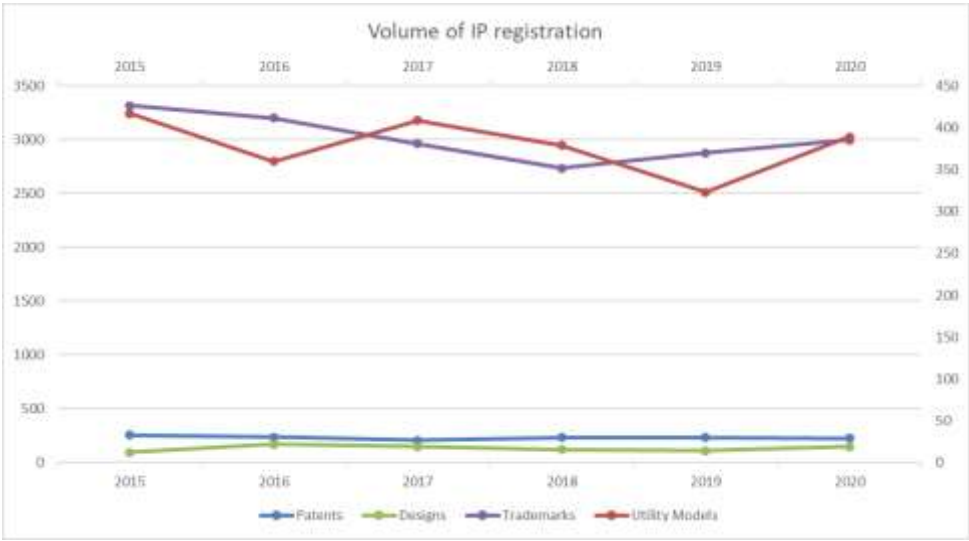
2.2 Impact on intellectual property

Based on the data from the Industrial Property Office of the Slovak Republic[4], the pandemic did not have a significant impact on the number of new intellectual property applications for registration. Areas of utility models, designs and trademarks even increased in 2020. The decrease of 4% was only reflected in the number of patents.

[3] National Bank of Slovakia: Selected economic and monetary indicators of the Slovak Republic. Online: https://www.nbs.sk/_img/Documents/_Publikacie/OstatnePublik/ukazovatele.pdf.
[4] Industrial Property Office of the Slovak Republic: Výročná správa 2020. [Online]. Banská Bystrica: UPV SR. 2021. Online: https://www.indprop.gov.sk/. ISBN 978-80-88994-97-8.

	2015	2016	2017	2018	2019	2020	yoy in %
Patents	256	235	206	231	234	225	-4%
Utility Models	417	360	409	379	323	389	20%
Designs	95	168	145	119	109	148	36%
Trademarks	3320	3202	2962	2737	2878	2999	4%

Chart 1: Number of new Intellectual property registrations in the Slovak Republic by the Industrial Property Office of the Slovak Republic (own interpretation).



Graph 4: Number of new Intellectual property registrations in Slovak Republic by the Industrial Property Office of the Slovak Republic (own interpretation).

2.3 Intellectual property impact on performance of companies

According to the report on Intellectual property rights and firm performance in the European[5] the figures about impact of intellectual property of business companies economic prosperity are impressive. A more detailed analysis of the overall picture reveals serious potential, especially when it comes to small and medium-sized enterprises (SMEs).

Although fewer than 9% of European SMEs rely on IPRs, this subset of companies appears to generate 68% higher revenues per employee than SMEs without IPR in their portfolios. The econometric analysis further shows that increases in companies performance depend on the type and combination of IPRs. The highest revenue-per-employee increases are linked to combined trade mark and design owners and combined patent, trade mark and design owners, with performance premiums of 63% and 60% respectively. Patent-only owners have 43% higher revenue per employee, trade mark-only owners 56%, design-only owners 31%, patent and trade mark owners 58%, and patent and design owners 39%. The highest revenue-per-employee gains are linked to bundles of trademarks, with performance premiums of 63% for the trade mark and design owners, and 60% for combined patent, trade mark and design owners. All the differences found are statistically significant, meaning that they are very unlikely to have come about purely by chance.

[5] EPO and the EUIPO: Firm-level analysis report: Intellectual property rights and firm performance in the European Union. [Online]. Munich: 2021, Pages 12-16. Online: www.epo.org/ipr-performance ISBN: 978-3-89605-263-6.

Companies that own IPRs also pay on average 19% higher wages than companies that do not. Revenue per employee for owners of IPRs (patents, trade marks and/or designs, national and/or European) is on average 20% higher than for non-owners of IPRs. This IPR ownership "revenue premium" is largest for patent owners at 36.3%, followed by design owners at 32.2%, and trade mark owners at 20.9%.[6]

3 CONCLUSION

I hope we are further than halfway in the "fight" with the Covid-19 pandemic. Effective vaccines are produced by several companies and their availability is constantly increasing. The expectations placed on the effect of the vaccine, protecting lives and health of the population, are linked to investors expectations of a return on their investment.

There is discussion about treating COVID-19 vaccines as global public goods because the protections of IPRs to the vaccine companies are slowing down the availability of the vaccine. On the other side, who will be willing to invest into research and development of the vaccine, without protection of the investment.

Bibliography:

Brown, G., Susskind, D.: International cooperation during the COVID-19 pandemic. Oxford Review of Economic Policy, Volume 36, Issue Supplement_1, 2020, Pages S64–S76. [Online]. Oxford: Oxford University Press, 2020. Online: https://doi.org/10.1093/oxrep/graa025.

EPO and the EUIPO: Firm-level analysis report: Intellectual property rights and firm performance in the European Union. [Online]. Munich: 2021, Pages 12-16. Online: www.epo.org/ipr-performance ISBN: 978-3-89605-263-6.

How Much Will It Cost to Get a COVID-19 Vaccine? Online: https://www.healthline.com/health-news/how-much-will-it-cost-to-get-a-covid-19-vaccine.

Industrial Property Office of the Slovak Republic: Výročná správa 2019. [Online]. Banská Bystrica: UPV SR. 2020. Online: https://www.indprop.gov.sk/. ISBN 978-80-88994-97-4.

Industrial Property Office of the Slovak Republic: Výročná správa 2020. [Online]. Banská Bystrica: UPV SR. 2021. Online: https://www.indprop.gov.sk/. ISBN 978-80-88994-97-8.

National Bank of Slovakia: Selected economic and monetary indicators of the Slovak Republic. Online: https://www.nbs.sk/_img/Documents/_Publikacie/OstatnePublik/ukazovatele.pdf

Sariola, S.: Intellectual property rights need to be subverted to ensure global vaccine access. [Online]. BMJ Global Health 2021;6:e005656. doi:10.1136/ bmjgh-2021-005656. Online: http://orcid.org/0000-0003-3401-7727.

Contact information:

Ing. Albert Priehoda, PhD.
albert.priehoda@flaw.uniba.sk
Comenius University in Bratislava, Faculty of Law, Institute of Economic Science
Šafárikovo nám. č. 6
P.O.BOX 313
810 00 Bratislava
Slovak Republic

[6] EPO and the EUIPO: Firm-level analysis report: Intellectual property rights and firm performance in the European Union. Munich: 2021, Pages 54-55, ISBN: 978-3-89605-263-6.

MONITORING OF EMPLOYEES DURING DOMESTIC WORK AND TELEWORK

Soňa Sopúchová

Comenius University in Bratislava, Faculty of Law

Abstract: The paper deals with the issue of legal monitoring of employees with reference to domestic work and telework. The crisis caused by the COVID-19 pandemic has caused an increase in cases of domestic work and telework, or cases that do not meet the legal definitions of domestic work and telework but are essentially the performance of work outside the workplace. The subject of the paper is an analysis of ways of monitoring employees and their possible use in cases of domestic work and telework, followed by clarification of whether such off-site monitoring is legally possible or whether domestic work and telework have such specifics that need to be taken into the account.

Abstract: Príspevok sa zaoberá problematikou zákonného monitorovania zamestnancov s poukazom na domácku prácu a teleprácu. Kríza spôsobená pandémiou ochorenia COVID-19 totiž spôsobila zvýšenie prípadov výkonu domáckej práce a telepráce, resp. prípadov, ktoré nesplňajú zákonné definície domáckej práce a telepráce, avšak reálne ide o výkon práce mimo pracoviska. Predmetom príspevku je rozbor spôsobov monitorovania zamestnancov a ich možného využitia v prípadoch domáckej práce a telepráce s následným objasnením, či je takéto monitovanie mimo pracoviska legálne možné alebo či majú domácka práca a telepráca také špecifiká, ktoré je pri otázke monitorovania potrebné vziať do úvahy.

Key words: employee monitoring, domestic work, telework

Keywords: monitorovanie zamestnancov, domácka práca, telepráca

1 INTRODUCTION

Employee monitoring is an issue that has aroused, continues to arouse, and is likely to continue to arouse, perhaps to a greater extent, discussions involving content ambiguities, different interpretations or differing opinions by employees, employers and also by impartial experts. However, there is a consensus that from a constitutional point of view, supported by legal sources of the Council of Europe and the European Union, employee monitoring, as a form of one of employers' rights, interferes with the right to privacy of a natural person. The status of a natural person as an employee does not change this fact. This statement will be further discussed in the paper and supported by legal arguments.

In today's digital society, information and communication technologies play an important role and are used in all areas of social life, including work. More and more employees use computers, telephones, computer programs, information systems and other information and communication technologies to perform their work, and more and more employers also find values of efficiency or reliability in them. These technologies can provide, on the one hand, a tool for employees for performing work tasks and, on the other hand, the possibility for employers for thoroughly ascertaining various information. In addition, the crisis caused by the COVID-19 pandemic has led to a huge change in the field of employment relations, which is primarily a matter of performing work outside the workplace and which is related to several aspects, including employee monitoring.

For the purposes of this paper, we have asked ourselves three questions. First of all, we found out whether the employer can legally monitor his employees during domestic work and telework. The second question concerned the monitoring of employees itself and its interference with two important human rights, namely the right to protection of personality and the right to protection of privacy, in connection with the employer's right to protection of his property and right to control of

employees' work efficiency. With the last question, we found out what legal protection does the Slovak legal system provide to employees affected by inadequate monitoring by their employers?

The aim of the paper is to answer and summarize the above questions, to draw attention to the identified ambiguities or inaccuracies and to provide considerations and suggestions to eliminate the consequences, which are often unjustified and capable of adversely affecting employees or their rights.

2 EMPLOYEE MONITORING AND PRIVACY

Monitoring of employees is an activity of the employer, which is based on the legal order of the Slovak Republic, specifically in the provision of 13 par. 4 of the Act no. 311/2001 Coll. Labor code (hereinafter referred to as the "Labor code"), the wording of which is as follows: „*The employer may not, without serious reasons based on the specific nature of the employer's activities, infringe on the employee's privacy at the workplace and in the employer's common areas by monitoring, recording telephone calls made by the employer's technical work equipment and checking e-mail sent from and delivered to the work e-mail address without notifying him in advance. If the employer implements a control mechanism, he is obliged to discuss with the employees' representatives the scope of the control, the method of its implementation, as well as its duration and inform the employees about the scope of the control, the method of its implementation and its duration*."[1]

It follows from the definition that in the case of monitoring there is a negative definition of cases where the employer cannot perform various, for example stated, activities, the essence of which lies in the monitoring of employees and their activities. However, we can also understand the issue in the opposite way, and thus when the employer may carry out such an activity. In general, these are legally defined possibilities for the employer's interference with the privacy of employees. It can be stated that here we encounter a significant consequence of monitoring employees, which is an invasion of their privacy. The importance of protecting privacy stems from article 8 of the Convention for the protection of human rights and fundamental freedoms, which guarantees everyone the right to respect for private and family life, home and correspondence.[2] The same right is enshrined in article 7 of the Charter of fundamental rights of the European union. Following mentioned European sources, it is not possible to omit the relevant legal regulation of the protection of privacy of a natural person within the Slovak Republic, in particular Act no. 460/1992 Coll. the Constitution of the Slovak Republic (hereinafter referred to as the "Constitution of the Slovak Republic")[3] and Act no. 40/1964 Coll. Civil code (hereinafter referred to as the "Civil code").[4]

---

[1] Provision 13 par. 4 of the Labor code.

[2] Article 8 par. 1 and 2 of the Convention for the Protection of Human Rights and Fundamental Freedoms.

[3] Article 16 par. 1 of the Constitution of the Slovak Republic: „*The inviolability of the person and his privacy is guaranteed. It may be limited only in the cases provided by the law.*"
Article 19 par. 2 of the Constitution of the Slovak Republic: „*Everyone has the right to protection against unauthorized interference with his or her private and family life.*"
Article 22 par. 1 of the Constitution of the Slovak Republic: „*Letter secrecy, secrecy of messages and other documents and protection of personal data are guaranteed.*"
Article 22 par. 2 of the Constitution of the Slovak Republic: „*No one shall violate the secrecy of letters or the secrecy of other documents and records, whether kept private or sent by post or otherwise; the exception is cases provided by the law. The secrecy of messages transmitted by telephone, telegraph or other similar device is also guaranteed.*"

[4] Provision 11 of the Civil code: „*A natural person has the right to the protection of his personality, in particular life and health, civil honor and human dignity, as well as privacy, his name and expressions of a personal nature.*"
Provision 12 par. 1 of the Civil code: „*Documents of a personal nature, portraits, images and video and audio recordings relating to a natural person or his expressions of a personal nature may be made out or used only with his permission.*"

2.1 General principles of employee monitoring

Violation of employees' right to privacy or its restriction by the employer is possible, but only in compliance with three principles - legality, legitimacy and proportionality. These principles are also reflected in the provisions of § 13 par. 4 of the Labor Code, which in the conditions of the Slovak Republic enables monitoring of employees.

The first of these principles, the principle of legality, means that invasion of privacy is only possible if it is in accordance with the law. This principle follows from the article 8 par. 2 of the Convention for the protection of human rights and fundamental freedoms[5], which is implemented in article 16 par. 1 of the Constitution of the Slovak Republic and was also confirmed by case law[6]. The principle of legitimacy follows from the same article and relates to the purpose of the intervention itself, which is permissible under this principle only if it is in the interests of the state (national and public security), society (country well-being, prevention of unrest and crime, protection of health or morals) or the individual (protection of the rights and freedoms of others). In this context, author Barancová states that the property interests of the employer can, under certain conditions, be considered as a legitimate aim of the interference with private and family life, residence and correspondence of the employee. Interference with the employee's privacy in that case depends mainly on the subject of the employer's activity, as well as on the assessment of the legal consequences in the event of a threat or violation of the employer's rights.[7] We agree with this view, because the categories of rights and freedoms of others can be classified both as a natural person and as an employer. The latter principle is the principle of proportionality, which refers to the need to comply with the necessary degree of intervention, that is to say, in the circumstances, a legitimate aim cannot be achieved otherwise. In practice, it is a matter of using the most lenient means so that the damage to the relevant human right is not disproportionate to the intended purpose and that the intervention is carried out in the spirit of the demands placed on a democratic society characterized by pluralism, tolerance and freedom.[8]

2.2 Conditions for monitoring employees according to the Labor Code

Conditions for monitoring employee are stated in the article 13 par. 4 of the Labor Code and employer who monitor employees has to be in compliance with them. In this part of the paper we will briefly explain the essence of these conditions and in the next part we will analyze them in connection with performance of domestic work and telework.

1. First of all, it is necessary to mention the condition of a serious reason consisting in the specific nature of the employer's activities as a justification for monitoring at all. The Labor Code does not specify what can be considered as a serious reason consisting in the special nature of the employer's activities, it does not provide a negative or positive definition, so it does not have to be a particularly dangerous activity or in any other way special. However, the legal interpretation of a serious reason must be interpreted in direct relation to the specific nature of the employer's activities.[9] The specific nature of the employer's activities may be activities in which the demands on the employee's behavior are increased (for example, with regard to the protection of classified information, confidentiality, protection of trade secrets, know-how, activities of financial institutions).[10] In the

[5] *„A public authority may not interfere with the exercise of this right unless it is not necessary in a democratic society in the interests of national security, public security, the economic well-being of the country, the prevention of unrest or crime, the protection of health or morals; the protection of the rights and freedoms of others.“*

[6] For example, Resolution of the Constitutional Court of the Slovak Republic, file no. II. 280/09-16 of the 10 September 2009. In addition, the legal basis for invasions of privacy should be sufficiently specific. Such a condition has been defined by the European Court of Human Rights, for example, in the judgment in Amann v. Switzerland of the 16 February 2000.

[7] BARANCOVÁ, H. Labor Code. Commentary, p. 251.

[8] The Ruling of the Constitutional Court of the Slovak Republic, file no. I. ÚS 274 / 05-73, of the 14 June 2006.

[9] BARANCOVÁ, H. Labor Code. Commentary, p. 250 .

[10] MACOVÁ, M. Violation of employee privacy at the workplace and in the common areas of the employer. In: Mzdové centrum.sk

interest of legal certainty of the employer and the employee, the employer may enshrine serious reasons for the stated purpose in the working rules, with which he is obliged according to the article 47 par. 2 of the Labor Code to inform the employee upon taking up employment. We deduce from the above that a serious reason for the specific nature of the employer's activities may be the protection of the company's assets (which is also the employer´s assets), including its know-how, information systems and the data contained in them, located in cyberspace.

2. The second condition for monitoring employees is that such an invasion of privacy can only take place at the workplace or in the common premises of the employer. As in the case of the first condition discussed, here we encounter a term that is not defined by the Labor Code, and that is the workplace. However, this term is legally defined in a by-law, which is the Regulation of the Government of the Slovak Republic no. 391/2006 Coll. on the Minimum safety and health requirements for the workplace, according to which a workplace is a place which is intended for the performance of employees' work on the employer's premises, to which the employee has access during the performance of work.[11] The term workplace must thus be distinguished from the term place of work, which is an essential part of the employment contract and can be a municipality, part of a municipality or another designated place. Thus, according to the available literature, a certain place in which an employee is to perform his work can be considered a workplace. It can be an office, a workshop or even a construction site.[12] This view has been confirmed several times by the case law, we refer to the decision of the Supreme Court of the Czech Republic, in which the court emphasized the difference between the place of work and the employee's workplace.[13] In accordance with the above-mentioned government regulation, we are of the opinion that the workplace is a narrower concept than the place of work and should be located in the premises belonging to the employer. In the case of domestic work and teleworking, it is questionable whether, for example, the employee's home could be considered a workplace, in particular in relation to safety and health aspects, observance of working hours and rest periods or observance of work discipline. These topics will be the subject of the next part of the paper.

3. The third condition for monitoring employees is the method of monitoring itself, which is set out in article 13 par. 4 of the Labor Code defined by various activities of the employer, the essence of which lies in monitoring the employee. These include monitoring, recording telephone calls and checking e-mail within the work e-mail address. At first glance, it seems that this is an exhaustive list of methods, but in a deeper analysis we find out that this list is, on the contrary, exemplary. This is due to the fact that while telephone call recording and e-mail control are relatively clear, the first method, which is monitoring, is a relatively broad activity that can include several activities from letter tracking, camera surveillance, through controlled entrances to buildings to remote access to computers, which can be used to check the visited websites and the time spent browsing them, to check any other activity of the employee or to block the visited websites.

4. The last condition of monitoring by the employer, which can be deduced from the wording of the article 13 par. 4 of the Labor Code, concerns the notification of an employee that he is being monitored. The legal diction is that the employer can not do so without notifying the employee in advance.[14] The ways of informing the employee can be different and the Labor Code does not specify the form of notification of employees, which means that this can also happen in an informal way, for example orally. The consent of employees is not required for the monitoring of employees, which also follows from the wording of the law, as it only presupposes notification of the employee that this activity

[11] Provision 2 of the Regulation of the Government of the Slovak Republic no. 391/2006 Coll. on the minimum safety and health requirements for the workplace.

[12] BARANCOVÁ, H. - SCHRONK, R. Labor Law, p. 259.

[13] Decision of the Supreme Court of the Czech Republic, file no. 21 Cdo 4596/2014, of the 26 November 2015.

[14] According to this provision, if the employer implements a control mechanism, he is obliged to discuss it with the employees' representatives, namely the scope, method and duration, and he is obliged to inform the employees about these conditions. If the employer does not have employee representatives, he can act alone without discussion, but still in compliance with the obligation to provide information to employees.

is taking place.[15] With regard to the latter condition of monitoring, we are of the opinion that in the event of an invasion of the employee's privacy, the warning and specific explanation of how the monitoring and invasion of his / her privacy takes place should be in a written and recordable manner. In our opinion, this condition becomes more significant in cases of domestic work and telework, where the monitoring of employees can take place in an environment outside the workplace, for example in his house.

3 Domestic work and telework

Slovak labor law legislation regulates the issue of domestic work and telework in the article 52 of the Labor code and the latest amendment to the Labor code was implemented as a result of the pandemic caused by the COVID-19 and amended mainly the wording of the provision regulating domestic work and telework. In the next part of the paper, we will analyze the new legislation, but the aim of the paper is not to compare the previous and current regulation.

Pursuant to the first paragraph of the article 52 of the Labor code, if it is work that could be performed at the employer's workplace, but the employee performs it regularly within the scope of his established weekly working time or part thereof from his household, it is a domestic work.[16] If domestic work defined in this way is carried out using information technologies, in which electronic data transmission at a distance takes place on a regular basis, it is a telework.[17] For the purposes of this paper, we call these types of housework and telework as „real" housework and „real" telework. As an example perceive we can mention a situation which is currently quite widespread, namely that an employee performs his work from home regularly once a week. The employer thus pursues his interests, because a certain number of employees work in the rented space-limited office space and another number works from home and these employees take turns at the workplace. For a given company, this means the possibility of reducing the cost of renting space, because smaller offices are enough. The employee also perceives this agreement positively, which can be confirmed by the fact that the so-called "home office" has become a job benefit, attracting employees to work in a company which offers the opportunity to work from home.

However, the second paragraph of the article 52 of the Labor code also contains a negative definition of what is not considered domestic work and telework. These are cases of work performed by the employee occasionally or in exceptional circumstances with the consent of the employer or in agreement with him from the household, provided that the given type of work allows him to perform from the household. In this context, we draw attention to the subsequent legislation, according to which it also applies that this type of work (which is not considered domestic work and telework but is performed from the household) will be subject to certain provisions on domestic work and telework, namely article 52 par. 8 letter (b) and paragraphs 9 to 11 of the same provision. We will call these cases „not real" housework and „not real" telework. As an example we can point out the current situation caused by the COVID-19, during which cases of domestic work and telework occurred occasionally, depending on the often changing epidemiological situation, or cases of prolonged domestic work and teleworking, but that were subject to exceptional circumstances and therefore it did not consider it real domestic work or real telework.

For the performance of real domestic work and real telework, the law provides several options for agreement and also several exclusions in connection with the application of certain provisions of the Labor code. In the next part of the paper, at the end of each point, we state whether that legislation also applies to not real domestic work and not real telework.

1. First of all, domestic work and telework must be agreed between the employer and the employee in the employment contract and one of the key aspects is the place of performance of such work. For a place agreed in the agreement can be also considered to be a place outside the

[15] In case the monitoring also relates to the personal data of the employee, Regulation 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46 / EC (General Data Protection Regulation) should be applied in connection with Act no. 18/2018 Coll. on the protection of personal data and on the amendment of certain laws.

[16] Provision 52 par. 1 letter a) of the Labor Code.

[17] Provision 52 par. 1 letter b) of the Labor Code.

employer's workplace[18], however it should not be any place outside the workplace, but one place agreed in advance. This obligation is also applicable to not real domestic work and not real telework.

2. The employee and the employer further adjust in the agreement the scope of domestic work or telework - the minimum time of work at the workplace and the distribution of working hours which the employee may determine himself within the whole week, or they agree that domestic work or telework will be performed during flexible working hours. If an employee can schedule working hours during domestic work and telework, his employment will be subject to exceptions from the application of certain provisions of the Labor Code, e. g. provisions on the allocation of specified weekly working hours, continuous daily rest and continuous weekly rest.[19] These working time arrangements do not apply to not real domestic work and not real telework.

3. As the last specific of domestic work and telework, we will mention the provisions of § 52 par. 8 of the Labor Code, according to which the employer is obliged to provide hardware and software equipment for the employee's work, ensure the protection of data processed during telework, reimburse the employee demonstrably increased costs if in agreement with the employer uses his own equipment, inform the employee about any restrictions on hardware and software equipment, to prevent the isolation of the employee and to enable the deepening of the qualification of the employee performing domestic work and telework so that it is comparable to the employee working at the employer's workplace.[20] These obligations of the employer apply to not real domestic work and not real telework only in the part of ensuring data protection.

In the context of the use of information and communication technologies in the field of labor law, the common denominator of several countries is the performance of work through teleworking. Within the countries of the European Union, the use of this method of work is relatively uneven, which is related to different approaches to the categorization of telework. Some countries define it in terms of place of work[21], others according to the frequency and regularity of its use in combination with the place of work.[22] The countries that have the largest share of telework include Denmark, Sweden or the Netherlands, and vice versa, the lowest share can be registered in Poland, Greece, Italy, but also in Slovakia and the Czech Republic.[23]

4 Conclusion

In the second chapter of this paper, we discussed the legal conditions for monitoring employees during the classic performance of work and we outlined the issue of compliance with them in the case of monitoring in the performance of domestic work and telework. In this context, it is necessary to reiterate that the Labor code regulates domestic work and telework in the provisions 52 par. 1, which we have called real and also cases that do not represent domestic work and telework, but they are the performance of work from the employee's household according to the provisions 52 par. 2, which we have called not real. The current time and existing information and communication technologies allow employers to monitor their employees remotely, and thus also during domestic work and telework. The subject of this paper was to determine whether in such a case all legal conditions of monitoring will be complied with, or is there a difference between monitoring in real domestic work and telework and not real domestic work and telework?

If we take a closer look at the conditions for monitoring employees, which we have divided into four points for the purposes of this paper, namely the serious reason consisting of the specific

[18] Provisions 52 par. 4 of the Labor Code.
[19] Provision 52 par. 7 of the Labor Code.
[20] Provision 52 par. 8 letter a) - f) of the Labor Code.
[21] MARTINO, V. The high road to teleworking. In: Dolobáč, M. The influence of telework on the mental health of an employee. In: Law, trade, economics . VII. Proceedings of the scientific symposium: 11.-13. October 2017, High Tatras. Košice: Pavel Jozef Šafárik University in Košice, 2017, p. 194 - 195.
[22] Eurofond and the International Labor Office. Working anytime, anywhere: The effects on the world of work. Publications Office of the European Union, Luxembourg, and the International Labor Office, Geneva, 2017, p. 5.
[23] Eurofond and the International Labor Office. Working anytime, anywhere: The effects on the world of work . Publications Office of the European Union, Luxembourg, and the International Labor Office, Geneva, 2017 p. 15.

nature of the employer's activities, workplace or common areas of the employer, methods of monitoring and notifying the employee about monitoring, we find that what it is necessary to analyze deeper is the workplace or common areas of the employer. In our opinion, other conditions can be followed in every type of employee monitoring, both in the classic performance of work and in domestic work and telework. If we start from the premise that the workplace is a place that is intended for the performance of employees' work in the employer's premises, to which the employee has access during work, then monitoring the employee in his household or other designated place under the provisions 52 par. 3 of the Labor code is not permissable. Employees working from their home, regardless of whether it is real domestic work and telework or not real domestic work and telework, use, in most cases, hardware and software provided by the employer, which is equipped with various software to ensure the cyber security of the company data, personal data and flows and other activities that occur in the performance of work by the employee. The valid legal regulation guarantees the employee the right to privacy also in the workplace and ownership of electronic devices for the performance of work shall not exclude the right to confidentiality of communication and other forms of privacy stipulated by the Constitution of the Slovak Republic. Another problematic aspect, which has not yet been mentioned in our legal analysis, is the absence of an adjustment of the employee's monitoring time. Provision 13 par. 4 of the Labor code does not stipulate when monitoring of an employee is possible and whether, for example, only within working hours. In that case, the question arises as to whether it can be deduced that the employee can be monitored only during working hours, as he stays in the workplace mainly during working hours. We consider this issue to be a complex legal issue, which is also related to the subject of this paper.

Legal protection of the employee in connection with his monitoring by the employer is regulated in the provisions 13 par. 8 of the Labor code, according to which an employee may seek legal protection in court if he considers that his privacy at the workplace or in the common premises of the employer has been violated by non-compliance with the legal conditions set out in paragraph 4 of the same provision. We believe that in the case of monitoring an employee and violating his privacy outside the workplace or outside the employer's common premises, the basic conditions of monitoring are violated, and thus the general principle of legality is violated because it is not performed in accordance with the law.

In connection with the development of information and communication technologies, it is necessary to admit that they always have an advantage over their regulation and the legal regulation must constantly respond to them. Fundamental human rights, such as the protection of privacy and the protection of the individual, are more endangered today than in the past, respectively there are new ways to violate or abuse them. The solution and our proposal de lege ferenda is an amendment to the Labor code, in which the legislator will deal with the fact that - the employee is monitored by the employer in the environment outside the workplace, because modern information and communication technologies basically allow it. Given their dynamic development and widespread use, it should be borne in mind that their use by employers in relation to employees should be regulated. The current crisis is an example that the situation we have known and in which we have been operating for years can change in a very short time.

References:

BARANCOVÁ, H. Labor Code. Commentary. First edition. Bratislava: C. H. Beck, 2017, 1424 p., ISBN: 9788081525285.

BARANCOVÁ, H. - SCHRONK, R. Labor Law. Second edition. Bratislava: Sprint, 2013, 598 p. ISBN 978-80-89393-97-8

MACOVÁ, M. Violation of employee privacy at the workplace and in the common areas of the employer. In: Mzdové centrum.sk

MARTINO, V. The high road to teleworking. In: DOLOBÁČ, M. The influence of telework on the mental health of an employee. In: Law, trade, economics. VII. Proceedings of the scientific symposium: 11.-13. October 2017, High Tatras. Košice: Pavel Jozef Šafárik University in Košice, 2017, p. 396-402, ISBN: 9788081525285

Convention for the Protection of Human Rights and Fundamental Freedoms

Act no. 311/2001 Coll. Labor code

Act no. 460/1992 Coll. the Constitution of the Slovak Republic

Act no. 40/1964 Coll. Civil code

Regulation of the Government of the Slovak Republic no. 391/2006 Coll. on the minimum safety and health requirements for the workplace
The Ruling of the Constitutional Court of the Slovak Republic, file no. I. ÚS 274 / 05-73, of the 14 June 2006
Eurofond and the International Labor Office. Working anytime, anywhere: The effects on the world of work. Publications Office of the European Union, Luxembourg, and the International Labor Office, Geneva, 2017, 72 p. ISBN 978-92-897-1569-0

Contact information:
JUDr. Soňa Sopúchová, Ph.D.
sona. sopuchova @ flaw.uniba.sk
Comenius University in Bratislava
Faculty of Law
Šafárikovo nám. 6, PO Box 313
810 00 Bratislava 1
Slovak Republic

THE IMPORTANCE OF COPYRIGHT DURING THE COVID-19 CRISIS

Petra Žárská

Právnická fakulta, Univerzita Komenského v Bratislave

Abstract: The Covid-19 crisis showed us the importance of a direct social contact. We might say that technological solutions saved us in the time of crisis, because it provides us with at least some social contact. While we cannot forget that technologies help us develop vaccines and keep in touch with relatives and friends, we should also mention tons of films and music consumed during this crisis in order to entertain us locked at our homes. We were able to watch films and listen to the music thanks to copyright. Undoubtedly, copyright through various technological means plays a vital role during the crisis. The author of this article focus on different benefits of the well-functioning copyright system and how it might help even more in future crisis.

Abstrakt: Kríza Covid-19 nám ukázala dôležitosť priameho sociálneho kontaktu. Mohli by sme povedať, že technologické riešenia nás zachránili v čase krízy, pretože nám poskytujú aspoň nejaký sociálny kontakt. Aj keď nemôžeme zabudnúť, že technológie nám pomáhajú vyvíjať vakcíny a byť v kontakte s príbuznými a priateľmi, mali by sme tiež spomenúť tony filmov a hudby použitých počas krízy, ktoré nás pobavili zamknutých v našich domovoch. Vďaka autorským právam sme mohli sledovať filmy a počúvať hudbu. Autorské práva prostredníctvom rôznych technologických prostriedkov nepochybne zohrávajú počas krízy zásadnú úlohu. Autorka tohto článku sa zameriava na rôzne výhody fungovania systému autorských práv a na to, ako by mohli v kríze v budúcnosti ešte viac pomôcť.

Key words: covid-19, crisis, copyright, technologies.

Kľúčové slová: covid-19, kríza, copyright, technológie.

1 INTRODUCTION

The Covid-19 crisis brought us many challenges. Suddenly, we found ourselves in a very unusual situation where one cannot go to work and see relatives and friends. While we were saved by technological progress in many occasions, like working from home and being in touch with family and friends, we also had to find a way a how to entertain ourselves during lonely evenings. Covid-19 showed us how important is the well-functioning system of Copyright. The author argues that the existing system of Copyright in EU helps us to overcome demanding times of Covid-19 crisis by offering applications, films and music that have kept us occupied and in touch with the world. The importance of Copyright is undeniable. All technologies using different kinds of copyrighted works played a vital role in fighting against the pandemic of Covid-19. The Author of article (further only as "Author") presents the advantages of the current Copyright system and then she focus on possible positive effects of article 17 of DSM Directive[1] on the Copyright system during Covid-19 crisis.

2 THE SUPORTIVE ROLE OF COPYRIGHT

Without doubts, the existing Copyright system enables people to access copyright protected works through various technologies. For the purpose of this article, the Author focuses on films, music and software used for communication, because the Author aims to highlight the importance of the well-functioning Copyright system in EU during the Covid-19 crisis by providing us with the

[1] The Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.

entertainment and communication. The world Copyright system is a complex organism consisting of international treaties governing the most important features of Copyright.[2] The Copyright system in EU accommodates all the international treaties and legislates its rules on Copyright in form of regulations and directives.[3] The international and regional EU protection of Copyright is completed by the national protection represented by national Copyright acts. Within this complex system of Copyright, stream services have to navigate its way of delivering films and music to consumers in the Covid-19 crisis. The providers of communication software rely on Copyright as well.

2.1 FILMS AND MUSIC

The Copyright system enables all consumers to access a content protected by Copyright, whether it is audio-visual or audio content. The providers of stream service are obliged to provide all content strictly within the law. The main legal means of providing the content by streaming services are license agreements. The biggest streaming services in terms of subscribers is Netflix.[4] "With 200+ million global subscribers, Netflix has capitalized on its position as the first and primary name in digital video streaming. In case of audio, Spotify is the biggest audio stream service and has 144 subscribers."[5] These streaming services can function due to the existing Copyright system. "Netflix partners with content providers to license streaming rights for a variety of TV shows and movies."[6] The streaming providers enter into the high number of license agreements due the high number and variety of offered films and shows. These agreements can be exclusive or non-exclusive depending on the authors of works. Thanks to the contract freedom, a principle upheld in EU and the majority of

[2] Berne Convection on the Protection of Literary and Artistic Works 1886, International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisation 1961, Agreement on Trade Related Aspects of Intellectual Property Rights 1994 (TRIPS Agreement), WIPO Copyright Treaty 1996 (WCT), WIPO Perfomances and Phonograms Treaty 1996 (WPPT), WIPO Beijing Treaty on Audiovisual Performances (BEIJING TREATY).

[3] The EU's regulatory framework for copyright and neighbouring rights (*acquis*) is a set of 12 directives and two regulations: Directive on the harmonisation of certain aspects of copyright and related rights in the information society ("InfoSoc Directive"), Directive on rental right and lending right and on certain rights related to copyright in the field of intellectual property ("Rental and Lending Directive"), Directive on the resale right for the benefit of the author of an original work of art ("Resale Right Directive"), Directive on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission ("Satellite and Cable Directive"), Directive on the resale right for the benefit of the author of an original work, Directive on the legal protection of computer programs ("Software Directive"), Directive on the enforcement of intellectual property right ("IPRED"), Directive on the legal protection of databases ("Database Directive"), Directive on the term of protection of copyright and certain related rights amending the previous 2006 Directive ("Term Directive"), Directive on certain permitted uses of orphan works ("Orphan Works Directive"), Directive on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online use in the internal market ("CRM Directive"), Directive on certain permitted uses of certain works and other subject matter protected by copyright and related rights for the benefit of persons who are blind, visually impaired or otherwise print-disabled, Directive on copyright and related rights in the Digital Single Market ("DSM Directive"), Regulation on the cross-border exchange between the Union and third countries of accessible format copies of certain works and other subject matter protected by copyright and related rights for the benefit of persons who are blind, visually impaired or otherwise print-disabled, Regulation on cross-border portability of online content services in the internal market ("Portability Regulation").

[4] *Visualcapitalist.com* [online webpage]. Which Streaming Service Has the Most Subscriptions?[cit. 2021-04-30]. Available at: https://www.visualcapitalist.com/which-streaming-service-has-the-most-subscriptions/

[5] *Visualcapitalist.com* [online webpage]. Which Streaming Service Has the Most Subscriptions?[cit. 2021-04-30]. Available at: https://www.visualcapitalist.com/which-streaming-service-has-the-most-subscriptions/

[6] *Netflix.com* [online webpage]. How does Netflix license TV shows and movies? ?[cit. 2021-04-30]. Available at: https://help.netflix.com/en/node/4976

jurisdictions, the content of agreements is mostly in the hands of parties. The parties can negotiate the term, territory and particular rights for licensing. The contract freedom of license agreements is a very important factor in offering works to consumers. Without such "wiggle room" the Copyright system would be stiff and would not accommodate the needs of streaming providers and consumers. The streaming services can negotiate license agreements directly with authors/rightholders or indirectly "rent the movies and shows from authorized distributors."[7] Although the licensing system is in majority of cases very convenient and practical, there are also disadvantages of it. The most serious disadvantage is territorially limitation of licensed rights[8]. Authors/rightholders may offer licenses only for a certain region or country, therefore a customer from EU cannot watch a film licensed only for the US and vice versa.

2.2 SOFTWARE

Another example of the well-functioning Copyright system is the communication software such as Skype, Teams, Zoom. The software was heavily use by billions of people for communication with families and friends. This virtual way of communication during pandemic has kept many families and relationships thriving. Not to mention the use for distant education and some novel ways of use, such as conducting medical interviews online[9]. The use of software applications is possible thanks to license agreements. Licensing of software is a very similar to licensing audio and audio-visual works with the same advantages and disadvantages. Licensing of communication software is easier thanks to the wide availability online. Consumers can download an application while agreeing to license conditions. Some communication software are even free of charge or the use is allowed under General Public License, which simplify the use for consumer and allow use this application around the world.

2.3 THE FUTURE OF COPYRIGHT SYSTEM

The future of Copyright system is digital and lies with paid streaming providers and free streaming providers like Youtube as well. In particular, free (or with certain paid memberships by subscribers) streaming services, legally defined as online content sharing service providers (further only "OCSS providers") could play a vital role in supporting authors and customers during the Covid-19 crisis. Why they did not play a vital role? The answer is connected to the fact that most of OCSS providers offer an unauthorised content - content without the consent of authors. EU attempts to improve the situation by implementing DSM Directive[10], specifically by article 17. This article has become highly controversial due to imposing the obligation of obtaining an authorisation from authors/rightholders. Moreover, the article also states that OCSS providers no longer can hide under the limitation of liability for hosting providers and when they share the content without authorisation, they are liable for unauthorised acts of communication to the public, including making available to the public, of copyright-protected works and other subject matter. The liability can be void when OCSS providers comply with three cumulative conditions. Firstly, they have to make best efforts to obtain an authorisation. Secondly, they have to make, in accordance with high industry standards of professional diligence, best efforts to *ensure the unavailability* of specific works and other subject matter for which the rightholders have provided the service providers with the relevant and necessary information. Thirdly, they have to act expeditiously, upon receiving a sufficiently substantiated notice from the rightholders, to disable access to, or to remove from their websites, the notified works or other subject matter, and made best efforts to prevent their future uploads. In the second obligation

[7] *Streamhash.com* [online webpage]. How does Netflix license TV shows and movies? [cit. 2021-04-30]. Available at: https://streamhash.com/how-does-netflix-license-tv-shows-and-movies/

[8] Kanza, Y. at all. *Smartmedia: Locally & contextually-adapted streaming media.* [online] SIGSPATIAL '20: Proceedings of the 28th International Conference on Advances in Geographic Information Systems. [cit. 2021-04-30]. Available at:https://dl.acm.org/doi/10.1145/3397536.3422338

[9] Ulman-Moskovits, J. et all. *Learning how to conduct medical interviews online forthe first time – this is what we learned in Frankfurt am Main.* In: GSM Journal for medical education, vol. 38(1), ISSN 2366-5017.

[10] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.

of OCSS providers, filters for unauthorised works are hidden. To *ensure the unavailability* of specific works has been proven as the biggest obstacle for OCSS providers. How is going the implementation of art. 17 going so far? Member states approach the implementation of DSM Directive in different manners. France, as a vocal supporter of DSM Directive, decided to speed up the implementation. "In order to speed up the transposition of the remaining provisions, the French government has chosen to include them in an authorisation law that allows the government to implement them by administrative decree. This Law on various provisions adapting to European Union law in economic and financial matters (DDADUE law) has been adopted by both houses of the French Parliament on the 18th of November 2020 and has been published in the official Journal on the 4th of December 2020. The DDADUE law gives the French government board leeway in implementing the provisions of the Directive. It specifies that the decree implementing Article 17 must be issued within six months after publication of the law in the official journal. For all other provisions of the Directive, the government has 12 months to implement (or six months and 4 days if the government wants to meet the implementation deadline of the Directive). In the Netherlands the proposed implementation law implementing all provisions of the directive is steadily moving through the legislative process. After the government introduced the law into parliament in June 2020, the legal affairs committee raised a number of concerns related to the implementation of Article 17 which was missing key user rights safeguards. In reaction, the Ministry of Justice proposed amendments that add the missing safeguards. On the 17th of November 2020 the second chamber of the Dutch parliament approved the implementation law with a broad majority. The proposed law is now before the 1st chamber (Senate) for a final yes-or-no vote which will likely happen early next year."[11] Germany is moving also steadily to implement DSM directive, while trying to improve its shortcomings. "In Germany the proposed implementation law has not reached Parliament yet and is still subject to intense public discussion. The German implementation proposal represents an ambitious approach to protect users' rights while at the same time ensuring that creators are remunerated for the use of their works on online platform. The German proposal does provide a template for implementing Article 17 in a way that minimises harm for users' rights while at the same time ensuring that creators are remunerated for uses of their works on online platforms."[12] How the situation regarding implementation in Slovakia. Although, Member States have until the 7th of June 2021 to implement the provisions of the Directive into their national laws, there are no news on the implementation on DSM Directive in Slovakia apart from listing the implementation of the DSM Directive in the Legislative plan of government for 2021.

Most Member states are waiting for the long delayed implementation guidance of the European Commission. France will have enough time to implement any changes stemming form the guidance and the Netherlands "implementation contains a clause that allows the government to issue further rules on the application of the provisions contained in Article 17. The Ministry of Justice has made it clear that it intends to use this clause to implement the Commission guidance as long as it serves the purpose of protecting users' rights. The Ministry of Justice has also indicated that it supports the Commission's proposal to limit the use of automated filtering to situations where a match can be considered to be likely infringing."[13] It seem wise to await for guidance before the implementation into national laws or allowing to have time for changes in laws after the deadline for implementation. The obligations are obtaining an authorisation from rightholders for the use of content.

[11] Communia-association.org [online webpage]. DSM Directive implementation update: six months to go and no end in sight [cit. 2021-04-30]. Available at: https://www.communia-association.org/2020/12/07/dsm-directive-implementation-update-six-months-go-no-end-sight/

[12] Communia-association.org [online webpage]. DSM Directive implementation update: six months to go and no end in sight [cit. 2021-04-30]. Available at: https://www.communia-association.org/2020/12/07/dsm-directive-implementation-update-six-months-go-no-end-sight/

[13] Communia-association.org [online webpage]. DSM Directive implementation update: six months to go and no end in sight [cit. 2021-04-30]. Available at: https://www.communia-association.org/2020/12/07/dsm-directive-implementation-update-six-months-go-no-end-sight/

3 CONCLUSION

Films, music, connections to relatives and friends have been provided through various technologies legally based on Copyright. The Author highlights the entertainment and connections, because the other types of the Intellectual property were popularize heavily, such as patents for vaccines. Generally, people do not realize how the well-functioning Copyright system improves our lives. The Covid-19 crisis has brought to light the fact, that we need the system to work its best. Before the Covid-19 crisis, probably not so many people were aware of deficiencies in the Copyright system. Some deficiencies are very serious and could impede the proper functioning of Copyright system. The Author argues that a very serious deficiency is the unauthorised content on websites of OCSS providers. EU devised the system of preventing it, though this system might not be perfect, it is worthy to try it out and find the ways how it could work efficiently. The Author also argues that if this system would function well before the Covid-19 crisis, it would increase revenues of authors/rightholders and improve access to copyrighted works by consumers.

Bibliiography:

Kanza, Y. at all. Smartmedia: Locally & contextually-adapted streaming media. [online] SIGSPATIAL '20: Proceedings of the 28th International Conference on Advances in Geographic Information Systems. [cit. 2021-04-30]. Available at:https://dl.acm.org/doi/10.1145/3397536.3422338

Ulman-Moskovits, J. et all. Learning how to conduct medical interviews online forthe first time – this is what we learned in Frankfurt am Main.In: GSM Journal for medical education, vol. 38(1), ISSN 2366-5017.

Online sources:

Communia-association.org [online webpage]. DSM Directive implementation update: six months to go and no end in sight [cit. 2021-04-30]. Available at: https://www.communia-association.org/2020/12/07/dsm-directive-implementation-update-six-months-go-no-end-sight/

Netflix.com [online webpage]. How does Netflix license TV shows and movies? ? [cit. 2021-04-30]. Available at: https://help.netflix.com/en/node/4976

Streamhash.com [online webpage]. How does Netflix license TV shows and movies? [cit. 2021-04-30]. Available at: https://streamhash.com/how-does-netflix-license-tv-shows-and-movies/

Visualcapitalist.com [online webpage]. Which Streaming Service Has the Most Subscriptions? [cit. 2021-04-30]. Available at: https://www.visualcapitalist.com/which-streaming-service-has-the-most-subscriptions/

Contact information:

Mgr. Petra Žárská, LL.M., PhD.
petra.zarska@uniba.sk
Comenius University
Šafárikovo námestie č. 6
Bratislava
Slovakia

PRÁVNICKÁ FAKULTA
Univerzita Komenského
v Bratislave