DIGITAL SURVEILLANCE IN THE TIMES OF COVID-19: LESSONS FROM SLOVAKIA

Matúš Mesarčík

Comenius University in Bratislava,
Faculty of Law, Institute of Information Technology Law and Intellectual Property Law,
Šafárikovo nám. č. 6, 811 00 Bratislava, Slovakia
matus.mesarcik@flaw.uniba.sk

Abstract

Digital surveillance in the form of dataveillance is one of the modern technological tools used for a variety of purposes. With the spread of coronavirus around the globe, digital measures were implemented to fight the pandemic. The article focuses on the right to privacy and the right to data protection as enshrined in the law of the European Union in terms of using such tools during the pandemic. Special emphasis is put on the analysis of the recent judgment of the Constitutional Court of the Slovak Republic suspending the effect of "Lex Corona" allowing public authorities access to location data held by telecommunication companies.

Key words: *digital surveillance, privacy, Covid-19, human right*

INTRODUCTION

The spread of different kinds of viruses globally is an integral part of our civilization. However, since the pandemics occurred at the beginning of the 20th century (e.g. Spanish flu in 1918), the situation has changed in terms of tools used to fight the spread of pandemic diseases.

With the development of computers and networks humanity is framed by the development of new technologies with a dynamic technological pace. It is no surprise that with the current pandemic caused by the uncontrolled spread of COVID-19, many countries deployed smart technology solutions aiding in many ways to stop or minimize the life & health risks. It is of the essence to note that many of the technologies involve the processing of personal data, therefore, triggering the application of data protection laws.

As the first COVID-19 cases had been discovered in Asia, Asian countries were first to implement technological solutions intended to "flatten the curve." The first smart solution was developed in Taiwan to enforce the obligatory quarantine.[1] In Singapore, the government obliged its citizens to install applications into their mobile phones exchanging information with other mobile phones in proximity via Bluetooth technology to trace potentially infected persons.[2] Moreover, people entering the country had to install another type of mobile application into their mobile phones and were obliged to wear also wristbands in order to monitor their compliance with mandatory quarantine.[3] The private sector in South Korea considered the tracking efforts of the government insufficient and supplemented the measures

1 Yasheng Huang , Meicen Sun and Yuze Sui. How Digital Contact Tracing Slowed Covid-19 in East Asia. Harvard Business Review Home. April 15, 2020. Available online: https://hbr.org/2020/04/how-digital-contact-tracing-slowed-covid-19-in-east-asia. [Accessed 22-05-2020].

2 https://www.gov.sg/article/help-speed-up-contact-tracing-with-tracetogether

3 https://www.coronavirus.gov.hk/eng/stay-home-safe.html

with own contact tracing apps for citizens.[4] China seized the options of insufficiently limited governmental access to data in the disposition of the private sector and also developed an app for surveillance of users.[5] The emergency just highlighted the specific dichotomy of privacy law in China as modern data protection rules are restricted by blanket governmental access to data and state surveillance rules [Pernot-LePlay, 2020].

Many digital initiatives introduced in Asia served as role models for the deployment of similar measures in the European Union (EU). However, respecting the values of human dignity and fundamental rights and freedoms as pillars of legal culture in the EU. Therefore, limiting indiscriminate and blanket use of such technologies. Restrictions of human rights and freedoms are subject to strict and specific legal conditions. On the other hand, the European Commission, however, is aware of the eventually positive impact of using technologies in the pandemic times, calls for a careful approach respecting fundamental rights and freedoms.[6]

Indeed, many countries introduced specific legal measures dedicated for development and implementation of technological tools to fight the spread of coronavirus within national borders. The Slovak Republic introduced the so-called "Lex Corona" allowing the state authorities to access data from telecommunication companies to help fight with the spread of COVID-19. However, the Constitutional Court of the Slovak Republic suspended the effect of the part of this law. The lessons from this decision could be seen as an example of future deployment of

4 https://hbr.org/2020/04/how-digital-contact-tracing-slowed-covid-19-in-east-asia

5 https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html

6 E.g. Coronavirus: a common approach for safe and efficient mobile tracing apps across the EU. https://ec.europa.eu/digital-single-market/en/news/coronavirus-common-approach-safe-and-efficient-mobile-tracing-apps-across-eu

such tools and laws in other EU member states.

This essay aims to emphasize the social and legal background of introducing smart technology solutions to protect health and life in the pandemic times on example of Slovakia. The first part of the article highlights the development of surveillance theories, legal background and soft law of digital surveillance (recommendations, opinions, and guidance) on the EU level in the context of the spread of coronavirus. The second part of the article examines adoption and analyses the wording of the Slovak "Lex Corona." The third part of the article is focused on the evaluation of the decision of the Slovak Constitutional Court of the Slovak Republic suspending effect of one part of "Lex Corona", and provides decision- based recommendations towards the future legal background of digital surveillance. Conclusions are delivered in the final part.

1. DIGITAL SURVEILLANCE AND THE EU APPROACH

1.1. Digital Surveillance

"The Big Brother is watching you" is one of the fundamental thoughts of George Orwell´s novel 1984. In the novel, behavior of society is enforced by constant video and audio surveillance. Although the plot is set in the near future, many academics and politicians refer to the novel when pointing out the threats and eventual abuse of digital technologies in terms of surveillance.

David Lyon defines surveillance as targeted, systematic and routine monitoring of personal data for influence, controlling, directing, and protection [Lyon, 2017: 14]. The aforementioned definition includes the use of modern technologies and shall be considered timeless. From the historical point of view, the shift from "physical" surveillance to digital surveillance may be observed. The aim of the article is not to provide a complete history of the surveillance theories [see Galič et. al, 2017]. However, we will point out the most important steps in the area. The first recognized concept of surveillance society is Panopticon creat-

ed by philosopher Jeremy Bentham. Bentham described prison "Panopticon" as rotunda- shaped area with an inspection tower in the middle, therefore, allowing one single guard to watch inmates in the cells around the rotunda [Bentham, 1791]. This concept was further analyzed by French philosopher Michele Foucault [Foucault, 1980]. The next phase of the surveillance theories leaves the traditional concept of Panopticon and reflect social and technological changes in the society. Gilles Deleuze emphasized globalization and capitalism in terms of surveillance of behaviour of consumers. The monitoring thus shifted from the state to private entities [Deluze, 1992]. The power of corporations is also noted by Kevin Haggerty and Richard Ericson criticizing the artificial application of Panopticon theories to every kind of surveillance [Hoggarty & Ericson, 2000]. Another rather popular surveillance theory emerged several years ago called "surveillance capitalism" coined by Shoshana Zuboff. This neo-Marxist theory of surveillance is based on the economic and political background of surveillance aimed to get profit from modeling and influencing the behavior of consumers by corporations. Zuboff even explicitly recognized the use of Big Data predictive technologies as a new tool to confirm her theory [Zuboff, 2015].

The current phase of surveillance theories is framed by the concept of dataveillance, i.e. data – based monitoring. The notion of dataveillance was first used by Roger Clarke in 1988. The object of the surveillance was the digital identity of the individual [Clarke, 1988]. Digital identity is composed of data of the individual based on his behavior in economic, social, and political relationships [Andraško, 2016]. With the emergence of profiling, data matching, data mining, and use of traffic or localization data a new definition of dataveillance have to be drafted. Roger Clarke together with Graham Greenleaf reframed the notion of dataveillance as "systematic creation and/or use of personal data for the investigation or monitoring of the actions or

communications of one or more persons." [Clarke & Greenleaf, 2017].

Dataveillance is not a science- fiction concept but reality and many individuals are subject to dataveillance without being aware of this. Using mobile applications with processing the information from the terminal equipment of users may be characterized as a form of dataveillance as providers of social media or other applications derive conclusions from our behavior and may use data for various purposes including marketing. What is more, monitoring via the collection of data is also a modern version of surveillance by state e.g. in case of tracking potential criminals or suspicious financial transactions [Mesarčík, 2018]. However, public authorities are under strict legal surveillance conditions, especially with dataveillance. Using such technologies shall not be blanket, indiscriminate, and shall respect the rule of law [Kasl, 2019], and such requirements are emphasised in the following next part of the article.

1.2. Legal Framework

Dataveillance as a form of surveillance involves the personal data processing and as such presents a threat to the privacy of individuals. In Europe, both rights to privacy and the right to data protection are strongly connected to the protection of human dignity and are stipulated as fundamental rights and freedoms.

The Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter referred to as "Convention") enshrines the right to respect private and family life in Article 8. The article contains positive and negative obligation of the states to protect privacy. The positive obligation means that everyone has the right to respect for his private and family life, his home and his correspondence and the state shall secure the performance of the right by legislation. On the other hand, negative obligation means that "there shall be no interference by a

public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[7] Although the Convention does not explicitly stipulate the right to data protection, many cases deliberated and decided by the European Court of the Human Rights concern the personal data processing,[8] therefore including the right to data protection within the scope of Article 8 of the Convention.

The law of the European Union (EU) establishes fundamental rights and freedoms in the primary law with secondary law specifying rules and values laid down by the primary law. The Charter of Fundamental Rights of the European Union (Charter) is part of the EU primary law and explicitly recognizes the right to privacy and the right to data protection as separate rights. The right to privacy is stipulated in Article 7 of the Charter and contains the same wording as Article 8 of the Convention. The right to data protection is enshrined in Article 8 of the Charter, and stipulates provisions that everyone has the right to the protection of personal data concerning him or her. Furthermore, it contains basic data protection principles and rules stating personal data shall be processed fairly for specified purposes and based on the consent of the person concerned or some other legitimate basis laid down by law. Some of the rights of data subjects are also presented in Article 8, namely right to access and right to rectification. Simultaneously, the Charter establishes the obligation for member states to designate one or more data

7 Article 8 (2) The Convention for the Protection of Human Rights and Fundamental Freedoms

8 To mention some S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, ECHR 2008 or Rotaru v. Romania [GC], no. 28341/95, ECHR 2000-V or Uzun v. Germany, no. 35623/05, ECHR 2010.

protection authorities supervising the processing of personal data by the private and public sectors. Secondary law lays down specifics of the data processing and the main legal act regulating the data protection area is currently the General Data Protection Regulation (GDPR).[9] However, another piece of secondary law has to be mentioned as "ePrivacy Directive"[10] and regulates the protection of privacy and electronic communications *inter alia* containing specific rules for providers of electronic communications (including telecommunication providers) and processing of information (including cookies) in the terminal equipment of users (including computers or mobile phones). This Directive shall be transferred to GDPR- like regulation, but the legislative procedure is slow and drafts of regulation are criticized by the private sector and academics [Mesarčík, 2019].

In terms of Slovak legal order, the Constitution of the Slovak Republic (hereinafter referred to as "Constitution")[11] stipulates the right to privacy and the right to data protection in several separate articles. The right to privacy and individual integrity is enshrined in Article 16 (1) of the Constitution. This provision is closely followed by Article 19 (2) declaring "the right to be free from unjustified interference in his or her private and family life." Human dignity and reputation are protected by Article 19 (1) of the Constitution and right to data protection are stipulated in Article 19 (3): "Everyone shall have the right to be protected against unjustified collection, disclosure and other misuse of his or her personal data." Article 22 of the Constitution provides the final installment in the mosaic of constitutional privacy pro-

9 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) (Text with EEA relevance). OJ L 119, 4.5.2016, p. 1–88.

10 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47.

11 460/1992 Coll. Constitution of the Slovak Republic.

tection protecting confidentiality of letters and communications including personal data. The relationship among the aforementioned articles is complex and has been the subject of the interpretation by the Constitutional Court of the Slovak Republic in many cases [Husovec, 2017]. These norms are of the utmost importance in the debate on dataveillance and using surveillance personal data - processing technologies in general.

1.3. The EU Approach During the Pandemic

The EU soon after the beginning of the spread of coronavirus recognized technological options and tools to stop or minimize the risks of the pandemic. After pilot solutions were developed, the European Commission (EC) issued several recommendations for using of these technologies.

The core of the use of smart tools involves the processing of localization data. Two solutions immediately emerged: (i) applications in smartphone and (ii) access to data processed by telecommunication companies. The importance of data together with artificial intelligence and supercomputers are explicitly emphasized by the EC as a useful tool in detecting patterns in the spread of the virus or potential treatments [EC.EUROPA, 2020]. The EC published a recommendation and communication in terms of use of these technologies namely:

- Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymized mobility data; and
- Communication from the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection 2020/C 124 I/01.

Data protection issues are also analyzed by the European Data Protection Board (EDPB) being the EU authority interpreting GDPR with its recommendations, opinions, and guidance. EDPB

issued Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak.

The recommendation of the EC aims to establish an effective pan-European approach in terms of using mobile applications enforcing social distancing or contact tracing together with the provision of a framework for the use of anonymized aggregated data for modeling predictions [REC, 2020: 1]. It provides a toolbox for developing such technologies and the use of data. The responsibility for the implementation of the recommendation is vested within the eHealth network, consisting of representatives of the EU member states [REC, 2020: 6]. Generally, with respect to the right to data protection, the recommendation emphasizes the strict limitation of the processing of personal data, regular review of the need for the processing of personal data and erasure of data after fulfilling the purpose [REC, 2020: 10]. Mobile applications processing personal data shall take into consideration respect for the right to privacy and the right to data protection. The recommendation explicitly highlights the implementation of safeguards ensuring respect for these rights including appropriate technical and cyber-security requirements for the security of data processing, using at least the invasive privacy solutions, require the erasure of personal data after fulfilling the purpose, and ensure sufficient transparency [REC, 2020: 16]. Concerning the second aim of the recommendation – modeling or predicting the spread of disease, the most preferred form of processing is the processing of anonymized or aggregated data preventing the de-identification [REC, 2020: 20].

Additionally, the EC issued a Communication concerning specifically on data protection issues in terms of trustful and accountable apps. Based on the Communication, national health authorities shall be controllers of personal data [COM, 2020: 3.1]. The Communication emphasizes that the individuals shall remain in control of data through the voluntary installation of the app and choosing different app functionalities. The individ-

ual shall have the choice to share his medical condition [COM, 2020: 3.2]. In terms of the legal basis, the Communication recommends using consent for storing and gaining access to the information stored in the device (ePrivacy directive) and legal obligation for national health authorities (GDPR) requiring member states to adopt specific laws regulating the legal obligation in question [COM, 2020: 3.3]. Controllers shall subsequently minimize personal data being processed for different purposes [COM, 2020: 3.4], restrict the access to data [COM, 2020: 3.5], provide specific purposes of processing [COM 2020: 3.6], adhere to the minimization of collection principle [COM, 2020: 3.7], ensure the security of processing [COM, 2020: 3.8] and accuracy of data processing [COM, 2020: 3.9]. Further clarification in terms of personal data processing is provided by the EDPB Guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak.[12]

However, the EDPB Guidelines address also the issue of the use of location data by other means than smart apps [EDPB, 2020: 2]. The Guidelines pragmatically differ between two sources of location data: (i) location data collected by electronic communication services providers, and (ii) location data collected by information society service providers [EDPB, 2020: 9]. The EDPB further elaborates on the legal framework provided by ePrivacy Directive regulating the processing of location data either directly collected by telecommunication companies or smart application providers. The guidelines highlight the potential need for derogations from general rules allowed by Article 15 ePrivacy Directive when they constitute a necessary, appropriate, and proportionate measure within a democratic society. This is the case of Slovak "Lex Corona."

12 See particularly part 3.

1.4. Limits of Surveillance in the EU Law: Digital Rights Ireland

Apart from the data processing perspective enshrined in the GDPR and ePrivacy Directive, digital surveillance conducted by the state has legal limits arising from the human rights perspective considering the right to privacy and right to data protection. Digital Rights Ireland[13] is the landmark decision of the Court of Justice of the European Union (hereinafter referred to as "CJEU") in this matter. Constitutional Court of the Slovak Republic follows the rationale of the judgment in its decisions.[14] The CJEU in Digital Rights Ireland assessed the compatibility of Data retention directive[15] in terms of Article 7 and Article 8 of the Charter. Data retention directive obliges the providers of publicly available electronic communications services or of public communications networks to retain telecommunication data generated or processed by them for potential access by law enforcement agencies in order to prevent, investigate and prosecute serious crime. The potential retention period was maximized to two years and the Directive obliges the retention of metadata, location data, and data necessary to identify the subscriber or user. The CJEU declared the data retention invalid due to wide-ranging interference with the right to privacy and data protection. The rationale of the judgment is essential because not only the CJEU declared the whole Directive invalid but it also provided requirements and their implementation stemming from the EU law for implementing surveillance measures in the digital society.

The CJEU clarified a two-step test in assessing the justifiability

13 C-293/12 from 8 April 2014 Digital Rights Ireland.

14 See e.g. PL. ÚS 13/2020-103 or PL. ÚS 10/2014.

15 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. OJ L 105, 13.4.2006, p. 54–63

of such interference with the right to privacy and data protection. Firstly, presence of an adequate ground for interference shall be assessed. Secondly, proportionality and severability of the measure are evaluated [Guild & Carrera, 2014:6]. In other words, collection of data shall be proportionate and necessary against the purpose of processing.[16] The CJEU further stipulates safeguards representing sufficient guarantees against the risk of abuse and against any unlawful access and use of that data,[17] namely subsidiarity of data use,[18] clear specification of purpose of processing,[19] and prior review carried out by a court or by an independent administrative body (independent supervision).[20] These criteria have been acknowledged and supplemented by the Constitutional Court of the Slovak Republic in the following data retention aftermath case after the Data Protection Directive was implemented in the Slovak legal order. This approach was expected by doctrine to solve the issue of national implementations [Martin, 2015] by the judiciary [Zanfir-Fortuna, 2015]. The Slovak court added three further criteria in terms of safeguards specifically ensuring a high level of protection and security,[21] erasure of data in a timely manner[22] and ex-post communication to data subjects about the data processing.[23]

These criteria and principles of necessity and proportionality shall be closely adhered to when drafting potential "surveillance" laws in any case including Slovak "Lex Corona."

16 § 58-59, Digital Rights Ireland.
17 § 54, Digital Rights Ireland.
18 § 62-63, Digital Rights Ireland.
19 § 61, Digital Rights Ireland.
20 § 62, Digital Rights Ireland.
21 § 124, PL. ÚS 10/2014.
22 § 136, PL. ÚS 10/2014 and § 68, Digital Rights Ireland.
23 § 136, PL. ÚS 10/2014.

2. SLOVAK "LEX CORONA"

2.1. Legislative Procedure

The new Slovak government was appointed on 21st March 2020, i.e. 15 days after the first COVID-19 infected person was detected in Slovakia. The government had to take immediate action to set up legislation and other measures in terms of the fight with the spread of coronavirus.

The first law introduced by the new government was the so-called "Lex Corona" *inter alia* allowing the National Health Authority (hereinafter referred to as "NHA") to ask telecommunication providers to provide data from mobile devices to help state authorities trace and contact potentially infected persons. It shall be noted that the law was adopted in the short legislative procedure - meaning that no public discussion took place and the law was adopted in 24 hours since it was introduced to the parliament. However, the Slovak legislation allows such procedure to be used e.g. in case of an imminent threat to human rights and freedoms.[24] Due to the fast pace of the spread of the coronavirus in the EU and danger for life and health the parliament decided to deliberate the draft of the law in the short legislative procedure. It shall be noted that the Constitutional Court of the Slovak Republic did not address the suitability of using the procedure in this matter.

2.2. Analysis of the Law

The amendment in question provides derogation from telecommunications secrecy in the Act on Electronic Communications (Act n. 351/2011 Coll.)[25] representing the implementation of the

24 § 89 (1), Act n. 350/1996 Coll. on the Rules of Procedure of the National Council of the Slovak Republic.

25 Available in the Slovak language at https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2011/351/20200327.

ePrivacy Directive[26] in Slovakia. The explanatory report[27] states that the aim of the Law is early identification of potentially infected individuals based on contact-tracing in the unnecessary time and scope to protect the life and health of citizens. The measure should be implemented based on positive experiences from Taiwan, Singapore, and South Korea.

The amendment allows NHA to ask telecommunications providers to provide localization[28] and related data[29] (traffic data were excluded) during the time or state of emergency in the healthcare. In Slovakia, the state of emergency has been declared by the government since March, and is based on constitutional law.[30]

Three situations (or purposes) of processing are provisioned in the amendment:

1. Anonymized data for statistical purposes to overcome, prevent and modeling for the prevention of health and life (Situation 1);
2. Identification of the recipient of messages that are informing about special NHA measures to protect health and life (Situation 2);
3. Processing exclusively to the extent necessary to identify

26 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47.

27 Available in the Slovak language at https://www.nrsr.sk/web/Dynamic/DocumentPreview.aspx?DocID=476589

28 § 57 (2) defines localization data as „any data processed in a network or by a service that indicates the geographic location of the terminal of a user of public service."

29 § 63 (1) b) defines related data: *„The related data of the communicating parties which are the telephone number, business name and the place of business of a legal person, or business name and the place of business of a natural person – undertaker or the personal data of a natural person which are the name, surname, title, and permanent residence address; the data published in the telephone directory shall not be subject to telecommunications secrecy.*"

30 Constitutional Act No. 227/2002 Coll. on State Security at the Time of War, State of War, State of Emergency, and the State of Crisis.

users to protect their life and health (Situation 3).

Data is provided on the specified NHA´s request to telecommunication companies. The NHA´s data processing is tied with the emergency period (the longest presumed period by the law is 31.12.2020).

3. THE DECISION OF THE SLOVAK CONSTITUTIONAL COURT

3.1. The Decision

Not shortly after the adoption of the Law, the most powerful party in opposition challenged the Law at the Constitutional Court of the Slovak Republic (CCSR) arguing a violation of privacy and insufficient safeguards against the data misuse.

On 13th May 2020, the Constitutional Court of the Slovak republic (hereinafter referred to as "CCSR") suspended the effect of the part of the amendment of the Slovak Act on Electronic Communications. It shall be highlighted that this is not the decision on the constitutionality itself. The CCSR decided to suspend the effect of the Law as there is an imminent threat of restriction of human rights and freedoms.

The legal analysis by the CCSR serves as a toolbox to provide the lawmaker with instructions in terms of future adoption of similar laws.[31] The CCSR in the introduction of the analysis stipulates that the Law allows indiscriminate and blanket processing of data by telecommunication companies and only the access of the NHA is specific and restricted.[32] All persons using mobile phones are therefore subjects of the surveillance measure.[33] The Court emphasized the need for fast implementation of technologies to fight the spread of disease. However, such implementation and a subsequent use shall not erode the rule of law.[34] The

31 § 112, PL. ÚS 13/2020-103.

32 § 63, PL. ÚS 13/2020-103.

33 § 64, PL. ÚS 13/2020-103.

34 § 71, PL. ÚS 13/2020-103.

CCSR only evaluated legal safeguards against potential abuse and clarity of the Law. Moreover, the legal analysis of the CCSR concerns also with possible risks of future application of the law and potential impact on human rights and freedoms.[1]

The Decision contains a separate analysis of collection and access to data for specific purposes. Concerning the processing of data exclusively to the extent necessary to identify users to protect their life and health (**Situation 3**), the CCSR held that the purpose of processing is vague, unclear and allows quantum of different interpretations.[2] The specification of purpose as ”protection of life and health” is not sufficient as the amendment is silent on specific measures and use of data.[3] The more invasive measure, the more precision of the clarity of the Law is required.[4] The CCSR thus concluded that due to potential abuse of accessed data by state for various purposes during the pandemic, the provision at stake does not comply with the Constitution of the Slovak Republic.[5] Concerning the legal safeguards, the CCSR noted that the Law did not contain specific mechanisms and control on the erasure of data, and the Law does not explicitly request the erasure itself, after fulfilling the purpose.[6] Furthermore, the amendment did not contain any independent supervision over the NHA´s access of data and no sanction in case of violation of the Law is provided.[7] In terms of subsidiarity, the CCSR stated that the Law did not require subsidiarity of the access and public control. In this case, the subsidiary would require access to data by public authorities restricted by time and scope based on the necessity of the ep-

1 § 78, PL. ÚS 13/2020-103.
2 §§ 82-85, PL. ÚS 13/2020-103.
3 § 83, PL. ÚS 13/2020-103.
4 § 84, PL. ÚS 13/2020-103.
5 § 85, PL. ÚS 13/2020-103.
6 §§ 87, 94, PL. ÚS 13/2020-103.
7 §§ 87, 92, PL. ÚS 13/2020-103.

idemiological situation.[8] Additionally, the amendment did not provide safeguards for the security of data processing and protection for data subjects.[9] The law does not reflect different levels of the necessity to gain the access based on epidemiological criteria as well.[10] The CCSR also emphasized that the Law did not contain any mechanism for informing the data subjects ex-post about the surveillance.[11]

Concerning the processing of data for the identification of the recipient of messages that are informed about special measures by the NHA to protect health and life (**Situation 2**), the CCSR´s opinion was that that unlike in Situation 2, the purpose is clear. However, the CCSR evaluated the process of transfer of data from telecommunication companies to the NHA and concluded that the state does not need to have any access to data for this purpose. Telecommunication companies can inform the data subjects without transferring the data to NHA on request. Therefore it is not necessary that data are firstly transferred to NHA and subsequently the NHA requests the telecommunication companies to inform data subjects about specific measures.[12] All safeguards mentioned in the previous parts of the Decision are absent for this situation as well.[13]

The CCSR did not suspend the effect of provisions allowing the collection and use of anonymized data for statistical purposes to overcome, prevent, and modeling for the prevention of health and life.

The Decision closely follows principles established in previous decisions in the surveillance cases in the EU (Digital Rights Ireland) and Slovakia (PL. ÚS 10/2014 – data retention case). In

8 §§ 87, 89-90, PL. ÚS 13/2020-103.
9 §§ 87, 93, PL. ÚS 13/2020-103.
10 § 87, PL. ÚS 13/2020-103.
11 § 95, PL. ÚS 13/2020-103.
12 §§ 104-106, PL. ÚS 13/2020-103.
13 § 107, PL. ÚS 13/2020-103.

addition, the Decision emphasizes that although the use of dataveillance technologies may serve as useful tools in fighting the pandemic, the scope and use of such technologies should be carefully assessed and balanced in terms of human rights.

3.2. Legislative Aftermath

After publishing the CCSR´s decision, the Parliament decided to amend the law in question. Moreover, all the situations covers also the NHA obligation to adopt organizational and technical measures for the protection of privacy and personal data processing. Furthermore, the request to access data is accompanied by the written or a verified consent of the data subject. Now, the Law explicitly requests the NHA to erase personal data after fulfilling the purpose of processing without undue delay and inform the data subject about such erasure by a written notice that contains the data processed. In addition, the NHA is obliged to submit "Report on the lawfulness of processing" to the Constitutional Law Committee of the Parliament by 31st January 2021.

In my opinion, the Parliament was too eager to adopt a constitutionally compliant amendment of the Law missing thus its aim. Although the new amendment contains the obligation to erase data after having the purpose fulfilled, the sanction is still absent in the legal order of the Slovak Republic as the supervising authority is not given any option for sanctioning the violation of provisions in the Act on electronic communications. Furthermore, the independent supervision by submitting the report to the Constitutional Law Committee of the Parliament is not strong enough as it represents an ex-post supervision without reflecting the assessment of lawfulness anyhow during the data processing by the NHA. Additionally, however the obligation to implement organizational and technical measures for the protection of privacy and personal data processing is a step forward, it still stays unclear whether these measures are suffi-

cient enough from the constitutional law point of view.

CONCLUSIONS

The EU recognises the right to privacy and the right to data protection as fundamental human rights. Every digital surveillance tool used for any purpose shall respect the essence of the aforementioned rights. Means of digital surveillance have significantly shifted from the first Panopticon theories to modern dataveillance conducted within the private or public sector.

These tools receive a wide attention now due to the spread of coronavirus worldwide and thus the surveillance measures enable to tackle the pandemic using modern technologies. The European Union´s bodies issued several communications and recommendations to emphasize the role of the right to privacy and the right to data protection concerning the time of using such measures. Two digital solutions emerged to fight against the pandemic – using some apps in smartphones, and an access to location data gathered from telecommunication companies enabling to trace the potentially infected individuals.

The Slovak Republic adopted "Lex Corona" allowing thus the National Health Authority accessing the location data held by telecommunication companies upon request for life & health protection purposes. This Law was challenged at the Constitutional Court of the Slovak Republic that suspended the effect of this Law. The Court highlighted that one of the possible purposes of the processing was unclear and vague. Moreover, legal safeguards against any abuse of such data were almost entirely missing. The Constitutional Court of the Slovak Republic closely followed its previous decision in data retention and the judgment of the Court of Justice of the European Union in Digital Rights Ireland. Although the Slovak parliament swiftly adopted the amendment of the "Lex Corona," the doubts on whether the requirements enshrined in the decision of the Constitutional Court of the Slovak Republic are fulfilled, stay still open.

REFERENCES

A Singapore Government Agency Website (2020), Help speed up contact tracing with TraceTogether, Available at: https://www.gov.sg/article/help-speed-up-contact-tracing-with-tracetogether [Accessed 22-05-2020].

Act n. 350/1996 Coll. on the Rules of Procedure of the National Council of the Slovak Republic, (1996), Available in the Slovak language at https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2011/351/20200327. [Accessed 22-05-2020].

Andraško, J. (2016), Bezpečná identifikácia a autentifikácia pri využívaní elektronických služieb verejnej správy. In Bratislavské právnické fórum 2016: Internet ako priestor možného porušovania práv. Bratislava: Univerzita Komenského, Právnická fakulta, 2016, p. 7-17.

Bentham, J. (1791), Panopticon; or the Inspection-House, T. Payne, London.

Clarke, R. - Greenleaf, G. (2017), Dataveillance Regulation: A research framework. University of New South Wales Law Research Series, s. 2.

Clarke, R. (1988), Information Technology and Dataveillance In Commun ACM 31,5, p. 498-512, Available at: http://www.rogerclarke.com/DV/CACM88.html [Accessed 22-05-2020].

COM. (2020), Communication from the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection 2020/C 124 I/01, Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020XC0417%2808%29 [Accessed 22-05-2020].

Constitutional Act No. 227/2002 Coll. on State Security at the Time of War, State of War, State of Emergency, and State of Crisis, (2002), Available in Slovak language at https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2002/227/20160102 [Accessed 22-05-2020].

Deleuze, G. (1992), Postscript on the societies of control, Winter.

EC.EUROPA (2020), Digital technologies - actions in response to coronavirus pandemic: Data, artificial intelligence and supercomputers, Available at: https://ec.europa.eu/digital-single-market/en/content/digital-technologies-actions-response-coronavirus-pandemic-data-artificial-intelligence-and [Accessed 22-05-2020].

EDPB (2020), Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, Available at: https://edpb.europa.eu/our-work-tools/our-documents/usmernenia/guidelines-042020-use-location-data-and-contact-tracing_en [Accessed 22-05-2020].

European Commission (2020), Coronavirus: a common approach for safe and efficient mobile tracing apps across the EU, Available at: https://ec.europa.eu/digital-single-market/en/news/coronavirus-common-approach-safe-and-efficient-mobile-tracing-apps-across-eu [Accessed 22-05-2020].

Foucault, M. (1980), Power/knowledge: selected interviews and other writings 1972–1977 (Ed. C. Gordon), Pantheon Books, New York.

Galič, M. – Timan, T. – Koops, B.-J. (2017), Bentham, Deluze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation, In Philosophy & Technology, Vol. 30, n.1.

Guild, E. & Carrera, S. (2014), The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive. CEPS Papers in Liberty and Security.

Haggerty, K. D. - Ericson, R. V. (2000), The surveillant assemblage. In British Journal of Sociology, 51(4), 2000, p. 605–22.

Harvard Business Review (2020), How Digital Contact Tracing Slowed Covid-19 in East Asia Available at: https://hbr.org/2020/04/how-digital-contact-tracing-slowed-covid-19-in-east-asia [Accessed 22-05-2020].

Husovec, M (2017), Courts, privacy and data protection in Slovakia, In Brkan, M. – Psychogiopoulou E., Courts, Privacy and Data Protection in the Digital Environment, Edward Elgar, Cheltenham.

The judgment of the Constitutional Court of the Slovak Republic PL. ÚS 13/2020-103, Available at: https://www.ustavnysud.sk/documents/10182/1270838/PL_+US+13_2020+-+Rozhodnutie+-+Uznesenie+z+predbezneho+prerokovania.pdf/464a47b6-66b4-4545-9a9f-eb0f10b4bd80 [Accessed 22-05-2020].

The judgment of the Constitutional Court of the Slovak Republic PL. ÚS 10/2014, Available at: https://www.ustavnysud.sk/docDownload/6c439346-cdfa-442d-86e7-5f616e2cf9f4/%C4%8D.%201%20-%20PL.%20%C3%9AS%2010_2014.pdf [Accessed 22-05-2020].

The judgment of the Court of Justice of the European Union n. C-293/12 from 8 April 2014 Digital Rights Ireland, Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 [Accessed 22-05-2020].

Kasl, F. (2019), Surveillance in digitalized society, In The Lawyer Quarterly, Vol 9, No 4.

Pernot-LePlay, E. (2020), China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU? In Penn State Journal of Law & International Affairs, Vol. 8, No. 1, 2020.

Lyon, D. (2017), Surveillance Studies. An overview. Polity.

Martin, L. (2015), The Fate of the Data Retention Directive: About Mass Surveillance and Fundamental Rights in the EU Legal Order. In Research Handbook on EU Criminal Law, Edward Elgar, Cheltenham.

Mesarčík, M. (2018), Sledovanie prostredníctvom údajov (dataveillance) v právnom poriadku Slovenskej republiky? In Bratislavské právnické fórum 2018 [elektronický dokument]: ústava na internete a internet v ústave. Bratislava : Právnická fakulta UK, s. 73-81.

Mesarčík, M. (2019), Predohra ku nariadeniu ePrivacy. In Comenius n. 11 (2019), p. 6-16.

New York Times (2020), In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags, Available at: https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html [Accessed 22-05-2020].

REC. (2020), Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data, Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32020H0518 [Accessed 22-05-2020].

The Government of Hong Kong Special Administrative Region (2020), "StayHomeSafe" Mobile App User Guide, Available at: https://www.coronavirus.gov.hk/eng/stay-home-safe.html [Accessed 22-05-2020].

Zanfir-Fortuna, G. (2015), How CJEU's 'Privacy Spring' Construed the Human Rights Shield in the Digital Age, In European judicial systems as a challenge for democracy", Intersentia, Cambridge-Antwerp-Portland.

Zuboff, S. (2015), Big other: surveillance capitalism and the prospects of an information civilization, In Journal of Information Technology, 30, 2015, p. 75–89.