DATA PROTECTION VS USING EMERGING TECHNOLOGIES: HOW TO FIGHT AGAINST COVID-19 WHILE STAYING LEGALLY COMPLIANT?

Szilvia Váradi
senior lecturer, University of Szeged, Faculty of Law and Political Sciences,
Department of International and European Law
H- 6721 Bocskai u. 10-12., Szeged, Hungary, e-mail: varadiszilvia@juris.u-szeged.hu

Abstract

The pandemic situation caused by the SARS-CoV-2 virus has changed our lives significantly. Recent research has shown that seeking competent and advanced technological solutions to combat the COVID-19 pandemic is crucial to address not only this pandemic situation, but similar epidemics and pandemics in the future as well. However, the legal compliance of their application especially with European data protection legislation can be challenging. In this work, we would like to highlight the relevant data protection provisions of the Council of Europe and the European Union, which should be borne in mind while using digital solutions to fight against the pandemic. In the second part of our paper, we will analyse the main challenges of the three most frequently used emerging technologies from data protection point of view. As a result of our research, we can state that the main problem is to meet the requirement of data minimisation. In case the source data is not accurate, the results might be ineffective, unreliable or it may lead to data breaches. Therefore, to solve this paradox, we emphasize the importance of the data protection by design approach.

Keywords: *Data protection, COVID-19, emerging technologies, mobile applications, artificial intelligence, drones, Genera Data Protection Regulation*

1. Introduction

In December 2019, the SARS-CoV-2, which is a new type of coronavirus, was reported first in Wuhan, China. Since then, the infection caused by this virus referred as COVID-19, spread throughout China and all around the world in several waves. The speciality of COVID-19 is that it is spreading rapidly, and the human body responds to it differently from no symptoms (asymptomatic) to severe pneumonia, and a severe disease can lead to death (ECDC, 2020). Besides, it can cause unexpected and unusual symptoms as well. With mutations especially the Delta and the newly identified Delta Plus variants raise the prospect that the fight against COVID-19 and the pandemic situation in the world is far from ending.

Recent research has shown that seeking competent and advanced technological solutions to combat COVID-19 pandemic is crucial, in order to address not only this pandemic situation, but similar epidemics and pandemics in the future as well. Otherwise, we could face an unmanageable crisis (Vaishya et.al, 2020).

In addition, in specific circumstances created by a pandemic, processing personal data is inevitable to introduce appropriate measures to stop the spread of the infection, and to prevent or minimise its impacts. These personal data in question can vary from the "general" types, such as name, address, workplace, other location data or travel information of data subject, which can be useful to discover, whether an individual might have visited affected areas or met with infected people. But the processing of special categories of personal data with sensitive nature such as health data (including test results, body temperature, chronic diseases, symptoms, etc.) are also essential to obtain an early indication, whether an individual is infected or not.

The application of emerging technologies facing the pandemic is a hot topic worldwide, even the Department of Economic and Social Affairs of the United Nations deals with the impact of using such technologies. However, in this work we focus on the three most frequently used technologies combating COVID-19, the application of which raise the most problematic and complex data protection implications under the European data protection regime.

2. The context of data protection

During the pandemic, digital technologies are used even more widely in public places to monitor the population and at individuals' home, while performing online learning, home officing or self-diagnosing. In the frame of the COVID-19 pandemic situation, the Member States should activate their emergency plans (WHO, 2020) and conduct administrative procedures or apply contact tracing, which is an effective disease control strategy that involves identifying infected persons and their contacts, then cooperating with them to interrupt disease transmission.

Since emergency measures have been adopted that have affected the right to privacy and data protection, in this work we plan to elaborate the relevance of our topic from data protection point of view.

Both the Council of Europe (CoE Joint Statement, 2020) and from the side of the EU (the European Data Protection Board and the European Data Protection Supervisor (EDPB, 2020a; Wiewiórowski, 2020), it was stressed out that data protection cannot be an obstacle for saving lives and that the applicable principles always allow for a balancing of the interests at stake. On the other hand, the European Data Protection Board (EDPB) stated that there is no need to lift the provisions of the General Data Protection Regulation (GDPR), just to observe them (EDPB response, 2020), and it is crucial to maintain the level of the protection guaranteed by the GDPR in each Member State during the pandemic. The key question is how the right to protection of personal data can be uphold, while contributing effective pandemic response using new digital solutions.

2.1. The Council of Europe

The Council of Europe (CoE) emphasized the importance of technology to find a way out of the current situation and that the principles of necessity, proportionality and non-discrimination must be kept in mind by using these digital tools. From the aspect of protection of fundamental rights, the CoE stated that alternatives to the application of such digital technologies need to be made available, and that their use should be optional with a temporary nature and form part of a comprehensive and coherent health strategy.

The CoE divided two main fields regarding the use of technologies. One of them is to set up a system enabling to store and provide health-related data on COVID-19. As an example, the administration of national systems monitoring vaccination can be mentioned. Usually, central databases should be avoided in order to minimise the amount of centrally stored personal data, and decentralised solutions (e.g. storage by vaccination centres or local health authorities) should be applied where possible. There are some obligations for data controllers to ensure fair and transparent data processing in the frame of these systems, such as to carry out an impact assessment to prevent and minimise risks to data subjects' fundamental rights and freedoms, and to guarantee data security with the respect of the data protection by design principle (CoE Statement, 2021). The CoE underlined the importance of purpose limitation, accuracy and data minimisation, which are the same principles relating to processing of personal data laid down in Article 5 of the GDPR. Besides, storage periods of personal data should be limited in time in these systems as well.

The other area according to the CoE is to create information systems to monitor the vaccination campaigns or for the attestation of immunity to COVID-19, such as a vaccine one has received, negative test results or past infections (CoE Statement, 2021). Based on these data, health or green pass, vaccine passport or digital health certificate were launched by the states. The European Union has introduced the EU Digital COVID Certificate, which is available from July 1st, 2021, and will act as a COVID pass for European citizens and residents. It is important to emphasize that these attestation systems must be provided by law, which also precisely specifies the circumstances, in which the attestation can be demanded. The data processing must be appropriate to ensure the attainment of the objective pursued and not to go beyond what is necessary for its attainment. Furthermore, the grant of access rights to the databases should be properly clarified.

Mobile applications are being intensively used for presenting the attestation, where unique identifiers such as barcodes or QR (Quick Response) codes can also provide means of tracing users, therefore data protection principles must be respected in all such tools. Decentralised solutions, especially storage of data on users' mobile devices, should be preferred in this context.

It is crucial by using new technologies that data subjects can exercise their rights and that data protection authorities can effectively monitor the compliance with data protection provisions. We can state that the knowledge about COVID-19 is increasing. But the main issues at present are the effects of vaccination and the duration of immunity of people which also require that particular care must be given to that the collected personal data are accurate and regularly updated.

The Data Protection Unit of the CoE prepared a detailed report about the data protection aspects of technical solutions, in which the application of the following principles and requirements were underlined:

- limited retention period of all collected personal data,
- the principle of purpose limitation,
- proportionality considering the effective results of the applied measures,
- cooperation with the national data protection authority,
- transparency and explainability of the data processing activities,
- accountability of data controllers (CoE Report, 2020).

The above-mentioned principles and aspects are also the main substantives of the General Data Protection Regulation of the European Union.

2.2. The European Union

As we mentioned before, it is crucial to maintain the level of the protection guaranteed by the GDPR in each Member State during the pandemic. Therefore, data controllers must follow the basic principles contained in Article 5 of the GDPR.

One of these principles is that personal data should be processed lawfully, which means the data controllers' obligation to rely on a legal basis contained in the GDPR. Regardless of the types of personal data, this requirement remains essential to guarantee the lawfulness of processing operations.

In our view, for processing “general” types of personal data (e.g, name, date of birth, contact information, etc.) the consent of the data subject is not always the best option, especially in a pandemic situation. This category of personal data can be processed in accordance with Article 6 (1) d), when it is necessary *to protect the vital interest of individuals* (i.e., to save the life of the data subject), or under Article 6 (1) e) *to protect public interest* or *in the exercise of official authority* vested in the controller. Recital 46 of the GDPR explicitly refers to the monitoring of epidemics and their spread as circumstances, in which the processing may serve both important grounds of public interest and the vital interest of data subjects.

In addition to the above, if the processing is necessary for compliance with *a legal obligation*, which the controller is subject to, Article 6 (1) c) also can be relied upon. According to Article 6 (3) of the GDPR, both public interest and legal obligation can only be determined by the law of the European Union or of a Member State, which the controller is subject to.

It is important to emphasize that personal data concerning health require higher protection due to their sensitive nature, and they belong to sub-categories of personal data, which are called the special categories of personal data. The processing of these kind of data is generally not allowed by the Article 9 (1) of the GDPR, unless at least one of the ten conditions of the possible exemptions under Article 9 (2) is met.

Under the Article 9 (2) a) of the GDPR, one of the possible legal bases for processing special categories of personal data, such as data concerning health is the *explicit consent* (Váradi, 2021) of the data subject. We emphasize that under the Recital 43 of the GDPR, a consent cannot be regarded as a valid lawful legal basis in those cases, when there is an imbalance of power between the data subject and the controller. According to the EDPB, this is clearly an issue in the study of the critically ill, where patients might be especially vulnerable and there might be a stark imbalance of power between the investigator and patient providing the data (EDPB Opinion 3/2019). Besides, some research suggests that while conducting epidemiological investigations, researchers did not always obtain the explicit consent of the data subjects (Ahn et.al. 2020).

Therefore, data controllers are suggested to seek to rely on either public or legitimate interests as legal basis, and only relying on the consent of the data subject, when it can be obtained in line with the legal requirements laid down in the GDPR, and the withdrawal of the consent will not adversely affect the proposed use of the data.

According to Recital 52 of the GDPR, a derogation is allowed for processing special categories of personal data *on the ground of the public interest*, in particular processing personal data for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health. The Recital 54 of the GDPR states that the processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without the consent of the data subject. Based on this provision, it can be stated that the public safety requires the “right to know” about the patients’ personal data regarding e.g. the status of infection (Ahn. et.al., 2020). This ground applies, if the processing is necessary to protect the population against a serious cross-border threat to health such as COVID-19 pandemic, or ensuring high quality standards and safety of healthcare, medicinal products or medical devices.

In order to decide, which one from the above-mentioned legal grounds will be the appropriate to the specified processing, an analysis has to be made on a case-by-case basis.

There is another legal option which can be used in the fight against COVID-19 as well. Under Article 23 of the GDPR with a legislative measure, EU law or national laws of the Members States can restrict the scope of the rights of data subjects and some of the obligations of the data controllers, while respecting the essence of the fundamental rights and freedoms, and if it is a necessary and proportionate measure in a democratic society to safeguard "*other important objectives of general public interest of the Union or of a Member State, in particular (...) public health (...).*" These restrictive legislative measures are only applicable for the limitation of the scope of data subjects' rights specified clearly by Article 23 (1) of the GDPR. These rights are also related to the data controllers, because their obligation is to ensure them. It is important to underline that those rights and obligations, which are not covered by Article 23, cannot be restricted. The restrictions should be foreseeable to persons subject to them, precisely limited in time (EDPB 2020.b.). On these grounds, safeguarding public health in emergency state is a reasonable and legally sound reason, but only accompanied by the above-mentioned conditions.

Concerning the safeguards to prevent abuse or unlawful access or transfer, since it is the obligation of the data controllers to guarantee the security of personal data, organisational and/or technical measures are suggested in the context of restricting measures as well (EDPB Guidelines 10/2020). These actions can cover in particular the so-called pseudonymisation and encryption of personal data, or the application of data protection by design and by default. For these technical solutions and organisational measures, it should be emphasized that their effectiveness needs to be regularly tested, assessed and evaluated, in order to ensure the security of the processed data.

After we examined the relevant legal provisions using digital solutions from data protection point of view in the European dimension, in the following section we will give an overview about the most frequently used technologies fighting against COVID-19 pandemic.

3. Most common technologies to fight against COVID-19

In this section, we have chosen three technical solutions for our analysis based on the frequency of their application in Europe, in order to show their features and impact on the personal data of individuals.

3.1. Mobile applications

In the previous section we mentioned the use of mobile applications, which can be considered as the main technology used by data controllers such as governments of the Member States and private companies (Bradford et al., 2020). They can be used by high-speed network, and help to track strategic locations, infected people and to model disease outcomes. Therefore, the purpose of these governmental or private applications can vary from contact tracing to medical reporting (e.g. in Italy), to send alert to the population (e.g. in Switzerland), to quarantine enforcement (e.g. in Hungary). The main technologies for proximity tracing are Bluetooth and global positioning system (Khemasuwan et.al., 2021), and the software of mobile phones and mobile applications may apply Artificial Intelligence methods or algorithms, therefore, it is also possible to combine them with other new technologies. The main challenge related to mobile applications is to fulfil the data minimisation principle, since a lot of identifiers of the individuals, such as location data, health data, can be collected by these applications combined with other smart devices as well.

In the case of contact tracing, the Member States are obliged to inform data subjects about the processing of their health data and about the right of access to their own personal data. Besides, procedures should be laid down to enable data subjects to request rectification or deletion of their personal data (van Kolfschooten et al., 2020). The use of mobile applications should be voluntary, the applications must be privacy preserving and can be dismantled as soon as no longer needed, which are considered the essential requirements for these technologies (Cristani, 2021).

In 2020, only Norway, Italy, Belgium, France and Finland accepted a specific legislation on using mobile apps for contact tracing purpose (FRA, 2020). In the EU Member States, traffic and location data were collected from mobile apps or mobile phones, and from social media and mobile network operators to reveal patterns and trends in social mobility and help forecasting the spread of the virus. These data were aggregated and anonymised data, which apparently fulfil the requirement of the compliance with European data protection provisions. However, the irreversibility of anonymisation and potential third-party access to the data has been compromised in Germany and Denmark (FRA, 2020).

The data protection authority required suspension of Smittestopp, which is the contact-tracing application in Norway. On one hand, only the 14 % of the population downloaded it (EDPB website, 2020) and this low number has an impact of effectiveness of the app, there were no solution for anonymizing and aggregating data for analysis. Besides, the app collected large quantities of personal data about app users, including continuous location data and information about app users' contact with others. Based on these concerns, the national authority decided to stop the collection of personal data, and to erase the collected data and requested to update the Smittestopp app with its supervision (EDPB website, 2020).

To sum up, the efficiency of app-mediated contact tracing depends on the level of population uptake, its ability to accurately detect infectious contacts, and the extent of adherence to self-isolation by notified contacts.

3.2. Artificial Intelligence

A Canadian health monitoring platform named BlueDot using Artificial Intelligence (AI) technology (AI HLEG, 2019) was the first who sent warning to its customers about the flu-like outbreak in Wuhan on 31 December 2019, while the US Centers for Disease Control and Prevention sent a notification on 6 January 2020. Despite the World Health Organization (WHO) received a report about the virus on 31 December 2019, its first notification to the public was delivered on 9 January 2020, and it declared the outbreak a "public health emergency of international concern" only on 20 January 2020. Big data plays an important role in the BlueDot application, as it uses foreign-language news reports, animal and plant disease networks, official proclamations as sources for their algorithms and has access to global airline ticketing data. Based on this information, its algorithms can predict which parts of the world are or will be danger zones and suggested for their clients to be avoid in advance (Niiler, 2020). In this case, AI-enabled early warning systems have been used by scientists to forecast on outbreaks and predict the spread of the virus. Furthermore, AI solutions are used for digital contact tracing combined with the outbreak detection approach as well (Khemasuwan et.al., 2021).

Another area of the application of AI is medical detection and diagnosis, since the early prediction and treatment of COVID-19 are crucial to combat against pandemic. The clinical features of COVID-19 are sometimes indistinguishable from other viral infections, therefore, there is a great effort to train AI algorithms to detect visual signs of COVID-19 on images from CT or X-ray lung scans. However, the accuracy, reliability and consistency of the results of AI algorithms depend on the available datasets, geography and specification of imaging. Imaging alone cannot be used solely to diagnose COVID-19, but AI solutions can provide clinical support systems for clinicians, particularly to help clarifying or confirming suspicious cases. Furthermore, AI solutions can help biomedical research as vast amount of biomedical data can be processed by AI algorithms to analyse genomic sequences or to contribute to drug or vaccine development (Abd El et. al., 2021).

These approaches involve health records of individuals, therefore, it is essential to ensure compliance with data protection provisions, which may encounter some difficulties. As AI algorithms use vast amount of data and large datasets, the principle of data minimisation can be particularly challenging, and because of the complex operation of these algorithms, transparency as well. In our opinion, to fulfil the requirements of data minimisation, the disclosure of the identity of an infected person is not necessary in most cases, while in a specific case the use of AI algorithm can help in the diagnosis.

To avoid data breaches, the European Parliament suggested that high-risk AI technologies, such as those with self-learning capacities, should be designed to allow for human oversight at any time. If a functionality is used that would result in a serious breach of ethical principles and could be dangerous, the self-learning capacities should be disabled and full human control should be restored (European Parliament, 2021).

In our opinion, the proper application of the basic principle of data security, especially data protection by design, would be preferable. This latter was also emphasized by the EDPB in the draft of the European legislation on AI, and it was recommended that the data protection compliance should be a precondition for AI systems to enter the European common market as CE marked product. To achieve this compliance by third parties, adaption of prior conformity assessment can be necessary (EDPB – EDPS, 2021).

While service providers have the obligation to perform initial assessment with a general nature, it is not always possible for them to assess all uses for the AI system. Therefore, the user of the system should also be able to conduct subsequent assessment the so-called data protection impact assessment (DPIA) considering the context of use and the specific use cases (EDPB-EDPS, 2021). The EDPB and EDPS recommended a ban, for both public authorities and private entities, on AI systems categorizing individuals from biometrics (for instance, from face recognition) into clusters according to ethnicity, gender, as well as political or sexual orientation, or other grounds for discrimination. But at this point it is important to emphasize that the pandemic is a special and extraordinary situation, where exceptions can be made with strict safeguards regarding data protection.

Although AI has the potential to be a tool in the fight against COVID-19 and similar pandemics, AI systems are still at a preliminary stage according to some experts (Bullock et al., 2020). In combatting the pandemic, it is essential to gather and analyse big data promptly, even if it may require that the authorities collect more personal data (Naudé, 2020). The extensive use of AI may lead to increased productivity, but it will also raise the requirements (in terms of infrastructure and qualification) to benefit from it, thus leading to a net increase in inequalities (Naudé et al., 2021).

3.3. Drones

During the pandemic, drones are used worldwide to spray disinfectant, monitor traffic, conduct aerial thermal sensing, deliver food and medicine in quarantined districts. Some Member States were using drones as well to monitor compliance with physical distancing measures in public spaces, others used thermal cameras to measure people’s temperatures, particularly at work (FRA, 2020). Police have been using drones with thermal sensors, night-vision cameras, high-definition zoom lenses to enforce movement restrictions in Belgium, Bulgaria, France, Greece, Lithuania, Spain, United Kingdom. Drones can help to reduce human contacts, as there is no need to apply human resources (health workers, officers) during the operation on the infected area. Moreover, the drone's software is being rewritten by state agencies and drone manufacturers to adapt to the new functions and to enforce restrictive measures. And there are some projects which combine drones with AI software, therefore, they can perceive their surroundings, which enables them to map areas, track objects and provide analytical feedback in real-time (Daley, 2020).

From the data protection point of view, the use of drones can increase the identification of individuals, affect people's right to privacy and anonymity. The problem is that drones usually collect vast amount and different types of personal data during systematic and generalised monitoring, their data processing system is fully automated with the capability of data stockholding, and they can do all these from a long distance far beyond human capabilities (Pusztahelyi, 2019).

Since informed consent is usually missing, the legal basis for data processing should be chosen carefully. In the context of a pandemic, for public authorities Article 6 and Article 9 of the GDPR allow for processing of personal data for reasons of public interest in public health, such as protecting against serious cross-border threats to health. And despite these above-mentioned features of drones, public authorities are suggested to avoid systematic and generalised monitoring and collection of health data and anonymous data should be used where it is possible. If it is not feasible, Article 15 of the ePrivacy Directive enables the Member States to introduce legislative measures temporarily pursuing national security and public security with appropriate safeguards to protect personal data (European Parliament, 2021). There were some problematic cases on the use of drones, as well. For example, in Greece, the accepted legislation on the use of drones did not contain explicitly data protection provisions. In France, there were no legal framework for the use of drones over Paris to monitor people’s movement during the lock-down period (CoE report, 2020).

To avoid data breaches, it is suggested to minimise the capture of images to those absolutely necessary. It is crucial to prevent the storage of irrelevant information relating to natural persons, and to apply techniques for the anonymization of images. In parallel, fixed retention period should be laid down when the storage of the collected data is necessary. Another solution can be from the technical point of view, if flights are performed at times where there are not large concentrations of people or when access to the flight zone can be restricted. In our opinion, to allow human oversight over the operation of drones and the collected data would be another best practice.

Finally, it is important to bear in mind that many of the exceptional measures controlling the use of drones are based on extraordinary powers and only to be used temporarily in emergencies. Therefore, specific safeguards need to be introduced so that full protections are afforded to personal data once the state of emergency is lifted.

4. Possible solutions for data security

When using different digital tools, there are some common solutions, which can be applied to guarantee the security of personal data. Regarding the processing of health-related data by public authorities, relevant recommendations have been issued by the Council of Europe. It has been stressed that communications to the public by health and government authorities should remain a priority, in order to protect, inform and advise the public. Nonetheless, during such communications, the publication of sensitive data (such as health-related data) of specific individuals should be avoided, and it is recommended that the processing of such data can only be performed, if additional technical and organisational measures complementing those applied to non-sensitive data are put in place.

Under Article 4 (5) of the GDPR of the EU, one of the potential solutions to ensure data security is pseudonymisation, which means the removal of data that allow for the identification of a person and their substitution by other identifiers, such as a random code, which does not directly relate to that person. Pseudonymised data are still considered personal data, if the data subject could be identified upon them combined with other information, therefore the data protection provisions remain applicable. However, the GDPR should not be applied to anonymous information, when such identification is not possible, and the pseudonymised data are no longer relate to an identified or identifiable natural person. According to the EDPB, data cannot be anonymised on their own, only whole datasets may be made anonymous. Based on the Guidelines of the EDPB, any intervention on a single data should be deemed as pseudonymisation (EDPB Guidelines 4/2020).

Recently, anonymisation processes and re-identification attacks are active fields of research. It is suggested for any controller using anonymisation solutions to follow recent developments in this field, especially concerning location data, which are known to be hard to anonymise. Indeed, a large amount of research has shown that location data thought to be anonymised may in fact not be. Mobility traces of individuals are inherently highly correlated and unique. Therefore, they can be vulnerable to re-identification attempts under certain circumstances (EDPB Guidelines 4/2020).

The de-identification solutions as pseudonymisation can be suitable answers to the privacy concerns, especially for data processing without a valid consent of the data subject. However, some experts have proved that there are re-identification methods usually combined with AI algorithms which can accurately estimate the likelihood of a specific person using 15 demographic attributes in any dataset (Rocher et.al., 2019).

In the context of medical research, conditions for third party access should be established. Any personal information provided to a third party should be made available in the form of non-identifying numbers or symbols. In case a third party need to use identified personal information, they should require personal consent. Researchers should design an operating system for personal privacy. Google and Apple recently released a tracking system with privacy features. Other scholars also introduced systems that encrypt data to ensure the protection of personal data in applications. These options offer additional safeguards for ensuring personal privacy.

5. Conclusions

In this paper we investigated a complex problem regarding the COVID-19 pandemic: how emerging technologies can be applied to fight against the coronavirus with maintaining the highest standards of data protection required by the European legislation at the same time.

In order to identify potential responses, we analysed the relevant legal provisions and principles in the context of two European organisations, namely the Council of Europe and the European Union. On these grounds we can state that the Council of Europe confirmed the importance of the same basic principles of data protection while processing personal data with digital solutions, which are the main pillars of the General Data Protection Regulation of the EU. These are the following: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; accountability of the controller. Regarding lawful data processing, we found that in most cases the consent is not an appropriate legal basis for the purposes of processing data under GDPR. Instead, especially in the context of the pandemic, the application of Article 9 (2) (i) of the GDPR is recommended, which allows the data processing on the ground of reasons of public interest regarding public health, based on the law of the Member States. Besides, in special circumstances such as a pandemic situation, Member States can accept restrictive legal measures, but the level of protection of personal data and their security must be maintained and guaranteed.

Regarding emerging technologies, it can be considered that they can provide extensive assistance to deal with medical and non-medical aspects of COVID-19, while using large amounts of data including personal data, which can come at a price from the data protection point of view. The compliance with the basic data protection principles can be challenging, especially with the data minimisation principle. All technologies analysed in this paper require vast amount and accurate data to operate in an efficient and useful way, therefore both quality and quantity of data are essential. If the source data is not accurate, the results might be unreliable, discriminative or it may lead to data breaches. Therefore, the data minimisation principle can lead to a paradox situation in the case of these technologies. While large datasets with personal data can help to improve the results of the technical solutions, the risks of the use of such data should ideally be mitigated through dedicated legal frameworks, in which the purpose and objectives of data processing, its collection, analysis, storage and sharing, as well as the erasure of data are laid down.

However, we believe that data protection has to be weighed against respective benefits and risks to strike a balance between them, applying the necessity and proportionality test. Different technologies can be combined with each other by using usually big datasets, therefore, it is crucial to treat them with necessary care and diligence.

General, unified methods cannot be found for all technologies, because depending on the purpose of the field of use, every software is different. Relying on the data protection by design principle can be a real solution for all challenges, where the data protection aspects should be built in the technologies at the very first stage of their development. In our opinion, the development of these technologies should be a teamwork: interdisciplinary cooperation is needed between software engineers, lawyers, economists and other experts to apply data protection friendly solutions. This cooperative work can achieve a balance between technological innovation and privacy considerations.

Considering the ethics of technology and solving the privacy challenges will be essential to the long-term success of emerging technologies. In the light of the above, we share the view that care should be taken in choosing the relevant and more fitting technical solution, and focusing not only on the fight against the virus, but on the need to preserve the protection of personal data as well. In this way, we can exploit the opportunities of new technologies in the most sufficient and appropriate way.

6. Acknowledgement

This research was supported by the EU-funded Hungarian grant EFOP-3.6.1-16-2016-00008.

References

[1] European Centre for Disease Prevention and Control (ECDC). (2020, March 25). *Coronavirus disease 2019 (COVID-19) pandemic: increased transmission in the EU/EEA and the UK*. (7th ed., pp. 1-31.) Stockholm. **https://doi.org/10.2807/1560-7917.ES.2020.25.12.2003261**

[2] Vaishya, R., Haleem, A., Vaish, A., Javaid, M. (2020). Emerging Technologies to Combat the COVID-19 Pandemic. *Journal of Clinical and Experimental Hepatology*, 10(4), 409-411. **https://doi.org/10.1016/j.jceh.2020.04.019**

[3] *WHO Director-General's opening remarks at the media briefing on COVID-19*, (5 March 2020). https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-mediabriefing-on-covid-19-5-march-2020

[4] *Joint Statement on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter,*

Data Protection Commissioner of the Council of Europe. (2020, 3March 30). Strasbourg. https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter

[5] European Data Protection Board (EDPB). *Statement on the processing of personal data in the context of the COVID-19 outbreak.* (2020, March 19). (2020.a.)

[6] Wiewiórowski, W. (2020, April 6). *EU Digital Solidarity: a call for a pan-European approach against the pandemic*.

[7] General Data Protection Regulation – GDPR, 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. OJ L 119, (2016, May 4). pp. 1-88.

[8] *EDPB response to Mrs Ďuriš Nicholsonová and Mr Jurzyca's letter on common guidance in the fight against the COVID-19 pandemic*s. (2020, April 24.). Brussels. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out2020-0030_mep_duris_covid19_en.pdf

[9] Council of Europe, Directorate General of Human Rights and Rule of Law. *Statement: COVID-19 vaccination, attestations and data protection*, (T-PD-BUR(2021)6rev2 adopted by the Committee on Convention 108 on 3 May 2021.

[10] Data Protection Unit of the Council of Europe. (2020, October). *Digital solutions to fight against COVID-19*. 2020 Data Protection Report.

[11] Váradi, Sz. (2021). „Hozzájárult. Vagy mégsem?" A személyes adatok kezeléséhez történő hozzájárulás érvényességének szempontjai. *FORUM: Acta Juridica Et Politica*, 11(1), 163-179.

[12] EDPB. (2019, January 23). *Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR).*

[13] EDPB. (2020, June 2). *Statement on restrictions on data subject rights in connection to the state of emergency in Member States*. (2020.b.)

[14] EDPB: *Guidelines 10/2020 on restrictions under Article 23 GDPR*. Version 1.0. Adopted on 15 December 2020.

[15] European Union Agency for Fundamental Rights (FRA). (2020, May 28). *Coronavirus pandemic in the EU – Fundamental Rights implications: With a focus on contact-tracing apps.* Bulletin 2.

[16] Cristani, F. (2021). Right to privacy and data protection during the coronavirus crisis: The debate over the use of tracking apps in Italy. In S. Kirchner (ed.): *Governing the Crisis: Law, Human Rights and COVID-19* (pp. 77-99). LIT Verlag, Münster.

[17] EDPB. Temporary suspension of the Norwegian Covid-19 contact tracing app. Official website of EDPB. (2020, June 22). https://edpb.europa.eu/news/national-news/2020/temporary-suspension-norwegian-covid-19-contact-tracing-app_en

[18] Bradford, L., Aboy, M., Liddell, K. (2020). COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes. *Journal of Law and the Biosciences*, 7(1). **https://doi.org/10.1093/jlb/lsaa034**

[19] Van Kolfschooten, H., De Ruijter, A. (2020). COVID-19 and privacy in the European Union: A legal perspective on contact tracing. *Contemporary Security Policy*, 41(3), 478-491. **https://doi.org/10.1080/13523260.2020.1771509**

[20] High-Level Expert group on Artificial Intelligence. (AI HLEG, 2019). *A definition of AI: main capabilities and disciplines*. https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines

[21] Bullock, J., Luccioni, A., Pham, KH. Lam, CSN. (2020). Luengo-Oroz, M.: Mapping the landscape of artificial intelligence applications against COVID-19. *ArXiv*. https://arxiv.org/abs/2003.11336v1 **https://doi.org/10.1613/jair.1.12162**

[22] Naudé, W. (2020). Artificial intelligence vs COVID-19: limitations, constraints and pitfalls. *AI & Soc*, 35, 761-765. **https://doi.org/10.1007/s00146-020-00978-0**

[23] Naudé, W., Vinuesa, R. (2021, July) Data deprivations, data gaps and digital divides: Lessons from the COVID-19 pandemic. *Big Data & Society*. **https://doi.org/10.1177/20539517211025545**

[24] Pusztahelyi, R.: *Recent EU Legislation Relating to Drones in the Light of Right to Privacy*. 2019 MultiScience - XXXIII. microCAD International Multidisciplinary Scientific Conference. **https://doi.org/10.26649/musci.2019.062**

[25] Khemasuwan, D., Colt, H. G. (2021). Applications and challenges of AI-based algorithms in the COVID-19 pandemic. *BMJ Innovations*, 7(2), 387-398. **https://doi.org/10.1136/bmjinnov-2020-000648**

[26] Niiler, E. (2020, January 25). An AI Epidemiologist Sent the First Warnings of the Wuhan Virus. Wired. https://www.wired.com/story/ai-epidemiologist-wuhan-public-health-warnings/

[27] Abd El-Aziz, A.A., Khalifa, N.E.M., Darwsih, A., Hassanien, A.E. (2021). The Role of Emerging Technologies for Combating COVID-19 Pandemic. In Hassanien A. E., Darwish, A. (Eds.), *Digital Transformation and Emerging Technologies for Fighting COVID-19 Pandemic: Innovative Approaches. Studies in Systems, Decision and Control* (pp. 21-41). Springer. **https://doi.org/10.1007/978-3-030-63307-3_2**

[28] European Parliament resolution of 20 January 2021 on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice. (2020/2013(INI) P9_TA(2021)0009.

[29] EDPB-EDPS *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence* (Artificial Intelligence Act).

[30] Daley, S. (2020, March) *Fighting Fires and Saving Elephants: How 12 Companies are Using the AI Drone to Solve Big Problems*. https://builtin.com/artificial-intelligence/drones-ai-companies

[31] EDPB (2020, April 21). *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak.*

[32] Rocher, L., Hendrickx, J. M., De Montjoye, Y. A. (2019). Estimating the success of re-identifications in incomplete datasets using. generative models. *Nature Communications,* 10. **https://doi.org/10.1038/s41467-019-10933-3**

[33] Apple and Google: Privacy-Preserving Contact Tracing. https://covid19.apple.com/contacttracing