The corona crisis, data protection and tracking apps in the EU: the Czech and Austrian COVID-19 mobile phone apps in the battle against the virus

JANA STEHLÍKOVÁ	Prague University of Economics and Business, Czech Republic
E-MAIL	xstej100@vse.cz
ORCID	https://orcid.org/0000-0002-8585-2303

ABSTRACT

The sudden outbreak of COVID-19 put governments under pressure to swiftly introduce measures to protect citizens and react appropriately to the emerging threat. This paper focuses on geo-location tracking mobile phone applications developed in the Czech Republic and Austria to monitor personal movement of those positively tested for COVID-19 to prevent the further spread of the disease. The aim of the analysis is to answer the question of whether the apps' functionalities complied with the EU data protection standards and to what extent the citizens' right to control the collection, evaluation and preservation of their personal data has been violated. Both countries belonged to the pioneers in COVID-19 apps. While they differed in several areas such as the legal and political circumstances under which the apps were developed and public communication, similarities between them were identified in the area of public trust in the apps and their utilisation. In both countries, certain illiberal issues were recognised as well.

KEYWORDS	geo-location tracking apps, COVID-19, data protection, data surveillance, liberal standards, Czech Republic, Austria
DOI	https://doi.org/10.32422/mv.1764

The COVID-19 outbreak turning into a global pandemic surprised the world at the beginning of 2020. Even though it is not the first time a virus with a high level of transmissibility through respiratory droplets has threatened humankind, never in history have we had the chance to make full use of digital technologies to fight it. Not to use the opportunity to utilise people's digital devices to stop or at least slow down the COVID-19 transmission would be absurd. Nevertheless, where a new opportunity emerges, potential negative side effects should also be examined. In this case, the individual's personal data and privacy are at stake (MALGIERI 2020; ZWITTER – GSTREIN 2020). Without an aim to disparage the benefits of digital technologies in combatting the disease, a global fight against a microscopic enemy should never serve as an excuse to undermine higher liberal values such as individuals' freedoms, human rights and privacy (MALGIERI 2020; MAATI – ŠVEDKAUSKAS 2020; GONZÁLEZ FUSTER – HILDEBRANDT 2020; LIPPERT – WALBY 2013; ZWITTER – GSTREIN 2020).

This paper focuses on the utilisation of digital technologies, namely geo-location tracking mobile phone applications, in two European Union (EU) countries, the Czech Republic and Austria, during the first months after the pandemic outbreak. The aim is to analyse whether the apps' functionalities complied with the EU data protection and liberal standards. Several reasons led to choosing these two countries for the analysis. Firstly, they represent two neighbouring states with comparable numbers of confirmed COVID-19 infections in their populations during the first wave of the pandemic.[1] Secondly, both countries were the European pioneers in introducing national geo-localisation apps, each putting the first version of its respective app in operation only a few weeks after the outbreak. Still, there are differences between the countries in other relevant aspects, such as the declaration of the state of emergency, the presence or absence of a long-term data protection public discourse, and communication of the app functionalities and standards to the public. The first wave also defines the time frame relevant to the case study, which is from March until August 2020.[2] This period was extraordinary due to the unforeseen challenge for the political authorities and the lack of experience and guidelines within Europe. The pressure to react to the crisis was high, while the guidelines were mostly missing and the control mechanism might have been failing. Thus, an opportunity for introducing some illiberal practices appeared (MAATI – ŠVEDKAUSKAS 2020; MALGIERI 2020).

Presenting two case studies, the article aims to answer the question of how the Czech Republic and Austria reacted to the spread of COVID-19 infection from the perspective of parallel respect for the privacy and personal data protection of their citizens. To fulfil this aim, each study is structured in four sections that provide answers to the following sub-questions: (1) Under which circumstances in the country were the measures undertaken and the national geo-localisation apps developed and introduced? (2) Do the national COVID-19 apps meet the requirements defined by the European *General Data Protection Regulation?* (3) How was the data protection concerning the COVID-19 app communicated to the public, and subsequently what was the citizens' reaction to the launching of the national app? (4) To what extent did the national authorities follow or reflect on the pan-European approach in their national response to COVID-19 in the area of personal data protection?

Methodologically, while being in the form of two case studies, the paper is based on an analysis of the digital tools introduced to slow down the COVID-19 spread and their compliance with the EU data protection framework and an evaluation of its liberal standards in regard to individual privacy. Besides reflecting on the current academic literature on (il) liberal practices, data surveillance and personal data protection in its first section, the paper mainly uses primary sources. These consist of data protection rules and regulations currently in force, governmental documents regarding measures undertaken during the pandemic in both countries and online sources dedicated to the developed geo-localisation applications.

The first section focuses on the (il)liberal practices regarding individual rights, privacy and data protection from the liberal perspective, and the perspective of security and critical surveillance studies. Furthermore, the section builds an evaluation framework of (il)liberal practices in a democratic system towards individual privacy and personal data protection to be used in the empirical part. The second section focuses on the personal data protection and privacy standards currently in force in the EU, which is followed by an overview of the guidelines provided by the European Commission and the European Data Protection Board in response to the pandemic outbreak. Finally, the last two sections are dedicated to an analysis of the data collection-related measures and the geo-localisation apps developed to slow down the spread of COVID-19 in the Czech Republic and Austria. Each of these two sections is divided into four parts according to the above-mentioned research questions.

(IL-)LIBERAL STANDARDS OF DATA PROTECTION AND GOVERNANCE OF PRIVACY

The digital age starting at the end of the 20th century has significantly transformed the world, not only from the perspective of international politics. Digitalisation has introduced scholars to a new dimension of thoughts, insights and understandings of security, privacy and freedom. Cyberspace is now considered the fifth domain of warfare, complementing the 'traditional ones' represented by land, sea, air, and space (CRAIG – VALERIANO 2018). With humans' unpreventable digital footprint, discussions over the role of governments in (non)regulation of cyberspace, monitoring of one's activities, personal data protection, and the state and other stakeholders' responsibility to protect their citizens' digital alter-egos have emerged and are represented in all authoritarian, post-authoritarian and democratic societies (ANDREW – BAKER 2019; BALL ET AL. 2019; BELLANOVA – GONZÁLEZ FUSTER 2018; COOKE 2015; HALLINAN ET AL. 2012; LIPPERT – WALBY 2013; UNVER 2017).

Opinions on a fundamental question – *whether to (not) regulate and to what extent?* – vary among authors. The liberal proponents' answers oscillate around the promotion of democratic principles, individual freedoms and human rights, equality, privacy, and protection of civil society instead of extensive state control and intervention (FLONK ET AL. 2020; HALLINAN ET AL. 2012; REIDENBERG 2000). Liberal authors thus advocate for the internet as a self-regulated sphere based on voluntary participation, albeit recognising the role of the state as an authority providing security and enforcing hard rules when needed (FLONK ET AL. 2020: 366). However, to define the line where one's privacy ends and the responsibility of the state to protect starts is not easy, regardless of the enemy represented by hybrid threats, surveillance, private companies or a biological threat.

The comfort that an online lifestyle provides to individuals, represented by the ease of finding a piece of needed information, contacting people from all around the world easily and free of charge, letting apps count the calories burned during a workout, etc., has left many people unaware of the data footprint they are leaving behind (BERG 2018; BUDAK ET AL. 2012; HALLINAN ET AL. 2012; FRIEDEWALD ET AL. 2017; ZAIA 2019). Despite the fact that the first warnings about data surveillance and its potential risk of interference in one's privacy appeared decades ago,[3] it has been the recent relevant cases, such as Edward Snowden's surveillance revelation,[5] the Cambridge Analytica affair[6] or the

US security concerns about the Strava app[7] followed by strengthening of data protection legislation in several countries, which have brought a well-deserved level of attention to this area. Once users are exposed to information on the data processing functionalities of the mobile location apps they use, their initial surprise is frequently replaced by a feeling of betrayal, indignation or resignation (FRIEDEWALD ET AL. 2017; SHKLOVSKI ET AL. 2014). *"The lack of understanding of the data environment [...] significantly reduces the ability for the individual to 'rationally' balance each action,"* explain Hallinan, Friedewald and McCarthy (HALLINAN ET AL. 2012: 12). Maybe surprisingly, when it comes to data surveillance in the European context, governments are considered to be more trustworthy than private companies by citizens (HALLINAN ET AL. 2012).

Data are not a given substance. They must be produced and captured (BELLANOVA – GONZÁLEZ FUSTER 2019) and as such they are rather neutral. At the same time, they represent a very valuable substance which can serve both public welfare and civilian oppression. As a positive example, data collected and analysed can be used for traffic and public transport utilisation to increase the efficiency of future urban planning or to reduce the energy intensity of buildings and lifestyles. The smart cities projects based on citizens' preferences, which are figured out according to their behaviour mapping, can provide inhabitants with various benefits (CHANDLER – FUCHS 2019). All these concepts are based on Big Data analysis – studying and evaluating of anonymised data packages of thousands of people in which an individual does not play any role. On the other hand, at the point of entry into the database system, the data are personal and represent one's usual behaviour, preferences, even private contacts. A single data set being misused can cause harm either to the individual him-/herself, or to the whole society if used to legitimise clustering and double standards, analysed by a specifically defined algorithm, etc.[7] (BALL ET AL. 2019; BELLANOVA – GONZÁLEZ FUSTER 2019; BIGO – TSOUKALA 2008; CAVELTY – LEESE 2018; CHAN – BENNETT 2015; HOSEIN – ALTSHULLER 2017).

The current debate about the liberal practices related to data protection can be framed by arguments made by scholars representing critical surveillance studies and data studies schools, though not exclusively. Indisputably, illiberal characteristics of privacy invasion can be present in democratic regimes, just as liberal standards are not exclusive and can be enforced by authoritarian regimes (BIGO – TSOUKALA 2008; FLONK ET AL. 2020; UNVER 2017).

Scholars and legal experts have introduced various concepts of personal data protection to prevent misuse and breach of personal information. Approaches focusing on liberal requirements emphasise democratic principles and individual freedoms, rights and privacy. Chris Berg (2018) describes the evolution of data protection regulation as a natural response to a rapidly changing technological environment. His arguments for the creation and enforcement of effective personal data protection standards are (1) the growing risk of violations of individuals' data privacy by both private and state entities, (2) the low level of digital literacy and (3) the need to support a multilateral institutional response to data surveillance as *"privacy violations in the twenty-first century require collective rather than individual responses"* (IBID.: 164). According to Rubinstein, *"[p]rivacy by design is an amorphous concept: there is no unique understanding or stabilized definition. A minimalistic view is that privacy by design happens when the attentive implementation of data protection principles is embedded in the design of a new technology"* (RUBINSTEIN 2011, QUOTED IN BELLANOVA 2017: 337).

The debate around data protection and state surveillance also demonstrates the attempts to disprove the "you have nothing to fear if you have nothing to hide" argument. This argument falsely reduces privacy to a form of secrecy aiming at hiding things (HALLINAN ET AL. 2012; SOVOLE 2011; ZAIA 2019). The right of every person to privacy should belong to the inviolable rights in all liberal societies, as is argued by liberal scholars against those advocating for more control to increase cyber- as well as human security (BALL ET AL. 2019; HALLINAN ET AL. 2012; RONA – GABOR 2016; SOLOVE 2011). Surveillance also potentially invades a variety of activities that are essential in a democratic society such as freedom of thought, expression or association. For that reason, high concerns were expressed about misuse of personal information, such as collecting too much information which can be potentially used against individuals either by the collector itself or by being shared without the permission of the concerned individuals (ANDREW – BAKER 2019; FRIEDEWALD ET AL. 2017). The individuals, despite having nothing to hide in the first place, are simply concerned about extensive information gathering by public as well as private entities (HALLINAN ET AL. 2012; FRIEDEWALD ET AL. 2017). Körner (2019) defined authoritarian regimes' surveillance and illiberal practices as systems under which *"elected governments and political groups might be tempted to use data to maintain their control, manipulate the electorate, and suppress dissent and opposition"* (KÖRNER 2019: 9). Illiberal regimes enjoy a level of access to the data of their citizens

that is not compatible with the norms of democratic societies, and which may allow them to bolster their position in a renewed competition of political systems for global supremacy (IBID.: 12).

Furthermore, Bellanova and González Fuster (2019) pointed out the contrast between the easiness of collecting and computer-processing enormous sets of data on one hand, and the difficulty and complexity of making relevant and meaningful use of them on the other, which complicates the surveillance control. The complexity of normative processes in cyberspace requires a high level of flexibility to accommodate to a constantly developing subject. Each situation is specific, and defined by its context and the identities of the actors involved, which might lead to prioritising contrary solutions in various contexts (FINNEMORE – HOLLIS 2016: 456–459). While online anonymity enhances the promotion of liberal values and democracy in authoritarian regimes, on the other hand, it also protects the perpetrators of malicious activity.

According to Lippert and Walby (2013), no dichotomy between technologies and security exists anymore, as IT tools have become an inseparable part of liberal governmentality. Surveillance, in the meaning of usage of personal details for purposes of management and protection, although containing definite authoritarian attributes, does not automatically refer to an illiberal order. The term digital authoritarianism refers to states' responding to losing control over the digital world by investing into surveillance technologies with a direct aim to regulate communication, monitor large segments of the population and collect an unprecedented amount of citizen information (UNVER 2017). The illiberal practices with dangerous implications emerge when the population is sorted, classified and subsequently inherently prevented from enjoying certain rights, opportunities and life chances as a consequence of the surveillance-related distributive justice (BALL ET AL. 2019; BIGO – TSOUKALA 2008). Furthermore, Bigo warns about the tendency to normalise exceptional measures on the part of the public.

Where does the regulator's authority end and one's private sphere begin? The primary responsibility of the state remains to ensure security and prevent future threats. In the context of the COVID-19 pandemic outbreak, the threat is represented by further spread of virus by infected individuals. Their personal data collection helps to isolate them from the rest of society, and hence serves as a preventive measure. Not using modern

technologies for this purpose would be absurd (ALI ET AL. 2016; HALLINAN ET AL. 2012; MALGIERI 2020), but this cannot serve as an excuse for any kind of unjustified ostracism or social exclusion. Furthermore, one's digital privacy should never be violated in the name of predicting and pre-empting threats to national security if unnecessary (AMOORE 2014, QUOTED IN COOKE 2015; DE GOEDE 2014; MALGIERI 2020).

The challenge of balancing personal data protection in the time of pandemic is obvious. The Austrian data privacy activist Max Schrems has warned citizens to remain careful of the rights they are giving away at a time of global panic: *"I am worried that we will accept state surveillance during the health crisis but that it will then take years in court to get rid of it"* (SCHREMS, QUOTED IN FINDES – ESPINOZA 2020). His words markedly remind one of warnings about surveillance practices implemented by governments worldwide in the context of the anti-terrorism measures after the 9/11 attacks (BIGO – TSOUKALA 2008).

So, how to define liberal practices in the fight against the COVID-19 pandemic while combining the maximal utilisation of digital technologies with a simultaneous respect for privacy, citizens' personal data protection and surveillance prevention? First, the existing legal framework in liberal democracies should be obeyed to ensure that the pandemic does not serve as an excuse for surveillance by any stakeholder, whether it be a state or a private one. Theoretically, the EU citizens are protected from personal data surveillance by the most ambitious and comprehensive normative framework yet existing in the developed world (BERG 2018: 161), based on decades of political and legal negotiations (BIGNAMI 2005; VAN ALSENOY 2019). Maintaining the rules while formulating the response to the COVID-19 pandemic should guarantee the appropriate liberal standards and liberal attitude promoted by the EU should have embraced aspects of international interdependence and called for heightened international cooperation (MAATI – ŠVEDKAUSKAS 2020). Yet with lacking clear guidelines, especially during the first wave of the pandemic, a temptation to abandon liberal values might have occurred.

THE REACTION TO THE PANDEMIC OUTBREAK AT THE EU LEVEL REGARDING THE PERSONAL DATA PROTECTION

The EU privacy and personal data protection framework not only regulates the private data created within the EU borders but poses the same limits on all private companies that are operating with the EU citizens' data all over the world. In the context of analysing the reaction to the pandemic,

the *General Data Protection Regulation* (GDPR) and the *ePrivacy Directive* play the main role. Whilst the *ePrivacy Directive* protects individual data located on mobile devices from being accessed via mobile communication networks, the GDPR regulates the collection, utilisation, preservation and transmission and of personal data. Despite the GDPR not being in effect for a long time yet, its core standards highlight the liberal principles incorporated in the *Charter of Fundamental Rights of the European Union* and Article 16 of the *Treaty on the Functioning of the European Union*, in which everyone's right to the protection of personal data is already incorporated and the EU institutions, as well as the Member States, are obliged to respect that and act accordingly (TFEU 2012).

To assess the compliance of the geo-localisation and tracking applications launched in EU countries to fight the spread of COVID-19, especially the Articles 4, 7, 8, 9, 11, 17 and 20 of GDPR need to be looked at. The personal data of EU citizens can be collected only upon their freely given, specific and informed consent (ARTICLE 4, GDPR), which can be withdrawn in an easy manner (ARTICLE 7, GDPR). All the data needs to be pseudonymised and after that, it can no longer be attributed to a specific data subject without the use of additional information (ARTICLE 4, GDPR). The data controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject (ARTICLE 11, GDPR). The data subject has the right to receive information about the personal data collected and processed concerning him or her at any time (ARTICLE 20). Furthermore, the data subject possesses the right to erasure if their personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed or if he or she withdraws their consent on which the processing is based (ARTICLE 17, GDPR).

However, because of the unforeseen dynamic outbreak of the COVID-19 pandemic, during its first days and weeks, specific guidelines for an adequate response to it within the EU borders that would comply with EU legal standards were missing. On March 19, 2020, the European Data Protection Board (EDPB)[8] adopted a statement on the processing of personal data in the context of the COVID-19 outbreak (EDBP 2020) to provide the Member States with the first guidelines on this in the liberal standards framework. The EDPB reminded the Member States that the GDPR foresees derogations to the prohibition of processing certain special categories of personal data, such as health data, where it is necessary for

reasons of substantial public interest in the area of public health (ARTICLE 9). Nevertheless, they also emphasized that: *"even in these exceptional times, the data controller must ensure the protection of the personal data of the data subjects.[..]Emergency is a legal condition which may legitimise restrictions of freedoms provided these restrictions are proportionate and limited to the emergency period"* (IBID.). In a democratic society, such an interference must be necessary, in the interest of national security and public safety, for the protection of health, and proportional (BIGNAMI 2005).

Moreover, for the processing of electronic communication data, such as mobile phone location data, the *ePrivacy Directive* must also be respected. Location data can only be used when made anonymous by the operator or with the consent of individuals. The *ePrivacy Directive* enables Member States to introduce legislative measures related to such data to safeguard public security (ARTICLE 15, EPRIVACY DIRECTIVE), and such exceptional legislation is only possible if it constitutes a necessary, appropriate and proportionate measure within a democratic society (IBID.).

The European Commission (EC) urged the national authorities not to misuse the exceptional situation by not respecting the legal standards and individuals' privacy when putting into force restrictive measures and developing geo-location tracking tools. That would possibly lead to an unwelcome abandonment of liberal values and, if further maintained, an unwelcome shift towards legitimisation of illiberal practices among the EU Member States. To prevent such a shift towards COVID-19-related data surveillance in the EU, the EC adopted the *Recommendation*[9] on April 8, 2020, followed by the *EC Guidance*[10] on April 17, 2020. Firstly, the EC's *Recommendation* recognises that the mobile phone applications might interfere with the exercise of certain fundamental rights related to privacy; thus, ensuring compliance with the data protection principles is a must. Secondly, in the document, three types of mobile application functions representing different levels of risk to people's privacy are differentiated. Whilst informative apps that provide users with erudite information about the virus only do not represent a threat to data surveillance, the warning and monitoring app functions, on the other hand, require various data inputs and collect information about users and their activity. Thus, particularly in the case of geo-location and tracking-based app, the principles of justification, proportionality and voluntariness are unbreakable. Citizens, as the EC emphasised, cannot be obliged to use movement tracking apps, all

the data collected by them must be encrypted, anonymised and aggregated, and their use is strictly limited to the purpose of fighting COVID-19. The principle of voluntariness also indirectly responds to the potential problem of discrimination as not every EU citizen owns a device that would enable them to use the application. Finally, the interoperability of the national applications is expected to not hamper combatting the virus by fragmentation as a restoration of freedom of movement is anticipated (EC 2020A).

To fulfil the *EC Recommendation*, specified rules for the tracing applications were introduced by the *EDPB Guidelines 04/2020*[11] on April 21, 2020. The *Guidelines* differentiate between two models. Under the centralised one, the anonymised data are uploaded to a remote server. Should a person become COVID-19 positive, contact matches with other users are processed. The decentralised model, on the other hand, gives users more control over the collected information. In this model all the data are stored in the mobile phone only. Each user is given a unique code, and the matches are made with people who may have been in contact with the virus (CRIDDLE – KELION 2020). According to the EDPB, preference should be given to the decentralised model by national authorities. The controller of any contact tracing application, preferably national health authorities, should use the data for purposes related only to the management of the COVID-19 crisis. Finally, the application should not under any circumstances collect information not related to COVID-19, such as one's civil status, communication identifiers, equipment directory items, messages, call logs, location data, device identifiers, etc. (IBID.). As the *Guidelines* are not legally binding, it is therefore up to app developers and national governments to decide how to proceed in this regard. Still, if any European approach to this is to be established, an opt-in represents a logical step forward.

In line with the liberal standard of international cooperation, in June 2020 EU Member States agreed on interoperability elements being adjusted to their national applications to strengthen the pan-European approach against COVID-19 (EHEALTH NETWORK 2020B, C, D). The implementing *Decision (EU) 2020/1023* in regard to the cross-border exchange of data between national contact tracing and warning mobile applications was adopted by the EC on July 15, 2020 (EC 2020C). The central data controller, which collects the personal date from all EU COVID-19 apps in operation, should become a newly established European Federation Gateway Service (EHEALTH NETWORK 2020B) with national bodies as joint controllers. Once the

system is in operation, the personal data transmitted to the federation gateway are to be stored in a pseudonymised format and should include key identifiers no older than 14 days (IBID.). To prevent a personal data breach, the deletion of personal data in the database should take place once all the participating Member States' servers have downloaded them or 14 days after their reception (IBID.: ANEX III).

In this regard, since the early stages of the pandemic, the attempts to introduce a joint approach among all the EU Member States based on common high standards of privacy and data protection have failed. As of the end of August 2020, 15[12] out of the 27 EU countries have national contact-tracing apps in operation, and four[13] more are working on their development. From among these countries, Austria and the Czech Republic were the first to introduce their national apps in the EU, both using the decentralised system (EC 2020B: 5).

THE DATA COLLECTION-RELATED MEASURES TAKEN IN THE CZECH REPUBLIC TO FIGHT COVID-19

Evaluation of the (il)liberal standards in the country during the first wave of the pandemic

In the Czech Republic, the first patient with COVID-19 was diagnosed on March 1, 2020. The government of the Czech Republic declared the state of emergency 12 days later (VLÁDA ČR 2020A). This step signalled the creation of an environment in which illiberal standards such as data surveillance could be potentially authorized more easily and quickly. Back then, the Czech Republic had evidence of 412 confirmed cases (AKTUÁLNĚ.CZ 2020) and belonged to the first EU countries to implement restrictive measures on travelling abroad (VLÁDA ČR 2020B).

In a form of a *Resolution*, the Government approved the use of geo-location tools to track persons with a demonstrably confirmed COVID-19 infection under Article 9 of the GDPR on March 18, 2020 (VLÁDA ČR 2020C). Under the *Resolution*, the geo-location tracking was originally supposed to be temporally limited by the duration of the state of emergency, which ended on May 17, 2020 (VLÁDA ČR 2020C), while the geo-location apps stayed in use and became a part of the new COVID-19 tracking regime (the "smart quarantine"). The authority responsible for ensuring

the technical as well as legal aspects of the geo-tracking and personal data protection was the Ministry of Health (MoH) (VLÁDA ČR 2020D), as recommended in the *EDPB Guidelines*, and it was supported by the Czech army until May 25, 2020.

Reflection on the privacy and data protection standards in the national covid-19 apps

As an aspect possibly positively contributing to the prevention of illiberal actions, the immediately established public-private partnership needs to be pointed out. Several Czech entrepreneurs, IT specialists and members of academia united to build the COVID19CZ initiative, an informal platform offering the Czech government pro-bono services. Among its other activities, specialists coordinated by 20 companies[14] programmed a custom-tailored technology based on the geo-location principle to control the spread of the virus in the population. Using a decentralised system of data collection, the software also meets the European data protection requirements (COVID19CZ 2020B). In the official manifesto of the COVID19CZ initiative, the members stated that they identify themselves with democratic values and people's privacy, and committed themselves to respect the GDPR. Furthermore, the creators guaranteed that they would transfer all intellectual rights to the developed technology under the MIT licence to the Czech government in 1–3 months to obey the GDPR requirement of one national data controller (IBID.). As the study of Hallinan, Friedewald, and McCarthy (2012) showed, in the EU, private companies are, in general, perceived as less trustworthy than governments concerning data surveillance. Therefore, the COVID19CZ initiative's contribution to the credibility of the app is rather negligible. The outcome of this public-private partnership was the creation of the application "eRouška" (which means "e-FaceMask" in Czech), which then became a fundamental part of the smart quarantine system of the Czech Republic.

The "smart quarantine" (also known as the "intelligent quarantine") is a project created by the Czech Government that was inspired by South Korea and Singapore. The system is based on tracking positively tested people by memory mapping of their recent activities. To help the patient create a memory map, data from a geo-localisation tracking app, such as eRouška, together with data provided by a mobile operator or bank services can be used (ČTK 2020A; MVČR 2020A). The smart quarantine was officially

activated on May 1, 2020, combining the use of personal data with a personal approach. In this system, the person with a confirmed COVID-19 infection is contacted by the responsible authority, namely the MoH, which is represented by the regional hygienic stations (RHS). During the call, the administrative staff of the RHS asks the COVID-19 patient whether he or she agrees with providing the authority with the personal data gathered by the application eRouška, the mobile operator and the bank. Only after being provided with the consent, the RHS receives the personal data, which are then used to create the memory map of the person's recent movement to detect other potentially infected people (IBID.). This procedure is a documented aspect of the liberal approach towards personal data protection of COVID-19-infected people in the Czech Republic.

The eRouška app was designed as a decentralised model of a geo-location contact tracing application. Every user is pseudonymised in the system by an automatically generated unique personal code. Using the Bluetooth technology, the database remembers the location data of other eRouška users the person was in contact with. All the data are stored in the users' mobile phones. Upon giving consent, the user provides the data so far stored in his or her mobile to the RHS. Using this data, the RHS receives the unique personal codes of people who were potentially exposed to the virus while being in close contact (less than 2 metres) for a longer period of time (15+ minutes within 24 hours) with a positively tested patient. These people are then notified by the RHS (EROUŠKA 2020A; EROUŠKA 2020B) and according to the information received, the RHS's personnel evaluates the risk of infection transfer and propose the next steps to take such as testing, quarantine, etc. (IBID.).

To meet the GDPR standards, the information about the data collected and the withdrawal option is available on the website dedicated to the coronavirus run by the MoH (MV ČR 2020A). According to the eRouška application's authors, after the consent is given, the related personal data are available to the respective RHS for 6 hours (IBID., INVESTIGACE.CZ 2020). As was pre-arranged in March 2020, all the intellectual rights were transferred to the official data controller, the MoH, at the end of May 2020 (VESELOVSKÝ 2020), by which another of the *EDPB Guidelines*' recommendations was met.

Interestingly, eRouška is not the only COVID-19 tracking app in the Czech Republic. During the state of emergency, another tracking

software besides eRouška was developed. This software was created by company Seznam.cz introducing a new function to its long-existing maps software "Mapy.cz". To utilise the new function, Mapy.cz users first need to express their consent to the data collection and its storage after the application instalment. For geo-localisation tracking, GMS triangulation is used by this COVID-19 app, which is less accurate than the Bluetooth technology (KUBIÁNOVÁ 2020). The algorithm assesses the data collected and notifies its users if they were in close contact (less than 2 metres for 15+ minutes) with a positively tested person. After being positively tested for COVID-19, the user must provide a second consent in order to provide the data to the RHS. The given consent can be withdrawn directly in the application. Meanwhile, the collected data are stored in the owners' (the private company Seznam a.s.) databank for one month before being deleted (SEZNAM.CZ 2020).

Liberal elements and data protection standards in the communication with the public related to the covid-19 national mobile phone apps

Concerns which appeared about the smart quarantine and both apps' liberal and data protection standards among the public can be divided into two areas. Firstly, there had been only one data controller, the Czech MoH (VLÁDA ČR 2020E), until the government surprisingly decided to create a new governmental body, the Council for Health Risks (CHR), on July 27, 2020. Since July 28, the smart quarantine is run by the CHR, which is represented by the Prime Minister, the Minister of the Interior, the Minister of Health, the Minister of Defence, government proxies for digitisation, science and research, the chairman of the Association of Regions and a representative of the biggest health insurance company. In the inner structures of the CHR, a specialised unit represented by the chief hygienist, representatives of the army and representatives of the MoH (ČTK 2020B; VLÁDA ČR 2020G) was established to control and manage the smart quarantine. In Article 17 of the GDPR, a request to a specified data controller is made, thus the establishment of the CHR is not directly in conflict with the GDPR. Nonetheless the currently disintegrated system in the Czech Republic instigates severe concerns. The more disintegrated the system is, the higher is the probability of data surveillance or cyberattack exposure. Appropriate reasoning for the decision to change the data controller was not provided.

Secondly, the smart quarantine has been criticised for its low utilisation, and thus its low effectivity. According to an Oxford University study, to ensure the proper functionality of the smart quarantine, approximately 60% of the population (which means over 6,000,000 people in the case of the Czech Republic) needs to be active users of the geo-tracking applications (UNIVERSITY OF OXFORD 2020). In August 2020, only approximately 250,000 people have downloaded the eRouška app (MARTINEK 2020) and almost 1,700,000 people allowed the Mapy.cz app to collect their geo-localisation data (SEZNAM.CZ 2020). The Oxford researchers said that when 15% of the population uses the given app, the first positive effects can be observed (UNIVERSITY OF OXFORD 2020), but at least eRouška is very far from meeting this goal.

Furthermore, as the representatives of the government confirmed, in the first three months since their activation, the data collected via the COVID-19 apps, mobile operators and banks have been requested by the RHS's personnel in 615 cases only[15] (MARTINEK 2020), although the number of confirmed COVID-19 cases exceeded 15,000 by that time (MV ČR 2020B). As the smart quarantine's design is dependent on both the total number of users and its utilisation by RHSs, the real numbers indicate that the system has failed so far.

No survey has been conducted among citizens to find out which factors caused the low utilisation. Possibly all the reasons one would normally think of, such as a fear of data breach and surveillance, a lack of awareness, user-unfriendly settings and the apps' prolonged unavailability for iOS users, play a role. One of the characteristics present in illiberal regimes is that people do not trust public authorities enough to provide data to them. Although the data about the Czech population's possible distrust of the COVID-19 apps due to potential data surveillance are not available yet, a warning sign to the Czech government regarding its trustworthiness was made by the electorate.

To respond to the obvious inefficiency, the government announced the launching of the "smart quarantine vol. 2" at the end of summer 2020. Whilst the CHR had high expectations for the improved system, and the Czech MoH started an eRouška promotion campaign to increase the number its users (MARTINEK 2020), the Head of the Czech National Data Protection Authority (NDPA), Ivana Janů, expressed her serious

concerns about the system in the Czech Senate: *"Not only was the smart quarantine project consulted with the official Czech data protection authority only in a limited scope, after its activation and upon request, but all the identified risks of personal data breach have not been eliminated yet [at the end of June 2020], while the preparation for the smart quarantine vol. 2 started. The eRouška app stores personal data and when it receives the user's consent, one but not the only condition for handling the user's personal data is met"* (UOOU 2020). The proposed solution by the Czech NDPA lies in the involvement of the legislative power and a closer cooperation of the government with the NDPA to legitimise further steps (IBID.). If this is not done, serious concerns about the potential governmental intentions regarding the data surveillance might occur.

Summary of the czech response to covid-19 and a reflection on the pan-european approach

To summarise the findings for the Czech Republic in the context of the research questions, first, the Czech geo-localisation apps were both developed under the extraordinary measures of Article 9 of the GDPR during the state of emergency which lasted until May 17, 2020. The apps have remained in operation after that and according to the statement of the Head of the Czech NDPA, their functionality requires improvement to ensure the full protection of personal data guaranteed by the GDPR. The lack of cooperation with the NDPA during the initial phase of the smart quarantine also leaves certain doubts about whether there was a full compliance with the liberal standards as defined. The main difference between Mapy.cz and eRouška lies in the used technology (GMS and Bluetooth) and data storage (the Seznam.cz database and users' mobile phones respectively). The public reaction to their introduction was rather vigilant and distrustful. Only a fragment of the Czech society showed an interest in downloading the apps, which led to a lower utilisation level than that which was needed to start bringing some real benefits. Besides the claimed lack of cooperation between the Czech NDPA and the COVID-19 apps' designers, a deflection from the *EDPB Guidelines* can be also observed in the decision to remove the exclusive responsibility for the smart quarantine's management from the MoH to the CHR at the end of July 2020. The final remark is to be made on the pan-European proposal in the context of the measures implemented in the Czech Republic during the first wave of the pandemic. Despite of the

decentralised model of eRouška, its interoperability with other EU apps for the cross-border exchange of data has not been secured yet.

THE DATA COLLECTION-RELATED MEASURES TAKEN IN AUSTRIA TO FIGHT COVID-19

Evaluation of the (il)liberal standards in the country during the first wave of the pandemic

With 27,000+ cases at the end of August 2020, Austria belonged to the mid-level affected countries in the EU (CORONA TRACKER 2020) during the first wave of the pandemic. Unlike many other states, Austria did not declare a state of emergency during the corona crisis. This supposedly should signify fewer opportunities for the implementation of illiberal standards as authorities had to fully comply with the Austrian constitutional framework (LACHMAYER 2020). The first restrictive measures in Austria were framed as a state of exception based on the historical *Epidemic Diseases Act* from 1950 (IBID.), and two new bills, the first and the second *Covid-19 Law* from March 15, 2020, and March 21, 2020, respectively (ATANASSOV ET AL. 2020: 2–3; EUROPEAN TRAINING AND RESEARCH CENTRE FOR HUMAN RIGHTS AND DEMOCRACY 2020: 2).

As the Austrian *Epidemic Diseases Act* was formulated decades before the digital age's arrival, an additional document extending its authority was released on February 28, 2020. With the *Enforcement of the Epidemic Law*, a document prepared by the Austrian Federal Ministry of Social Affairs, Health, Care and Consumer Protection (known as the *Sozialministerium*), the regional health departments received permission to collect personal data of people positively tested for COVID-19. The data include their address, occupation, social contacts, etc. and are to be used to track individuals potentially exposed to infection. Under this act, the data controller was the national epidemiology unit operating under the Sozialministerium (SOZIALMINISTERIUM AT 2020). Direct references to the data protection regulation can be found in the second *Covid-19 Law*. In its Article 1, the *Telecommunications Act* from 2003 has been changed to allow the Austrian Government to be provided upon request with the customers' data to be used for free warning purposes. The data should be in a form fulfilling the data protection requirements currently in force, which means the GDPR inclusively (PARLIAMENT AT 2020A).

Interestingly, a controversial data transfer with certain characteristics of data surveillance took place in Austria already before the Act was enacted. On March 17, 2020, the biggest Austrian telecom operator, A1, confirmed that it had provided the Austrian Government and the Austrian Red Cross (ARC) with analyses of the aggregate movement of people from March 7, 2020 until March 15, 2020 out of its own initiative. The data of mobile phone owners were analysed to provide the officials with an insight into whether the then recently implemented regulatory measures reducing social contact starting from March 10, 2020, have made a difference or not (DUBMRAVA 2020: 5; IBID.: 10). Supposedly, no customers were informed about A1's intentions in advance (SULZBACHER – AL-YOUSSEF 2020), which represents a deviation, albeit an exceptional one, from the liberal standards. A1 argues that all the data were provided in fully anonymised manner (using a 20-digit code which was changed every 24 hours), and thus the activity represented a Big Data analysis and was in full compliance with the GDPR (IBID.) as well as with the *ePrivacy Directive*. According to Rainer Knyrim, an Austrian lawyer specialised in data protection, as the data were anonymised, no additional consent of users was necessary from the legal perspective (RAINER KNYRIM, QUOTED IN BECHTOLD ET AL. 2020). On the other hand, an Austrian expert on data protection, Christof Tschohl, stated that the case represents an interference into citizens' privacy, despite being understandable in the times of pandemic (SULZBACHER – AL-YOUSSEF 2020). The unveiled affair naturally provoked distrust among the Austrian population (ORF 2020). In a survey conducted by the Vienna Centre for Electoral Research (VCER) at the end of March 2020, over 80% out of 1,541 respondents rejected the idea of people's personal data being collected and further analysed without their knowledge (PARTHEYMÜLLER ET AL. 2020A).

Reflection on the privacy and data protection standards in the national covid-19 app

Like in the Czech Republic, a geo-localisation mobile phone application based on a decentralised model of data collection was developed in Austria. It was Stopp Corona, a contact tracing app run by the ARC on behalf of the Federal Ministry of Health. On March 25, 2020, it became the very first national COVID-19 geo-tracking app in operation to be released in the EU (EC 2020B: 5). The app was developed in cooperation with the private sector as well, namely with the consulting company

Accenture Austria and the Uniqa private foundation, the main shareholder of the private Austrian insurance company of the same name (DAUM – GASSER 2020).

In terms of how it functions, Stopp Corona can be easily described as a combination of both of the Czech apps and ensures a high standard of personal data protection in compliance with the EU legislation. Once users install the app, their consent to the data collection is required. The data are stored in the user's mobile phone for 14 days and protected from potential misuse by two codes, a temporary exposure key (TEK) and a rolling proximity identifier (RPI) (STOPP CORONA 2020A). The application uses Bluetooth technology to collect all RPIs that were present within a short distance (less than 2 metres) from the given mobile phone for a longer period of time (15+ minutes). To ensure an even higher data protection, the RPI code changes every 10 minutes automatically. Should an app user be positively tested for COVID-19, the collected data from the user's mobile phone are with his/her consent provided to the ARC. Other users who came into contact with the infected person within the past 54 hours are notified via the app. For the notification purposes, the personalised TEK data of the infected users together with their RPIs are used. To register in the Stopp Corona app, users are not obliged to provide their mobile phone number. The notification is processed in the application system only. Although further contact details such as the user's phone number can smoothen the notification process and communication, providing them at the time of registration is voluntary (IBID.).

Interestingly, the Austrian application provides users also with a possibility to report a "suspicion of COVID-19 infection". In this case, all users who were in close contact with the person who suspects that he/she is infected are notified as well. Should the person's actual test turn out negative, the user can use the false alarm notification and cancel the original warning notifications. For the false alarm notification, the user needs to provide his/her mobile phone number to the relevant authority to prevent misuse. The consent to store the phone number details can be withdrawn anytime, in which case the body has 30 days to delete the stored data (IBID.). This supports the previous statement of the high data protection standards guaranteed to the Stopp Corona app users.

Liberal elements and data protection standards in the communication with the public related to the covid-19 national mobile phone app

In regard to the communication of data protection standards to the public, the official Stopp Corona app website deserves special attention, as it provides very detailed information on the app's functionality, its operation system, the data collected and the methods of data analysis (STOPP CORONA 2020B). Next to that, the data protection section of the Stopp Corona app website explicitly refers to articles of the GDPR that the app is in compliance with (IBID.). In this regard, the Austrian procedure can serve as a good practice for other countries promoting liberal standards.

However, despite all these efforts, a reluctancy to install the app accompanied the first wave of the COVID-19 pandemic in Austria. With approximately 15% of the population being users of the app, the utilisation remains low, although reaching the minimum level to observe positive effects that was defined by the Oxford researchers (HUBER 2020; JELENKO – BENEDIKT 2020; UNIVERSITY OF OXFORD 2020). In July, the Austrian data protection expert Max Schrems officially confirmed that the ARC's Stopp Corona app meets all the GDPR and *ePrivacy* requirements. Based on his expertise, the concerns about the app among Austrian citizens might have arisen due to its swift introduction in March 2020, shortly after the pandemic outbreak, while in other EU countries COVID-19 apps have not been developed until recently (VIENNA ONLINE 2020).

According to the ARC, what stands behind the low utilisation is perhaps the political debate about people potentially being forced to download the app through illiberal law enforcement, which has negatively resonated within the public society. In another VCER public opinion survey from April 2020, the majority of respondents rejected the idea of obligatory use of the Stopp Corona app (PARTHEYMÜLLER ET AL. 2020B) which would be also in contradiction with the EC *Recommendation* from April 2020. The political debates in Austria about the potential obligation to use the COVID-19 tracking app started in April 2020, as Wolfgang Sobotka, Austria's President of the National Council and former Federal Minister of the Interior, expressed his support for this option (MÜNCH – MUTH 2020). The Austrian Administrative Court reacted to the statement immediately. By declaring the potential obligation to be a disproportionate interference in the fundamental and

data protection rights as well as the freedom of individuals, the Court appealed to the government not to *"override the principles of the rule of law"* (DER STANDARD 2020; SALZBURGER NACHRICHTEN 2020).

Still, especially during the negotiations about the *Amendment of the Epidemic Act 1950*, the opposition parties SPÖ (Sozialdemokratische Partei Österreichs) and FPÖ (Freiheitliche Partei Österreichs) made use of the negative mood in society and repeatedly reopened the discussions to express their concerns about potential app-use enforcement (MARCHART – SCHMID 2020). In the finally approved *Amendment*, unsurprisingly, no illiberal obligations to install the COVID-19 app were enacted (LACHMAYER 2020; PARLIAMENT AT 2020B). A statement confirming that no one can be forced to install a COVID-19 tracking app was also published on the Austrian NDPA's website dedicated to COVID-19 (DATENSCHUTZBEHÖRDE 2020).

Despite the fact that the Austrian government has repeatedly denied all accusations of its having future plans to make the use of the COVID-19 app an obligation, the political debates continued. They especially intensified after the Slovenian parliament approved the obligatory use of a tracking app for those who are verifiably infected or ordered to quarantine, which has set up a potentially dangerous illiberal precedent for other EU states (NOVAK 2020). On July 18, 2020, Susanne Fürst, a member of the Austrian Parliament from FPÖ, addressed a query to the Austrian chancellor Sebastian Kurz. In the text, the answers to eleven questions on the governmental cooperation with US companies on the Stopp-Corona app's development and citizens' monitoring via the app were requested (PARLIAMENT AT 2020C). In his reaction, Sebastian Kurz repeated that the Austrian government does not strive for any kind of monitoring of people, or a nationalisation of collected personal data (PARLIAMENT AT 2020D).

Summary of the Austrian response to covid-19 and a reflection on the pan-European approach

To sum up the findings related to the Austrian measures briefly, as there was no state of emergency declared during the first wave of the pandemic, all the actions undertaken had to strictly comply with the current data protection standards. The exceptional case of the country was further framed by its outdated *Epidemic Diseases Act* from 1950, which required a prompt legislative update to meet the requirements of the contemporary digital

world. Besides the questionable data transfer of the telecommunication operator A1 in March 2020, no data surveillance has been yet observed in the country. The Stopp Corona app, although being the first COVID-19 app in operation among all the EU Member States, seems to provide other countries with a good practice example of a geo-localisation tracking app with high standards of personal data protection, especially due to its double coding (TEK and RPI).

Especially Wolfgang Sobotka's expressed support for making the installation of the COVID-19 app obligatory, and the following prolonged negotiations of the new *Amendment of the Epidemic Act* and intense political debates, contributed to Austria's negative attitude towards the Stopp Corona app, which was not changed even by the high informative standards of its website and the published expert opinions on its data security. Finally, although the app represents a decentralised model of architecture as well and meets other EDPB recommended standards, the interoperability goal has not been achieved yet. The official plan is to incorporate the Stopp Corona app into the pan-European tracking-app architecture by the end of October 2020 (WIESE 2020).

CONCLUSION

the first wave of the COVID-19 pandemic surprised Europe in March 2020, putting political leaders under pressure to swiftly introduce adequate measures to prevent the infection from the spreading, whilst guidelines on how to do so in compliance with, among other things, personal data protection rules and a high respect for privacy, were not then available yet. Situations like this might lead the decision-makers in one of two directions: either choosing the way of strict compliance with liberal and democratic standards or opting for a more authoritarian and oppressive alternative.

Through the two case studies, the article answered the following questions one by one: (1) how and under which circumstances the Czech and Austrian governmental representatives reacted to the spread of COVID-19 infection from the perspective of utilising digital technologies, (2) whether the liberal standards lying in respect for privacy and personal data protection of citizens were maintained and (3) how the data protection standards were communicated to the public and what the level of the app's acceptance and perceived trustworthiness was. The findings show

that in both countries, during the first wave of the pandemic the liberal approach was chosen and mostly maintained, albeit imperfectly. From the perspective of the actions analysed in the given time frame, the rights of citizens were to a wide extent respected.

Regarding the circumstances, in the Czech Republic, both apps were developed and introduced during the state of emergency while the smart quarantine system was activated afterwards. The eRouška app functions represent higher personal data protection standards than those of Mapy.cz, although its utilisation remained lower. This might be caused by its novelty. In contrast to eRouška, the application Mapy.cz had already existed before the pandemic, and its portfolio was only extended by software collecting data and notifying users about possible COVID-19 exposure. Serious concerns about data protection and privacy standards were caused by the lack of cooperation between the government and the Czech DPA during the preparation and initial phase of the smart quarantine, as well as the unprecedented change of the data controller authority in July 2020. Regarding the *EDPB Guidelines* from April 2020 and the agreed interoperability standards from June 2020, the Czech smart quarantine system is built on a decentralised model, which sends a positive message towards Brussels, although the interoperability has not yet been arranged.

The Austrian government did not declare a state of emergency during the first wave of the COVID-19 pandemic. Additionally, the country faced some unusual issues at the beginning of March 2020 due to its outdated *Epidemic Diseases Act* from 1950. Still, one of the country's major achievements was that it became the first EU Member State to put a COVID-19 app into operation. Furthermore, the Stopp Corona app, especially thanks to its double coding (TEK and RPI), was found to ensure high data protection standards. Nevertheless, as the questionable data transfer by A1 was given a lot of publicity, citizens probably became rather sceptical toward the tracking app. Furthermore, the ill-considered statement of a potential obligation to instal the Stopp Corona app supported the Austrians' reluctance to download and use it. The utilisation thus remained low, hardly reaching the minimum of 15% of the population that is required for the app to start bringing some benefits. As the Austrian Stopp Corona app is designed on a decentralised architecture model, hopes for its future interoperability with other EU COVID-19 apps are present, despite this not having been achieved by the end of August 2020.

The last research question reflected on the national implementation of the pan-European approach. Despite the fact that the interoperability standards elements were agreed among EU Member States in June 2020, only a tight majority of the EU countries (15 out of 27 as of the end of August) have national tracing and warning mobile applications in use. Both the Czech and the Austrian apps met the requirements for future interoperability thanks to their decentralised model of data storage, despite the it has not been achieved yet.

One comparative remark can be made in the reflection on different citizens' reactions to the political development around the COVID-19 and national apps' implementation. While in the Czech Republic the establishment of the CHR or the lack of cooperation between the government and the Czech NDPA did not provoke much negativity in the society, in Austria, the debate about potential app-use enforcement resonated significantly among the politicians as well as the public. The long-term cultural and public discourse about data protection and privacy in Austria which has been missing in the Czech Republic could serve as a potential explanation. Data protection and privacy have echoed in the discourse for several years already, as is proven by the quoted and well-known Austrian privacy experts Max Schrems and Christof Tschohl. However, as this assumption is still lacking any scientifically approved evidence, this can be a subject for further research.

ENDNOTES

1 At the end of August 2020, the Czech Republic had evidence of 24,000+ confirmed cases while the corresponding figure for Austria was 27,000+.

2 The World Health Organisation declared the global pandemic of COVID-19 in March 2020. In the Czech Republic and Austria, the governmental representatives started to officially refer to a second wave of the pandemic in September 2020.

3 A reference to such a risk could be found in the famous Warren and Brandeis article published in 1890. Of the many recent authors dealing with this issue, see, for example: Allmer 2011; Bellanova 2006; Bigo – Tsoukala 2008; Cavelty – Leese 2018; Hallinan et al. 2012; Hosein – Altshuller 2017.

4 Snowden's disclosures in 2013 revealed several surveillance programmes operating globally (Zaia 2019).

5 The Cambridge Analytica consultancy company faces accusation of using Facebook users' data to influence the Brexit campaign without the knowledge of the people whose Facebook profile data were data-mined (Naik 2018; Sherr 2018).

6 Users of the fitness application Strava among U.S. active military personnel revealed their deployment through its use in 2018 (Hern 2018).

7 Discriminatory ill-treatment based on predictive policing algorithms and analysis of asylum seekers based on automatic language recognition can be named as two examples of this.

8 The EDBP is an independent body responsible for contributing to the consistent application of data protection rules throughout the EU.

9 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.

10 Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection (2020/C 124 I/01).

11 The EDPB Guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak.

12 Austria, Croatia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Ireland, Italy, Lithuania, Norway, Poland and Spain.

13 Belgium, Malta, Portugal and Slovakia.

14 Seznam.cz, Alza.cz, Keboola, Pale Fire Capital, O2, mluvii, Clevermaps, Česko. Digital, Liftago, Stories.bi, DataSentics, Dateio, Expertkom, Actum, WMC/Grey, Rockaway, Invia.cz, Daktela, Prusa Research, Reservio (COVID19CZ 2020a).

15 As of July 27, 2020 (Martinek 2020).

REFERENCES

A

Aktuálně.cz (2020): Česko přesáhlo hranici tisícovky nakažených. Hasiči rozvezou roušky a další materiál. *Aktuálně.cz*, 22. 3. 2020, <https://zpravy.aktualne.cz/domaci/online-koronavirus-karantena-cesko/r~5ed4192666b311eab115ac1f6b220ee8/>.

Ali, Anwaar – Qadir, Junaid – Rasool, Raihan ur – Sathiaseelan, Arjuna – Zwitter, Andrej – Crowcroft, Jon (2016): Big Data for Development: Applications and Techniques. Big Data Anal, <https://doi.org/10.1186/s41044-016-0002-4>.

Almer, Thomas (2011): Critical Surveillance Studies in the Information Society. *TripleC*, Vol. 9, No. 2, <https://doi.org/10.31269/vol9iss2pp566-592>.

Andrew, Jane – Baker, Max (2019): The General Data Protection Regulation in the Age of Surveillance Capitalism. *Journal of Business Ethics*, Vol. 168, pp. 565–578, <https://doi.org/10.1007/s10551-019-04239-z>.

Atanassov, Nikolai – Dalli, Hubert – Dumbrava, Costica – Eckert, Gianna – Jurviste, Ulla – Radjenovic, Anja – Voronova, Sofija (2020): States of Emergency in Response to the Coronavirus Crisis: Situation in Certain Member States II. European Parliament Research Service, 13. 5. 2020, <https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2020)651914>.

B

Ball, Kirstie – Bellanova, Rocco – Webster, William (2019): Surveillance and Democracy: Sympathies and Antagonisms. In: Ball, Kristie – Webster, William (eds.): *Surveillance and Democracy in Europe*, Routledge Studies in Surveillance, pp. 1–15, <https://doi.org/10.4324/9781315638355-1>.

Bechtold, Franziska – Prenner, Thomas – Dax, Patrick (2020): Ausgangsbeschränkung: A1 liefert Bewegungsdaten an Regierung. 17. 3. 2020, <https://futurezone.at/netzpolitik/ausgangsbeschraenkung-a1-liefert-bewegungsprofile-an-regierung/400783565>.

Bellanova, Rocco – González Fuster, Gloria (2018): No (Big) Data, No Fiction? Thinking Surveillance with/against Netflix. In: Sætnan, Ann Rudinow – Schneider, Ingrid – Green, Nicola (eds.): *The Politics and Policies of Big Data: Big Data Big Brother?* London: Routledge, pp. 227–246.

Bellanova, Rocco – González Fuster, Gloria (2019): Composting and Computing: On Digital Security Compositions. *European Journal of International Security*, Vol. 4, No. 3, pp. 345–365, <https:// doi:10.1017/eis.2019.18>.

Bellanova, Rocco (2017): Digital, Politics, and Algorithms: Governing Digital Data through the Lens of Data Protection. *European Journal of Social Theory*, Vol. 20, No. 3, pp. 329–347, <https://doi.org/10.1177/1368431016679167>.

Berg, Chris (2018): *The Classical Liberal Case for Privacy in a World of Surveillance and Technological Change*. Springer International Publishing, <https://doi.org/10.1007/978-3-319-96583-3>.

Bignami, Francesca (2005): Transgovernmental Networks vs. Democracy: The Case of the European Information Privacy Network. *Michigan Journal of International Law*, Vol. 26, No. 3, pp. 807–868, <SSRN: https://ssrn.com/abstract=1821562>.

Bigo, Didier – Tsoukala, Anastassia (2008): *Terror, Insecurity and Liberty. Illiberal Practices of Liberal Regimes after 9/11.* London: Routledge.

Bradford, Laura – Aboy, Matteo – Liddell, Kathleen (2020): COVID-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR, and Data Protection regimes. *Journal of Law and the Biosciences*, Vol. 7, No. 1, pp. 1–21, <https://academic.oup.com/jlb/article/7/1/lsaa034/5848138>.

Breiner, Josh – Harel, Amos – Landau, Noa (2020): Attorney General Approves Cyber Tech to Track Coronavirus Patients. *HAARETZ*, 15. 3. 2020, <https://www.haaretz.com/israel-news/.premium-israel-to-use-cyber-tech-to-track-coronavirus-patients-1.8675008?=&ts=_1584226332456>.

Budak, Jelena – Damir, Anic – Rajh, Edo (2012): Public Attitudes Towards Surveillance and Privacy in Croatia. *Innovation: The European Journal of Social Science Research*, Vol. 26, No. 1–2, <https:// doi:10.1080/13511610.2013.723404>.

C

Cavelty, Myriam – Leese, Matthias (2018): Politicising Security at the Boundaries: Privacy in Surveillance and Cybersecurity. *European Review of International Studies*, Vol. 5, No. 3, *Special Issue: The Politicisation of Security: Controversy, Mobilisation, Arena Shifting*, pp. 49–69, <https://doi.org/10.3224/eris.v5i3.03>.

Chan, Janet – Bennett MosesIs, Lyria (2015): Big Data Challenging Criminology? *Theoretical Criminology*, Vol. 20, No. 1, pp. 21–39, <https://doi.org/10.1177/1362480615586614>.

Chandler, D. – Fuchs, C. (2019): *Digital Objects, Digital Subjects: Interdisciplinary Perspectives on Capitalism, Labour and Politics in the Age of Big Data*. London: University of Westminster Press.

Cook, Thomas N. (2015): Security, Power, and Digital Privacy. *E-International Relations*, <https://www.e-ir.info/2015/04/30/security-power-and-digital-privacy/>.

Corona Tracker (2020): Austria, <https://www.coronatracker.com/country/austria/>.

COVID19CZ (2020a): Manifest COVID19CZ, <https://covid19cz.cz/covid19-cz/manifest>.

COVID19CZ (2020b): Závazek datové důvěry, <https://covid19cz.cz/covid19-cz/zavazek-datove-duvery>.

Craig, Anthony – Valeriano, Brandon (2018): *Realism and Cyber Conflict: Security in the Digital Age*. Bristol: E-International Relations Publishing.

Criddle, Cristina – Kelion, Leo (2020): Coronavirus Contact-Tracing: World Split between Two Types of App. *BBC*, 7. 5. 2020, <https://www.bbc.com/news/technology-52355028>.

ČTK (2020a): Startuje chytrá karanténa. Co to je a kde ve světě už funguje? *ČTK*, 1. 5. 2020, <https://www.tyden.cz/rubriky/domaci/startuje-chytra-karantena-co-to-je-a-kde-ve-svete-uz-funguje_543015.html>.

ČTK (2020b): Dnes se poprvé sejde vládní rada pro zdravotní rizika. ČTK, 28. 7. 2020, <https://www.ceskenoviny.cz/zpravy/dnes-se-poprve-sejde-vladni-rada-pro-zdravotni-rizika/1916316>.

D

Datenschutzbehörde (2020): Information der Datenschutzbehörde zum Coronavirus (Covid-19), 1. 10. 2020, <https://www.dsb.gv.at/download-links/informationen-zum-coronavirus-covid-19-.html#Frage_13>.

Daum, Matthias – Gasser, Florian (2020): Die Nachbarn sind uns eine App voraus. *Zeit.de*, 31. 5. 2020, <https://www.zeit.de/digital/internet/2020-05/tracing-app-coronavirus-oesterreich-schweiz>.

Davidson, Helen (2020): China's Coronavirus Health Code Apps Raise Concerns over Privacy. *The Guardian*, 1. 4. 2020, <https://www.theguardian.com/world/2020/apr/01/chinas-coronavirus-health-code-apps-raise-concerns-over-privacy>.

de Goede, Marieke (2014): The Politics of Privacy in the Age of Preemptive Security. *International Political Sociology,* Vol. 8, No. 1, pp. 100–104, <https://doi.org/10.1111/ips.12042>.

Deník N (2020): Chytrá karanténa se blíží: Co bude obnášet a jak se změní nouzový stav. *Deník N*, 17. 4. 2020, <https://www.denik.cz/z_domova/chytra-karantena-20200417.html>.

Der Standard (2020): Verwaltungsrichter: App-Pflicht wäre unverhältnismäßiger Eingriff in Grundrechte. *Der Standard*, 13. 4. 2020, <https://www.derstandard.at/story/2000116805190/vfgh-richter-app-pflicht-waere-unverhaeltnismaessiger-eingriff-in-grundrechte>.

Dumbrava, Costica (2020): Tracking Mobile Devices to Fight Coronavirus. *European Parliamentary Research Service*, April 2020, <https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/649384/EPRS_BRI(2020)649384_EN.pdf>.

E

EC (2020a): Commission Recommendation (EU) 2020/518 of April 8 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. *European Commission*, 8. 4. 2020, <https://eur-lex.europa.eu/eli/reco/2020/518/ojhttps://eur-lex.europa.eu/eli/reco/2020/518/oj>.

EC (2020b): Mobile applications to support contact tracing in the EU's fight against COVID-19. *European Commision*, June 2020, <https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_202006progressreport_en.pdf>.

EC (2020c): IMPLEMENTING DECISION (EU) 2020/1023 of July 15 2020 amending Implementing Decision (EU) 2019/1765 as regards the cross-border exchange of data between national contact tracing and warning mobile applications with regard to combatting the COVID-19 pandemic. *European Commission*, 15. 6. 2020, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020D1023&from=EN>.

EC (2020d): Coronavirus: Member States agree on an interoperability solution for mobile tracing and warning apps. *EC Press Corner*, 16. 6. 2020, <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1043>.

EDBP (2020a): Statement on the processing of personal data in the context of the COVID-19 outbreak. *European Data Protection Board*, 16. 6. 2020, <https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_it>.

EDPB (2020b): Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak. *European Data Protection Board*, 20. 4. 2020, <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf>.

eHealth Network (2020a): Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States. *eHealth Network*, 15. 5. 2020, <https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf>.

eHealth Network (2020b): eHealth Network Guidelines to the EU Member States and the European Commission on Interoperability specifications for cross-border transmission chains between approved apps. *eHealth Network*, 12. 6. 2020, <https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_interoperabilityspecs_en.pdf>.

eHealth Network (2020c): Interoperability guidelines for approved contact tracing mobile applications in the EU. *eHealth Network*, 13. 6. 2020, <https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf>.

eHealth Network (2020d): Towards a common approach for the use of anonymised and aggregated mobility data. *eHealth Network*, 30. 6. 2020, <https://ec.europa.eu/health/sites/health/files/ehealth/docs/modelling_mobilitydata_en.pdf>.

ePrivacy Directive (2002): DIRECTIVE 2002/58/EC. ELI, <http://data.europa.eu/eli/dir/2002/58/oj>.

eRouška (2020a): eRouška časté dotazy. *eRouška*, <https://erouska.cz/caste-dotazy>.

eRouška (2020b): eRouška GDPR. *eRouška*, <https://erouska.cz/gdpr>.

EURLEX (2020): Commission Implementing Decision (EU) 2020/1023. *EURLEX*, 15. 6. 2020, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020D1023&from=EN>.

European Training and Research Centre for Human Rights and Democracy (2020): Coronavirus COVID-19 Outbreak in the EU. Fundamental Rights Implications. *European Union Agency for Fundamental Rights*, 23. 3. 2020, <https://fra.europa.eu/sites/default/files/fra_uploads/austria-report-covid-19-april-2020_en_0.pdf>.

F

Fildes, Nic – Espinoza, Javier (2020): Tracking Coronavirus: Big Data and the Challenge to Privacy. *Financial Times*, 8. 4. 2020, <https://www.ft.com/content/7cfad020-78c4-11ea-9840-1b8019d9a987>.

Finnemore, Martha–Hollis, Duncan (2016): Constructing Norms for Global Cybersecurity. *American Journal of International Law*, Vol. 110, No. 3, pp. 425–479, <https://doi.org/10.1017/S0002930000016894>.

Flonk, Danielle – Jachtenfuchs, Markus – Obendiek, Anke (2020): Authority Conflicts in Internet Governance: Liberals vs. Sovereigntists? *Global Constitutionalism*, Vol. 9, No. 2, pp. 364–386, <https://doi.org/10.1017/S2045381720000167>.

Friedewald, Michael – Burgess, Peter J. – Čas, Johann – Bellanova, Rocco – Peissl, Walter (2017): *Surveillance, Privacy and Security: Citizens' Perspectives*. London: Routledge.

Futurezone (2020): Stopp Corona App funktioniert nicht richtig. *Futurezone*, 2. 7. 2020, <https://futurezone.at/apps/stopp-corona-app-funktioniert-auf-iphones-und-android-nicht-richtig/400982240>.

G

GDPR (2016): Regulation (EU) 2016/679, <https://gdpr-info.eu/art-4-gdpr/>.

González Fuster, Gloria – Hildebrandt Mireille (2020): Fundamental Rights More Important Than Ever. *VUB Today*, 9. 4. 2020, <https://today.vub.be/en/article/fundamental-rights-more-important-than-ever>.

Google Play (2020): eRouška. *Google Play*, <https://play.google.com/store/apps/details?id=cz.covid19cz.erouska&showAllReviews=true>.

H

Hallinan, Dara – Friedewald, Michael – McCarthy, Paul (2012): Citizens' Perceptions of Data Protection and Privacy in Europe. *Computer Law & Security Review*, Vol. 28, No. 3, pp. 263–272, <https://doi.org/10.1016/j.clsr.2012.03.005>.

Hern, Alex (2018): Fitness Tracking App Strava Gives Away Location of Secret US Army Bases. *The Guardian*, 28. 1. 2018, <https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases>.

Hosein, Gus – Altshuller, Maria (2017): Privacy and Security in a Digital Age: An Interview with Dr. Gus Hosein. *Harvard International Review*, Vol. 38, No. 3, pp. 67–71.

Huber, Anna Maria (2020): Nur 5 Prozent nutzen „Stopp-Corona-App". *Dolomite Stadt Magazin*, 6. 8. 2020, <https://www.dolomitenstadt.at/2020/08/06/nur-5-prozent-nutzen-stopp-corona-app/>.

I

Investigace.cz (2020): Koronavirus: Strach versus svoboda. *Investigace.cz*, 8. 4. 2020, <https://www.investigace.cz/koronavirus-strach-versus-svoboda/?utm_source=ads&utm_medium=google&utm_campaign=chytra_karantena&utm_source=ads&utm_medium=google&utm_campaign=clanky_temata&gclid=CjwKCAjwmf_4BRABEiwAGhDfScP8SXK_D2GQKomQzBqmKRuKGHdLFI_Up9QgQ2d92dSQYFOTnhEbXhoC_YoQAvD_BwE>.

J

Jelenko-Benedikt, Maria (2020): Stop Corona App von nur 15 Prozent genutzt. *MeinBezirk*, 21. 8. 2020, <https://www.meinbezirk.at/wieden/c-lokales/stop-corona-app-von-nur-15-prozent-genutzt_a4200522>.

K

Körner, Kevin (2019): Digital Politics: AI, Big Data and the Future of Democracy. EU Monitor Digital Economy and Structural Change. *Deutsche Bank Research*.

Kubiánová, Eva (2020): Koronavirus: Lidi mají právo chránit své soukromí i za pandemie. *Investigace.cz*, 10. 4. 2020, <https://www.investigace.cz/koronavirus-lidi-maji-pravo-chranit-sve-soukromi-i-za-pandemie/>.

L

Lachmayer, Konrad (2020): Austria: Rule of Law Lacking in Times of Crisis. The Austrian State of Emergency in the COVID-Crisis. *Verfassungsblog*, 28. 4. 2020, <https://verfassungsblog.de/rule-of-law-lacking-in-times-of-crisis/>.

Lippert, Randy K. – Walby, Kevin (2013): Governing through Privacy: Authoritarian Liberalism, Law, and Privacy Knowledge. *Law, Culture and the Humanities*, Vol. 12, No. 2, <https://doi.org/10.1177/1743872113478530>.

M

Maati, Ahmed – Švedkauskas Žilvinas (2020): Framing the Pandemic and the Rise of the Digital Surveillance State. *Mezinárodní vztahy*, Vol 55, No. 4, pp. 48–71, <https://doi.org/10.32422/mv-cjir.1736>.

Makarychev, Andrey (2020): "Bad Weather" Regionalism and the Post-Liberal International Order at Europe's Margins. *Polity*, Vol. 52, No. 2, <https://doi.org/10.1086/707789>.

Malgieri, Gianclaudio (2020): Data Protection and Research: A Vital Challenge in the Era of COVID-19 Pandemic. *Computer Law & Security Review*, Vol. 37, <https://doi.org/10.1016/j.clsr.2020.105431>.

Marchart, Jan Michael – Schmid, Fabian (2020): Opposition befürchtet weiter „Corona-App"-Pflicht. *Der Standard*, 28. 4. 2020, <https://www.derstandard.de/story/2000117153465/opposition-befuerchtet-weiter-corona-app-pflicht>.

Martinek, Jan (2020): Vojtěch: Trasovat už umíme, podzimu se bát nemusíme. *Novinky.cz*, 31. 7. 2020, <https://www.novinky.cz/koronavirus/clanek/vojtech-trasovat-uz-umime-podzimu-se-bat-nemusime-40332145#seq_no=1&source=hp&dop_ab_variant=390810&dop_req_id=uAkq7rEMB0f-202007311301&dop_source_zone_name=novinky.szn hp.box&utm_campaign=&utm_medium=z-boxiku&utm_source=www.seznam.cz>.

Münch, Peter – Muth, Max (2020): Debatte um Pflicht zu Corona-App-Nutzung. *Süddeutsche Zeitung*, 6. 4. 2020, <https://www.sueddeutsche.de/politik/corona-app-pepp-pt-tracing-oesterreich-deutschland-1.4868497>.

MV ČR (2020a): Chytrá karanténa. *Ministerstvo vnitra ČR*, <https://koronavirus.mzcr.cz/chytra-karantena/>.

MV ČR (2020b): COVID-19: Přehled aktuální situace v ČR. *Ministerstvo vnitra ČR*, <https://onemocneni-aktualne.mzcr.cz/covid-19>.

N

Naik, Ravi (2018): We're Taking on Cambridge Analytica in a Legal Fight for Data Rights. *The Guardian*, 23. 3. 2018, <https://www.theguardian.com/commentisfree/2018/mar/23/suing-cambridge-analytica-data-rights-regulators-silicon-valley-tech>.

Novak, Marja (2020): Slovenian Parliament Endorses Coronavirus Contact Tracking App. *Reuters*, 9. 7. 2020, <https://www.reuters.com/article/us-health-coronavirus-slovenia-app/slovenian-parliament-endorses-coronavirus-contact-tracking-app-idUSKBN24A326>.

O

ORF (2020): Regierung bekommt Handybewegungsdaten. *ORF.at*, 17. 3. 2020, <https://orf.at/stories/3158211/>.

P

Parliament AT (2020a): 16. Bundesgesetz: 2. COVID-19-Gesetz. *Parliament Republik Österreich*, 21. 3. 2020, <https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2020_I_16/BGBLA_2020_I_16.pdfsig>.

Parliament AT (2020b): 43. Bundesgesetz, mit dem das Epidemiegesetz 1950 und das Apothekengesetz geändert werden (16. COVID-19-Gesetz). *Parliament Republik Österreich*, 14. 5. 2020, <https://www.parlament.gv.at/PAKT/VHG/XXVII/A/A_00484/index.shtml>.

Parliament AT (2020c): Anfrage 2378/J. Pflicht zur Nutzung der Stopp-Corona-App für Schulkinder. Schriftliche Anfrage der Abgeordneten Dr. Susanne Fürst, Kolleginnen und Kollegen an den Bundesminister für Bildung, Wissenschaft und Forschung betreffend Pflicht zur Nutzung der Stopp-Corona-App für Schulkinder. *Parliament Republik Österreich*, 18. 6. 2020, <https://www.parlament.gv.at/PAKT/VHG/XXVII/J/J_03010/index.shtml>.

Parliament AT (2020d): Schriftliche Beantwortung (2410/AB) vom 18.08.2020 zu 2378/J (XXVII. GP). *Parliament Republik Österreich*, 18. 8. 2020, <https://www.parlament.gv.at/PAKT/VHG/XXVII/J/J_02378/index.shtml>.

Partheymüller, Julia – Kritzinger, Sylvia – Song, Hyunjin – Plescia, Carolina (2020b): Von Südkorea lernen? Zur Nutzung und Akzeptanz der „Stopp Corona"-App in Österreich. *Austrian Corona Panel Project*, 6. 5. 2020, <https://viecer.univie.ac.at/corona-blog/corona-blog-beitraege/blog31/>.

Partheymüller, Julia – Plescia, Carolina – Kritzinger, Sylvia (2020a): Staatliche Überwachungsmaßnahmen in der Corona-Krise? Was die österreichische Bevölkerung darüber denkt. *Austrian Corona Panel Project*, 4. 4. 2020, <https://viecer.univie.ac.at/coronapanel/corona-blog/corona-blog-beitraege/blog02/>.

Proschofsky, Andreas (2020): „Stopp Corona"-App: Was hat das Rote Kreuz bloß falsch gemacht. *Der Standard*, 11. 7. 2020, <https://www.derstandard.at/story/2000118645764/stopp-corona-app-was-hat-das-rote-kreuz-bloss-falsch>.

R

Reidenberg, Joel R. (2000): Resolving Conflicting International Data Privacy Rules in Cyberspace. *Stanford Law Review*, Vol. 52, No. 5, Symposium: Cyberspace and Privacy: A New Legal Paradigm? <https://doi org/10.2307/1229516>.

Rona, Gabor – Aarons, Lauren (2016): State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace. *8 J.NAT'L SECURITY L. & POL'Y-Cardozo Legal Studies Research Paper No. 503.*

S

Salzburger Nachrichten (2020): Verwaltungsrichter: Corona-App-Pflicht wäre unverhältnismäßig. *Salzburger Nachrichten*, 13. 4. 2020, <https://www.sn.at/politik/innenpolitik/verwaltungsrichter-corona-app-pflicht-waere-unverhaeltnismaessig-86162821>.

Seznam.cz (2020): Mapy.cz: Zastav covid, <https://www.seznam.cz/zastav-covid/>.

Sherr, Ian (2018): Facebook, Cambridge Analytica and Data Mining: What You Need to Know. *Cnet.com*, 18. 4. 2018, <https://www.cnet.com/news/facebook-cambridge-analytica-data-mining-and-trump-what-you-need-to-know/>.

Shklovski, Irina – Mainwaring, Scott D. – Skladttir, Halla Hrund – Borgthorsson, Höskuldur (2014): Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use. *SIGCHI Conference on Human Factors in Computing Systems*, April 2014, <https://doi.org/10.1145/2556288.2557421>.

Solove, Daniel (2011): *Nothing to Hide: The False Tradeoff between Privacy and Security*. New Haven: Yale University Press.

Sozialministerium AT (2020): Erlass, Vollzug des Epidemiegesetzes, Sicherstellung der einheitlichen Vorgangsweise. Geschäftszahl: 2020-0.143.421

Stopp Corona (2020a): Datenschutz. *Roteskreuz.at*, <https://www.roteskreuz.at/datenschutz/>.

Stopp Corona (2020b): DATENSCHUTZINFORMATION STOPP CORONA APP. *Roteskreuz.at*, <https://www.roteskreuz.at/site/faq-app-stopp-corona/datenschutzinformation-zur-stopp-corona-app/#c253467>.

Sulzbacher, Markus – Al-Youssef, Muzayen (2020): Mobilfunker A1 liefert Bewegungsströme von Handynutzern an Regierung. *Der Standard*, 17. 3. 2020, <https://www.derstandard.at/story/2000115828957/mobilfunker-a1-liefert-bewegungsstroeme-von-handynutzern-der-regierung>.

T

TFEU (2012): Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union. 2012/C 326/01, <https://eur-lex.europa.eu/eli/treaty/tfeu_2012/oj>.

U

University of Oxford (2020): Digital Contact Tracing Can Slow or Even Stop Coronavirus Transmission and Ease Us out of Lockdown. *University of Oxford Research*, 16. 4. 2020, <https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown>.

Unver, H. Akin (2017): Digital Challenges to Democracy: Politics of Automation, Attention, and Engagement. *Journal of International Affairs*, Vol. 71, No. 1, pp. 127–146.

UOOU (2020): Ochrana soukromí v době koronavirové a projekt Chytrá karanténa. *UOOU*, 25. 6. 2020, <https://www.uoou.cz/ochrana-soukromi-v-nbsp-dobe-koronavirove-a-nbsp-projekt-chytra-karantena/d-43029>.

V

Van Alsenoy, Brendan (2019): *Data Protection Law in the EU: Roles, Responsibilities and Liability*. Cambridge: Intersentia.

Veselovský, Martin (2020): Chytrá karanténa funguje, udělaly se skvělé věci, hapruje ale testování, říká Doležal. *DVTV*, 28. 7. 2020, <https://video.aktualne.cz/dvtv/chytra-karantena-funguje-udelaly-se-skvele-veci-hapruje-ale/r~e8e84a64d04011ea9c800cc47ab5f122/?fbclid=IwAR2qP-Rw4xK1tmvMC_NHjR5RJcnI40Tw65PWLmY5CUOUkXdSM89fcugFLMk>.

Vienna Online (2020): Datenschützer Max Schrems kann Kritik an Corona-App nicht ganz nachvollziehen. *Vienna Online*, 21. 7. 2020, <https://www.vienna.at/datenschuetzer-max-schrems-kann-kritik-an-corona-app-nicht-ganz-nachvollziehen/6684610>.

Vláda ČR (2020a): Usnesení vlády České republiky o vyhlášení nouzového stavu pro území České republiky z důvodu ohrožení zdraví v souvislosti s prokázáním výskytu koronaviru /označovaný jako SARS CoV-2/ na území České republiky na dobu od 14.00 hodin dne 12. března 2020 na dobu 30 dnů. *Vláda ČR*, 12. 3. 2020, <https://apps.odok.cz/attachment/-/down/IHOABMNHPBSV>.

Vláda ČR (2020b): USNESENÍ VLÁDY ČESKÉ REPUBLIKY ze dne 12. března 2020 č. 197 o dočasném znovuzavedení ochrany vnitřních hranic České republiky. *Vláda ČR*, 12. 3. 2020, <https://apps.odok.cz/attachment/-/down/IHOABMNHPHXW>.

Vláda ČR (2020c): Epidemie koronaviru. *Vláda ČR*, <https://www.vlada.cz/cz/epidemie-koronaviru/dulezite-informace/mimoradna-opatreni-_-co-aktualne-plati-180234/>.

Vláda ČR (2020d): USNESENÍ VLÁDY ČESKÉ REPUBLIKY ze dne 18. března 2020 č. 250 k zajištění zvýšené ochrany obyvatel – trasování. *Vláda ČR*, 18. 3. 2020, <https://apps.odok.cz/attachment/-/down/IHOABMTJPDJA>.

Vláda ČR (2020e): Poprvé jednala Rada vlády pro zdravotní rizika, hlavním úkolem je další vylepšování Chytré karantény. *Vláda ČR*, 27. 8. 2020, <https://www.vlada.cz/cz/media-centrum/aktualne/poprve-jednala-rada-vlady-pro-zdravotni-rizika---hlavnim-ukolem-je-dalsi-vylepsovani-chytre-karanteny-182870/>.

Vláda ČR (2020e): Rada vlády pro zdravotní rizika. *Vláda ČR*, 27. 8. 2020, <https://www.vlada.cz/cz/ppov/rada_vlady_pro_zdravotni_rizika/uvodni-text-rada-vlady-pro-zdravotni-rizika-183146/>.

W

Warren, Samuel D. – Brandeis, Louis D. (1890): The Right to Privacy. *Harvard Law Review,* Vol. 4, No. 5, pp. 193–220.

Wiese Jana (2020): Bilanz nach einem halben Jahr „Stopp Corona"-App. *ORF.at*, 10. 10. 2020, <https://help.orf.at/stories/3202229/>.

Worldometers (2020): Coronavirus Cases. *Worldometers*, <https://www.worldometers.info/coronavirus/#countries>.

Z

Zaia, Mathew (2019): Exploring Consciousness: The Online Community's Understanding of Mobile Technology Surveillance. *Surveillance & Society*, Vol. 17, No. 3/4, pp. 533–549, <https://doi.org/10.24908/ss.v17i3/4.11934>.

Zwitter, Andrej – Gstrein, Oskar J. (2020): Big Data, Privacy and COVID-19 – Learning from Humanitarian Expertise in Data Protection. *Journal of International Humanitarian Action*, Vol. 5, No. 4, <https://doi.org/10.1186/s41018-020-00072-6>.

NOTE

This paper was elaborated within the IGA Project "Disintegration Risks for the European Union" No. F2/55/2020.

AUTHOR BIOGRAPHY

Jana Stehlíková is a PhD candidate in International Political Relations at the Faculty of International Relations, the Prague University of Economics and Business. She specialises in EU affairs, digital agenda and digital technologies' impact on international relations, especially focusing on personal data protection, e-diplomacy, online platforms and disinformation in the European Union.