Marlena Jankowska, Mirosław Pawełczyk, Ewelina Badura

Enabling Society 5.0 through COVID-19 Digital Transformation, New Data Ecosystems, and Sustainability. Post-pandemic Legal Reflections*

The COVID-19 pandemic has accelerated the adoption of new technologies and raised societies' technological development. Legal regulations play an important role in the implementation of the latest technologies. The contact tracking applications that have been deployed almost all over the world do not, in most cases, provide an adequate level of personal data protection. An essential aspect of competition law regarding data protection is ensuring data security (trade secrets, personal information). Although entrepreneurs' use of cloud data stores is well-established, we have never witnessed adoption on such a large scale as during this pandemic. This was influenced by, among other factors, the need to provide remote access to enterprise resources despite limitations on the movement of people. Furthermore, because many companies faced an immediate need to enable remote working and collaboration, many solutions were adopted without the usual due diligence that should apply to such a business decision. Therefore, questions arise as to whether the legal frameworks for the functioning of such data ecosystems ensure their security. Moreover, since technological innovations are of key importance for sustainable development, it is worth reviewing the framing assumptions (concerning sustainable development) of active sustainability initiatives and the possibilities of still achieving their goals despite the major setback of the pandemic. Furthermore, the rapid and forced changes resulting from the coronavirus pandemic cannot remain in place without adverse impact on the data protection landscape. During the pandemic, legal regulations regarding personal data protection, environmental protection, and competition law began to be questioned. The author shows that the legal regulations in force in these areas are no longer sufficient and require adaptation to the rapidly changing reality.

Marlena Jankowska
associate professor
University of Silesia in Katowice
ORCID – 0000-0001-5425-9593
e-mail: marlena.jankowska@us.edu.pl

Mirosław Pawełczyk
associate professor
University of Silesia in Katowice
ORCID – 0000-0003-1344-8026
e-mail: pawelczyk@pawelczyk.pl

Ewelina Badura
PhD in law
Cracow University of Economics
ORCID – 0000-0002-5514-6299
e-mail: ewebadura@gmail.com

Key words:
application, pandemic, tracking, security, data

https://doi.org/10.36128/priw.vi44.603

1. Introduction

The COVID-19 pandemic has caused severe social and economic disruption worldwide. The legal framework plays an important role in interpreting the rights and obligations of many actors in this crisis: individuals, entrepreneurs, communities, and governments. Regarding the legal framework, there is a need to ensure the transparency of jurisdictions between the different tiers of government responsible for responding to public health crises and other aspects of life. After all,

* The research was co-financed by the funds granted under the Research Excellence Initiative of the University of Silesia in Katowice.

legal provisions aimed at protecting public health should also take into account personal rights and freedoms[1].

The legal regulations regarding quarantine and public health confer governments with broad powers to limit: free movement, collecting and processing personal data, and conducting business activities[2]. Despite a certain justification for these limitations, they are also clearly part of a wider social context[3].

---

1 Glenn Cohen, Sara Gerke, Daniel B. Kramer, „Ethical and Legal Implications of Remote Monitoring of Medical Devices" *Milbank Quarterly*, No. 4 (2020): 1257. doi: 10.1093/jlb/lsaa034; Leonie Kahnbach, Dirk Lehr, Jessica Brandenburger, Tim Mallwitz, Sophie Jent, Sandy Hannibal, Burkhardt Funk, Monique Janneck, „Quality and Adoption of COVID-19 Tracing Apps and Recommendations for Development: Systematic Interdisciplinary Review of European Apps" *Journal of Medical Internet Research*, No. 2 (2021): e27989. doi:10.2196/27989; James O'Connell, Manzar Abbas, Sarah Beecham, Jim Buckley, Muslim Chochlov, Brian Fitzgerald, Liam Glynn, Kevin Johnson, John Laffey, Bairbre McNicholas, Bashar Nuseibeh, Michael O'Callaghan, Ian O'Keeffe, Abdul Razzaq, Kaavya Rekanar, Ita Richardson, Andrew Simpkin, Cristiano Storni, Damyanka Tsvyatkova, Jane Walsh, Thomas Welsh, Derek O'Keeffe, „Best Practice Guidance for Digital Contact Tracing Apps: A Cross-disciplinary Review of the Literature" *JMIR Mhealth Uhealth*, No. 6 (2021): e27753. doi: 10.2196/27753; Hui Li, Yifel Zhu, Yi Niu, „Contact Tracing Research: A Literature Review Based on Scientific Collaboration Network" *International Journal of Environmental Research Public Health*, No. 15 (2022): 9311, doi: 10.3390/ijerph19159311; Andrew Anglemyer, Theresa Hm Moore, Lisa Parker, Timothy Chambers, Alice Grady, Kellia Chiu, Matthew Parry, Magdalena Wilczynska, Ella Flemyng, Lisa Bero, „Digital Contact Tracing Technologies in Epidemics: A Rapid Review" *Cochrane Database of Systematic* Reviews, No. 8 (2020): CD013699. doi: 10.1002/14651858.CD013699.

2 Barbara Nussbaumer-Streit, Verena Mayr, Andreea Iulia Dobrescu, Andrea Chapman, Emma Persad, Irma Klerings, Gernot Wagner, Uwe Siebert, Dominic Ledinger, Casey Zachariah, Gerald Gartlehner, „Quarantine Alone or in Combination with Other Public Health Measures to Control COVID-19: A Rapid Review" *Cochrane Database of Systematic* Reviews, No. 9 (2020): CD013574. doi: 10.1002/14651858.CD013574.pub2.PMID: 33959956.

3 Belinda Bennett, „Legal Rights During Pandemics: Federalism, Rights and Public Health Laws – a View from Australia" *Public Health* (2006): 232-236. doi: 10.1016/j.puhe.2008.12.019; Wafaa M. El-Sadr, Joey

The perception of individual freedoms and individual rights has significantly evolved since the very first versions of most public health laws were adopted. Today, society has high expectations of the preservation of personal freedoms and freedom of movement[4]. The extent to which the state can and should exercise its powers (e.g., the imposition of an obligation to quarantine and self-isolate) in a public health emergency situation is becoming increasingly important for the wider cause of public health itself. The measures taken, including introducing social distancing, quarantine, or restrictions on movement, violate personal freedoms and have serious and severe economic consequences. Some industries have been temporarily banned from doing business at the local level. In others, turnover has decreased significantly due to the introduction of public health measures or other restrictions. The rights and duties of individuals are multifaceted[5]. Rights and obligations regarding public health in cases of contagious disease are both global and national in

Platt, Melanie Bernitz, Melissa Reyes, „Contact Tracing: Barriers and Facilitators" *American Journal of Public Health*, No. 7 (2021): 1025-1033. doi: 10.2105/AJPH.2022.306842.Epub 2022 Jun 2.

4 Jacob Burns , Ani Movsisyan, Jan M Stratil, Renke Lars Biallas, Michaela Coenen, Karl Mf Emmert-Fees, Karin Geffert, Sabine Hoffmann, Olaf Horstick, Michael Laxy, Carmen Klinger, Suzie Kratzer, Tim Litwin, Susan Norris , Lisa M Pfadenhauer, Peter von Philipsborn, Kerstin Sell, Julia Stadelmaier, Ben Verboom, Stephan Voss, Katharina Wabnitz, Eva Rehfuess, „International travel-related control measures to contain the COVID-19 pandemic: a rapid review" *Cochrane Database of Systematic Reviews,* No. 3 (2021): CD013717. doi: 10.1002/14651858.CD013717.pub2.PMID: 33763851; Jacob Burns, Ani Movsisyan, Jan M Stratil, Michaela Coenen, Karl Mf Emmert-Fees, Karin Geffert, Sabine Hoffmann, Olaf Horstick, Michael Laxy, Lisa M Pfadenhauer, Peter von Philipsborn, Kerstin Sell, Stephen Voss, Eva Rehfuess, „Travel-related control measures to contain the COVID-19 pandemic: a rapid review" *Cochrane Database of Systematic* Reviews, No. 10 (2020): CD013717. doi: 10.1002/14651858.CD013717.PMID: 33502002.

5 Inter alia: article 5, The European Convention on Human Rights (ECHR; formally the Convention for the Protection of Human Rights and Fundamental Freedoms). https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=005. [accessed: 12.10.2022]; article 6-19, Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391–407; article 30; The Constitution of the Republic of Poland of April 2, 1997, adopted by the National Assembly on April 2, 1997, adopted by the Nation in a constitutional referendum on May 25, 1997, signed by the President of the Republic of Poland on July 16, 1997, (Journal of Laws of 1997, No. 78, item 483).

scope[6]. Therefore, in order to be able to assess whether the introduced legal regulations are adequate in the event of a pandemic, it is necessary to analyze whether these regulations are in line with international obligations[7].

This study argues that, despite the numerous problems and damage caused by the COVID-19 pandemic, the crisis also provides a good opportunity to extract some positive outcomes and achieve new sustainable development goals (SDG goals 8 and 9)[8] and adopt a new perspective on data protection. Three areas have been subject to legal analysis. The second chapter presents the 5.0 Society in light of the IT portfolio theory. The third chapter discusses the issues of personal data protection that arise from the implementation of tracking applications. Chapter four presents the issue of new business models triggered by the pandemic and competition law as it relates to the creation of data ecosystems. The coverage of this topic took into account the change in technological trends related to data storage and processing with the use of large, international Internet platforms. In conclusion, it is noted that appropriate legal regulations ensuring the protection of personal data, trade secrets, and environmental protection are integral to sustainable development and the modern digital economy.

2. IT Portfolio theory in Society 5.0

IT investments give firms a competitive advantage while positioning them in the marketplace. Capital investment (assets) provides many benefits,

6 Ibidem, and also article 168, Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, p. 47–390; Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, OJ L 88, 4.4.2011, p. 45-65; Decission No 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC Text with EEA relevance, OJ L 293, 5.11.2013, p. 1–15.

7 Federica Lucivero, Luca Marelli, Nora Hangel, Bettina Maria Zimmermann, Barbara Prainsack, Ilaria Galasso, Ruth Horn, Katharina Kieslich, Marjolein Lanzing, Elisa Lievevrouw, Fernandos Ongolly, Gabrielle Samuel, Tamar Sharon, Lotje Siffels, Emma Stendahl, Ine Van Hoyweghen, „Normative Positions towards COVID-19 Contact-tracing Apps: Findings from a Large-scale Qualitative Study in Nine European Countries" *Critical Public Health* (2021): 1-14. doi: 10.1080/09581596.2021.1925634.

8 The Sustainable Development Goals Report (2020). https://unstats.un.org/sdgs/report/2020/The-Sustainable-Development-Goals-Report-2020.pdf.

not only informational but also transactional, strategic, and infrastructural[9]. Society 5.0's distinction between public and industrial infrastructure is no longer apparent (e.g., mobile banking)[10]. Building a futuristic organization is a risky adventure demanding players to be ahead of their competitors[11].

MIT Sloan School of Management researchers examined IT investments made by 640 significant US corporations[12].

They determined that an „IT portfolio" or investment spread consists of four primary categories of IT assets. These are:

Transactional investments: Investing in transactions allows for effective cost reduction or throughput expansion. IT handles and supports the

9 Jones Downes, Goodman Jordan, „Dictionary of Finance and Investment Terms" (NY: Deakin University, 1991). https://www.futurelearn.com/info/courses/competitive-advantage/0/steps/28143. [accessed: 14.10.2022].

10 Bridget Pratt, Susan Bull, „Equitable Data Sharing in Epidemics and Pandemics" *BMC Med Ethics*, No. 1 (2021): 136. doi: 10.1186/s12910-021-00701-8; Ji E Chang, Alden Yuanhong Lai, Avni Gupta, Ann M Nguyen, Carolyn A Berry, Donna R Shelley, „Rapid Transition to Telehealth and the Digital Divide: Implications for Primary Care Access and Equity in a Post-COVID Era" *Milbank Quarterly*, No. 2 (2021): 340-368. doi: 10.1111/1468-0009.12509; Kyle Knierim, Christina Palmer, Erik Seth Kramer, Rachel S Rodriguez, Jill VanWyk, Alison Shmerling, Peter Smith, Heather Holmstrom, Brian S Bacak, Shandra M Brown Levey, Elizabeth W Staton, Jodi Summers Holtrop, „Lessons Learned During COVID-19 That Can Move Telehealth in Primary Care Forward" *Journal of the American Board of Family Medicine*, No. 34 (Suppl) (2021): 196-202. doi: 10.3122/jabfm.2021.S1.200419; Marco Bardus, Melodie Al Daccache, Noel Maalouf, Rayan Al Sarih, Imad H Elhajj, „Data Management and Privacy Policy of COVID-19 Contact-Tracing Apps: Systematic Review and Content Analysis" *JMIR Mhealth Uhealth*, No. 7 (2022): e35195. doi: 10.2196/35195; Jan-Patrick Weiß, Moritz Esdar, Ursula Hübner, „Analyzing the Essential Attributes of Nationally Issued COVID-19 Contact Tracing Apps: Open-Source Intelligence Approach and Content Analysis" *JMIR Mhealth Uhealth*, No. 3 (2021): e27232. doi: 10.2196/27232.

11 Balebako Rebecca, Jung Jaeyeon, Lu Wei, Cranor Lorrie Faith, Nguyen Carolyn, *Little Brothers Watching You Raising Awareness of Data Leaks on Smartphones* (Proceedings of the Ninth Symposium on Usable Privacy and Security, Newcastle, UK, 24-26 July 2013), 1-11.

12 Peter Weill, Sinan Aral, „Generating Premium Returns on Your IT Investments" *MIT Sloan Management Review*, No. 2 (2006): 39.

company's fundamental, routine transactions. Such assets utilise infrastructure support services.

Informational investments: Investments in information provide information for management control and decision-making processes like accounting, reporting, compliance, communication, or analysis. These assets use transactional systems and the IT infrastructure.

Strategic Investments: Investments made strategically help provide a competitive edge by facilitating entry into new markets or by assisting in the development of new goods, services, or operational procedures. Remember that what was previously strategic might change to become transactional or infrastructural (for example, ATMs were once a strategic IT endeavour but over time, they turned transactional).

Infrastructure investments: Do various apps use shared IT services (such as servers, networks, laptops, and customer databases)? Infrastructure investments can provide a flexible foundation for future business activities or, depending on the service, can lower long-term IT costs through consolidation.

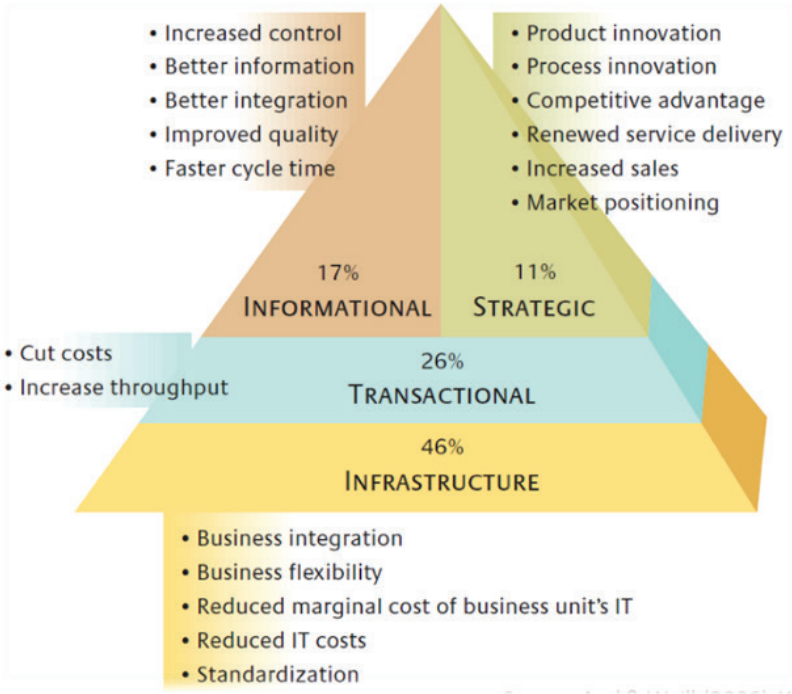

Figure 1: Business value returns from the IT Portfolio (Weill, Sinan, „Generating", 39 and ff)

IT Portfolio Investment Type	Business Value	Risk
Informational (typically 17% of investment)	Increased control; Better information; Better integration; Improved quality; Better cycle time	Moderate risk/return
Strategic (typically 11% of investment)	Product innovation; Process innovation; Competitive advantage; Renewed service delivery; Increased sales; Market positioning	High risk, potentially high return
Transactional (typically 26% of investment)	Cut costs; Increase throughput	Low risk, solid return
Infrastructure (typically 46% of investment)	Business integration; Business flexibility; Reduced marginal cost of business unit's IT; Reduced IT costs; Standardisation	Moderate risk / return. Risk of lock-in

Figure 2: Juxtaposition of IT Portfolio assets, their business values, and types of risks

IT portfolio theory is a complex investment decision method because it enables investors to categorise, calculate, and manage the type and quantity of expected risk and return[13].

3. Personal data protection in pandemic times

The COVID-19 pandemic has caused governments worldwide to restrict civil liberties to a greater or lesser extent, including the right to free movement. In order to ensure the safe lifting of such restrictions, new technologies – such as contact tracking applications – have been developed or implemented. Many arguments were made that these applications should be mandatory, justified by the need to automate labor-intensive tasks crucial to arrest the spread of the virus. Tracking applications are in operation or implemented in almost all Europe, Asia, Oceania, and North America[14].

13 John Downes, Jordan Goodman, *Dictionary of Finance and Investment Terms* (New York: Barron's Educational Series, 2014), 233-256.

14 For example: Stop COVID-19, TousAntiCovid, Corona-Warn-App, COVID Tracker, Immuni, Apturi Covid, #OstaniZdrav, COVIDSafe, Koronavilkku, LeaveHomeSafe, Ehteraz application, Tabaud, COVID AlertSA.

While tracking applications can play a crucial role in fighting COVID-19, there is no doubt that they also raise questions about protecting personal data[15]. Supplemented with other methods of counteracting the pandemic, the tracking applications can ensure greater accuracy and help limit the further spread of the coronavirus pandemic. Legal regulations play a key role in reinforcing the rights and obligations of individuals and entire communities, including governments, ensuring transparency and accountability for decision-making[16]. In modern society, with its high expectations as to the rights and freedoms of individuals and the assumption of a properly functioning public health care system, legal regulations are essential to ensure a properly functioning public health protection system while respecting civil rights and freedoms. Adequate preparation for a pandemic does not stop at the border of one country, as the coronavirus pandemic has affected all parts of the world. Bearing in mind that new pandemics can occur in the future, it should be remembered that global cooperation is essential. The guidelines for developing applications related to COVID-19, prepared by the European Commission in cooperation with the Member States, the European Data Protection Supervisor, and the European Data Protection Board, aim to guarantee sufficient data protection and to limit interference with citizens' rights and freedoms. In line with these guidelines, applications should fully comply with EU regulations regarding the protection of personal data, particularly with the General Data Protection Regulation (GDPR) and the Directive on privacy and electronic communications[17].

3.1. Tracking apps – privacy and personal data protection

Governments faced difficulties tracing contacts during the COVID-19 outbreak. UK authorities use and continue to develop technology designed to monitor and control the spread of COVID-19. One helpful

15 Gianluca Montanari Vergallo, Simona Zaami, Enrico Marinelli, „The COVID-19 Pandemic and Contact Tracing Technologies, between Upholding the Right to Health and Personal Data Protection" *European Review for Medical and Pharmacological Sciences*, No. 5 (2021): 2449-2456. doi: 10.26355/eurrev_202103_25286.

16 Laura Bradford, Mateo Aboy and Kathleen Liddell 2020, „COVID-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR, and Data Protection Regimes" *Journal of Law and the Biosciences*, No. 1 (2020): 1-21. https://doi.org/10.1093/jlb/lsaa034.

17 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201, 31/07/2002, 0037-0047.

source, among others, was a contact tracing approach using CCTV footage. Although the National Health Service (NHS) developed its contact tracking smartphone app, it quickly became apparent, as announced on 18 June 2020, that the app's limitations rendered it impractical, as a result of which the UK chose to reimplement it based on a system jointly developed by Apple and Google. It is planned to be operational in autumn 2020 at the earliest.

The NHS COVID-19 app[18] is a quick and easy way to get the latest advice and find out if you may have been exposed to coronavirus (COVID-19). The NHS COVID-19 app is available to download for free in England and Wales. The app will be updated from time to time with new functionality and improvements. The latest version includes up-to-date features and advice, so it is important to keep the app updated. The NHS COVID-19 app uses Bluetooth Low Energy (BLE) to understand the distance, over time, between app users. Typically, you'll be sent an exposure notification with guidance if you've been within 2 meters of someone for 15 minutes or longer who has since tested positive for COVID-19.

As to the use of this application, there were concerns about its security and privacy protection rules[19]. Additional aspects were questioned: the scope of the downloaded data, transparency, and liability rules on the part of private users and the authorities to which the data is transferred. The emerging doubts also a concern, among other things, supervision of the collection of surplus data and their use for unrelated purposes as the principles of appropriate storage and processing of the obtained data[20]. Due to the nature of the pandemic, the data will be stored indefinitely. There is no liability on the part

18 NHS COVID-19 app: user guide, https://www.gov.uk/government/publications/nhs-covid-19-app-user-guide.

19 Mahmoud Elkhodr, Omar Mubin, Zainab Iftikhar, Maleeha Masood, Belal Alsinglawi, Suleman Shahid, Fady Alnajjar, „Technology, Privacy, and User Opinions of COVID-19 Mobile Apps for Contact Tracing: Systematic Search and Content Analysis" *Journal of Medical Internet Research*, No. 2 (2021): e23467. doi: 10.2196/23467; Katarzyna Kolasa, Francesca Mazzi, Ewa Leszczuk-Czubkowska, Zsombor Zrubka, Márta Péntek, „State of the Art in Adoption of Contact Tracing Apps and Recommendations Regarding Privacy Protection and Public Health: Systematic Review" *MIR Mhealth Uhealth*, No. 6 (2021): e23250, doi: 10.2196/23250.

20 EDPS, 'Preliminary Opinion of the European Data Protection Supervisor Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy' March (2014): 72-76. Available at: https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf.

of the authorities for violations arising in connection with the gathering and processing of data, which mainly concern sensitive data, i.e., health problems of the population[21].

In France, the National Institute for Research in Digital Science and Technology (INRIA) developed the „StopCovid" application, made available for general use on 2 June 2020. At the same time, the legal framework for the operation of this application was introduced in the regulation on data processing called „StopCovid" (Decree 2020-650 of 29 May 2020). In June, the application was downloaded by fewer than 2 million residents, of whom only 14 people were notified of contact with a person infected with the coronavirus[22].

However, it soon emerged that the application collects more data than initially thought. It was revealed, inter alia, that all cross-contacts are sent to a central server. According to the guidelines, only the data of app users who had been in contact for a minimum of 15 minutes within 1 meter of a person diagnosed with COVID-19 should have been collected. This case proves that the principles of gathering data only to the extent necessary were not upheld. Despite this, the French data protection authority (CNIL) has found that the app complies with EU laws and French data protection requirements. The concerns of French society, in this case, are related to the use of a centralized server, which increases the risk of possible cyber-attacks. In addition, there are allegations of discrimination against people who do not use this application because they may have a problem finding a job or obtaining ready access to certain public areas. When the consent of people who download the tracking

21 Glenn Cohen, Lawrence O. Gostin, Daniel J. Weitzner, „Digital Smartphone Tracking for COVID-19: Public Health and Civil Liberties in Tension" *JAMA*, No. 23 (2020): 2371-2372. doi: 10.1001/jama.2020.8570.2766675; Nicole Martinez-Martin, Sarah Wieten, David Magnus, Mildred K Cho, „Digital Contact Tracing, Privacy, and Public Health" *Hastings Center Report*, No. 3 (2020): 43-46. doi: 10.1002/hast.1131; Robert A Kleinman, Colin Merkel, „Digital Contact Tracing for COVID-19" *Canadian Medical Association Journal*, No. 24 (2020): E653-E656. doi: 10.1503/cmaj.200922; Bridget Pratt, Michael Parker, Susan Bull, „Equitable Design and Use of Digital Surveillance Technologies During COVID-19: Norms and Concerns" *The Journal of Empirical Research on Human Research Ethics*, No. 5 (2022): 573-586. doi: 10.1177/15562646221118127.

22 Délibération n° 2020-056 du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile dénommée, StopCovid, (demande d'avis n° 20008032). https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000041937703; https://www.service-public.fr/particuliers/actualites/A14069?lang=en.

application to their phone is not given voluntarily, it means that it is invalid. Additionally, the StopCovid application is not anonymised and provides inadequate protection.

The first French StopCOVID app didn't work, but a new coronavirus tracking tool, TousAntiCovid, was launched on 22 October 2020. The StopCOVID application was criticized from the very beginning by IT specialists and doctors themselves. Just over 2 million users downloaded it, and only a few hundred thousand ran it, most of whom then uninstalled it. Its use was voluntary, and the companies involved in its creation worked almost pro publico bono. The new app contains information about the coronavirus and where users can get tested. It also allows contact tracking, i.e., of people in contact with infected individuals.

On 16 June 2020, Germany (along with several other countries) launched Corona Warn App (CWA), a mobile phone-based digital contact tracing system[23]. This application is designed for contact tracing („PEPP-PT"), and

23 Stephan Ellmann, Markus Maryschok, Oliver Schöffski, Martin Emmert, „The German COVID-19 Digital Contact Tracing App: A Socioeconomic Evaluation" *International Journal of Environmental Research Public Health* No. 21 (2022): 14318. doi: 10.3390/ijerph192114318; Michael Winter, Harald Baumeister, Ulrich Frick, Miles Tallon, Manfred Reichert, Rudiger Pryss, *Exploring the Usability of the German COVID-19 Contact Tracing App in a Combined Eye Tracking and Retrospective Think Aloud Study* (Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2021), 2215-2221. doi: 10.1109/EMBC46164.2021.9630949.PMID: 34891727; Lorina Buhr, Silke Schicktanz, Eike Nordmeyer, „Attitudes Toward Mobile Apps for Pandemic Research Among Smartphone Users in Germany: National Survey" *JMIR Mhealth Uhealth*, No. 1 (2022): e31857. doi: 10.2196/31857. PMID: 35072646; Kai T Horstmann, Susanne Buecker, Julia Krasko, Sarah Kritzler, Sophia Terwiel, „ Who does or does not Use the »Corona-Warn-App« and Why?" *European Journal of Public Health*, No. 1 (2021): 49-51. doi: 10.1093/eurpub/ckaa239; Annelies G Blom, Alexander Wenz, Carina Cornesse, Tobias Rettig, Marina Fikel, Sabine Friedel, Katja Möhring, Elias Naumann, Maximiliane Reifenscheid, Ulrich Krieger, „Barriers to the Large-scale Adoption of a COVID-19 Contact Tracing App in Germany: Survey Study" *Journal of Medical Internet Research*, No. 3 (2021): e23362. doi: 10.2196/23362; Torben Heinsohn, Berit Lange, Patrizio Vanella, Isti Rodiah, Stephan Glöckner, Alexander Joachim, Dennis Becker, Tobias Brändle, Stefan Dhein, Stefan Ehehalt, Mira Fries, Annette Galante-Gottschalk, Stefanie Jehnichen, Sarah Kolkmann, Annelene Kossow, Martin Hellmich, Jörg Dötsch, Gérard Krause, „Infection and Transmission Risks of COVID-19 in

its back-end infrastructure is fully open source under the Apache 2.0 license. Using Bluetooth Low Energy technology, the Corona-Warn app collects data from nearby cell phone owners. When at least two users are about two meters away from each other and stay at that distance for fifteen minutes or more, their applications exchange data via BLE. If a user tests positive for COVID-19, he can upload the test result using the Corona-Warn app. Corona-Warn will then inform all stored contacts anonymously. The data is stored locally, preventing any third parties from accessing it. The Corona-Warn application was designed with an emphasis on privacy protection, but it quickly emerged that users can be „de-anonymised" in a fairly simple way. Moreover, since Apple and Google are the operating system vendors, they have access to all data that passes through their interfaces[24]. There are, therefore, some concerns regarding access to the collected data.

In Germany, „Datenspende-App" collects general information about the movement[25]. The Corona-Datenspende App, created by the Robert Koch Institute (RKI), aims to facilitate the recognition of coronavirus symptoms and to control its spread[26]. The application saves data on the user's health, downloaded from smartwatches and fitness bands. For this purpose, the application user agrees to the anonymous sharing of this data and provides

Schools and their Contribution to Population Infections in Germany: A Retrospective Observational Study Using Nationwide and Regional Health and Education Agency Notification data" *PLOS Medicine*, No. 12 (2022): e1003913. doi: 10.1371/journal.pmed.1003913. eCollection 2022 Dec.PMID: 36538517.

24 Tamar Sharon, „Blind-sided by Privacy? Digital Contact Tracing, the Apple/Google API and Big Tech's Newfound Role as Global Health Policy Makers" *Ethics and Information Technology*, No. 23 (2020): 45-57. doi: 10.1007/s10676-020-09547-x; Jennifer Nicholas, Katie Shilton, Stephen M Schueller, Elizabeth L Gray, Mary J Kwasny, David C Mohr, „The Role of Data Type and Recipient in Individuals' Perspectives on Sharing Passively Collected Smartphone Data for Mental Health: Cross-sectional Questionnaire Study" *JMIR Mhealth Uhealth*, No. 4 (2019): e12578. doi: 10.2196/12578; Hamad Alamri, Carsten Maple, Saad Mohamad, Gregory Epiphaniou, „Do the Right Thing: A Privacy Policy Adherence Analysis of over Two Million Apps in Apple iOS App Store" *Sensors (Basel)*, No. 22 (2022): 8964. doi: 10.3390/s22228964.

25 Cf. Robert Koch Institute. COVID-19-Impfungen_in_Deutschland: Impfdashboard. 2021. Available from: https://impfdashboard.de/. [accessed: 15.11.2022].

26 https://www.bundesregierung.de/breg-de/themen/coronavirus/datenspende-app-1739928. [accessed: 14.11.2022]; https://corona-datenspende.de/#funktion. [accessed: 22.11.2022].

their postal code. The collected data is categorized by postal code. As heart rate, sleep rhythm, and human activity levels fluctuate due to respiratory disease, the Institute says the app can also pinpoint areas of high COVID-19 infection by accessing this data.

In Italy, a well-known software company was commissioned to develop a pandemic tracking application. The rules governing the operation of this application have been laid down in Decree No.28 of 30 April 30, 2020. The contact tracking application „Immuni" was made available throughout Italy on 15 June. Under the adopted regulations, the data controller is the Ministry of Health, and the data will be stored on servers in Italy. According to the Italian Data Protection Authority, the above regulation complies with other provisions in force in the field of personal data protection and user privacy[27]. Despite this, there are some concerns about the operation of this application. They are concerned with the issue of data minimization, the security of the obtained data, the risk of re-identification, and the actual use of data for other purposes. Italian entrepreneurs who want to monitor their employees (their work) must also meet strict requirements provided in legal regulations on remote employee monitoring.

In Poland, due to the COVID-19 pandemic, two applications have been made available for use: „Home quarantine" (pol. „Kwarantanna domowa") and „ProteGO Safe"[28]. The first is intended for people undergoing a 14-day mandatory home quarantine due to suspected COVID-19 infection. This application uses geolocation and facial recognition technology to ensure that the right people are quarantined. The „ProteGO Safe" application is designed to allow users to monitor the risk of infection. If the user installs this

27 Noemi Scrivano, Rosario Alfio Gulino, Daniele Giansanti, „Digital Contact Tracing and COVID-19: Design, Deployment, and Current Use in Italy" *Healthcare,* No. 1 (2021): 67. doi: 10.3390/healthcare10010067; Silvia Ussai, Marco Pistis, Eduardo Missoni, Beatrice Formenti, Benedetta Armocida, Tatiana Pedrazzi, Francesco Castelli, Lorenzo Monasta, Baldassare Lauria, Ilaria Mariani, „»Immuni« and the National Health System: Lessons Learnt from the COVID-19 Digital Contact Tracing in Italy" *International Journal of Environmental Research Public Health*, No. 12 (2022): 7529. doi: 10.3390/ijerph19127529; Flavia Beccia, Andrea Di Pilla, Francesco Andrea Causio, Bruno Federico, Maria Lucia Specchia, Carlo Favaretti, Stefania Boccia, Gianfranco Damiani, „Narrative Review of the COVID-19 Pandemic's First Two Years in Italy" *International Journal of Environmental Research Public Health*, No. 23 (2022): 15443. doi: 10.3390/ijerph192315443.

28 Julia Banasiak, „Application ProteGo Stop Covid – Could it have been an Opportunity to Prevent Covid-19 Spreading?" *Political Preferences*, No. 29 (2021): 47-59.

application, it allows him to search the surrounding area for other smartphones using the application and saves the contact history. Because there is no clarity as to the app's methods for protecting the collected personal data, there is a risk of data leakage. Due to the fear that the use of the „Home Quarantine" application violates users' rights to personal data protection, the Human Rights Defender asked the President of the Personal Data Protection Office for an opinion on this matter.

In turn, the second application, „ProteGO Safe" raises concerns about the possibility of revealing the history of social connections. According to some specialists, this application raises a security risk for users due to the constantly enabled Bluetooth and the automated decision-making system.

In the beginning, no single technology was used nationwide in Russia[29]. Monitoring the spread of COVID-19 was local, and some technologies were introduced in certain regions of Russia. The solution, borrowed from China, used quick response graphic codes (QR) and a "social monitoring" application. The downloading of the application was mandatory for all those infected with COVID-19 who were quarantined at home. It enabled, for example, the police and the National Guard to track sick people (place of lodging, health condition, etc.) by accessing the full content of a mobile phone. For Muscovites forced to move around the city (e.g., for professional reasons), it was necessary to download a QR code to the phone, which gave access to geolocation databases and health information.

Moscow, where the number of cases was highest, was the first city to implement technology for monitoring the location of citizens and their close contacts with citizens tested positive for COVID-19 via an app called „Social Monitoring". This application monitors violations of the quarantine regime imposed on people receiving treatment at home or those with restrictions on leaving their residence. As to the functioning of this application, there are also numerous concerns regarding the possibility of violating the privacy of its users. These concerns mainly relate to possible cyber-attacks, information leakage, and further disclosure to unauthorized third parties. Due to the fact that this application allows for monitoring of geolocation and of any movements from the place of residence, it allows identification of persons who break the applicable regulations on movement during the pandemic and exposes users to high penalties for violations. Moreover, the scope of the information collected and transmitted by the application is also questionable. It is especially true for photographs uploaded using the application. Considering that the information on the operation of this application is quite limited,

29 Polish Institute of International Affairs (PISM), Coercion and control – Russia during the COVID-19 epidemic, 1 June 2020. https://www.pism.pl/publikacje/Przymus_i_kontrola__Rosja_w_trakcie_epidemii_COVID19. [accessed: 26.12.2022].

questions arise as to whether the information transmitted by it is adequately protected.

Although no tracking application has yet been implemented in the Netherlands, the Dutch government is considering such a possibility. Therefore, the country's authorities solicited public opinion before presenting a proposal. Still, it was found that none of the proposed applications meets the requirements for, inter alia, an appropriate level of data security[30]. Society was very divided on the implementation of a tracking application.

3.2. Changes in data protection law triggered by COVID-19

Aside from the implementation of an application, amendments to data protection law were discussed[31]. Changes were made to the Dutch Telecommunications Act (in Dutch: Telecommunicatiewet) to allow the National Institute of Health and Environment (in Dutch: Rijksinstituut voor Volksgezondheid en Milieu) to access data on the location and movement of citizens through the Dutch Central Statistical Office (in Dutch: Centraal Bureau voor de Statistiek) to control the spread of COVID- 19. The Dutch data protection authority (DDPA) pointed to the need to narrow the scope of the new regulations to crises such as COVID-19 and clarify the powers granted to the National Institute of Health and Environment. In addition, it rightly emphasized the necessity to specify the maximum retention period of the obtained data. DDPA also referred to the new regulations, stating that the collected data is not properly anonymized and that the purpose and justification for adopting new regulations should be specified. According to the DDPA, the primary safeguards were not sufficient.

30 Majid Hatamian, Samuel Wairimu, Nurul Momen, Lothar Fritsch, „A Privacy and Security Analysis of Early-deployed COVID-19 Contact Tracing Android Apps" *Empirical software engineering*, No. 26 (2021): 36. doi: 10.1007/s10664-020-09934-4; Achilleas Papageorgiou, Michael Strigkos, Eugenia Politou, Efthimios Alepis, Agusti Solanas, Constantinos Patsakis, „Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice" *IEEE Access*, No. 6 (2018): 9390-9403. doi: 10.1109/ACCESS.2018.2799522; Agarwal Yuvraj, Hall Michael, „Protect My Privacy: Detecting and Mitigating Privacy Leaks on iOS Devices Using Crowdsourcing", [in:] *Proceedings of the 11th Annual International Conference on Mobile Systems, Applications, and Services* (Taipei, 2013), 97-110.

31 Sandra Wachter, Brent Mittelstadt, „A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI" *Columbia Business Law Review*, No. 2 (2019): 443-493.

Published on 16 April 2020 by the European Commission[32] , working with the Member States, the European Data Protection Supervisor, and the European Data Protection Board, guidelines aim to guarantee sufficient data protection. It was stressed that the applications must fully comply with EU data protection law, particularly the General Data Protection Regulation (GDPR) and the e-privacy directive. The regulations mentioned above ensure the principle of voluntary participation, the minimization of collected data, and the time limitation of stored data. These rules are necessary for these applications to function in a legally unproblematic fashion on a large scale. These guidelines aim to provide the legal framework to guarantee citizens adequate data protection and reduce the risk of surveillance when using such applications. The main criteria for creating the applications mentioned above should therefore be the maintenance of users' control over their data, limiting the use of personal data, strict restrictions on data storage and data security, and the involvement of national data protection authorities[33].

32 Communication from the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection 2020/C 124 I/01 - C/2020/2523 - OJ C 124I, 17.4.2020, p. 1–9 On 16 April 2020 EU Members States, supported by the Commission, have developed an EU toolbox for the use of mobile applications for contact tracing and warning in response to the coronavirus pandemic. This is part of a common coordinated approach to support the gradual lifting of confinement measures. https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf. [accessed: 25.12.2022]. cf. Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data. EUR-Lex. 2020. Apr 08, [accessed: 23.06.2021]. http://data.europa.eu/eli/reco/2020/518/oj/eng. [accessed: 27.12.2022]. Commission Implementing Decision (EU) 2020/1023 of 15 July 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 (Text with EEA relevance) EUR-Lex. 2020. Jul 15. http://data.europa.eu/eli/dec_impl/2020/1023/oj/eng. [accessed: 28.12.2022].

33 Adam Schwartz, Andrew Crocker, *2020. Electronic Frontier Foundation. Governments Haven't Shown Location Surveillance Would Help Contain COVID-19.* https://www.eff.org/deeplinks/2020/03/governments-havent-shown-location-surveillance- would-help-contain-COVID-19. [accessed: 26.12.2022].

In a resolution adopted on 17 April 2020, The European Parliament stressed that digital measures to counter the pandemic must comply with data protection and privacy rules. At the same time, it was stated that the use of applications should not be compulsory, and those application providers should provide for their withdrawal after the pandemic ends. It was emphasized that the obtained data should be anonymized and, for security reasons, not stored in centralized databases. The need to explain how a given application works and how it will contribute to fighting the pandemic with transparent rules of operation was also noted. Moreover, the Commission concluded that applications based on Bluetooth technologies are preferable to those based on geolocation. Indeed, it was considered that applications based on geolocation collect real-time data about the exact location and movement of people, including information about their health, which poses a greater threat to privacy.

Undoubtedly, digital surveillance technologies are useful to combat the COVID-19 pandemic (Ting, Carin, Dzau, Wong 2020). However, how these applications contain the spread of COVID-19 remain under-researched.

4. Technology and competition law

The changes caused by the COVID-19 pandemic are also noticeable in areas related to the implementation of new business models[34]. The COVID-19 pandemic has presented organizations and society with the challenge of collecting, integrating, and analyzing huge amounts of data, including trade secrets[35]. The pandemic outbreak forced most organizations to undertake new tasks and forms of cooperation[36]. One example is the implementation of

34 Robert M. Davison, „The transformative potential of disruptions: A viewpoint" *International Journal of Information Management* (2020): 226, doi: 10.1016/j.ijinfomgt.2020.102149. Michael Jacobides, Martin Bruncko, Rene Langen, *Regulating Big Tech in Europe: why, so what, and how understanding their business models and ecosystems can make a difference* (London: London Business School, 2020). https://ssrn.com/abstract=3765324. [accessed: 28.12.2022].

35 Jie Sheng, Joseph Amankwah-Amoah, Zaheer Khan, Xiaojun Wang, „COVID-19 Pandemic in the New Era of Big Data Analytics: Methodological Innovations and Future Research Directions" *British Journal of Management*, No. 4 (2021): 1164-1183. https://doi.org/10.1111/1467-8551.12441.

36 Paula Caligiuri, Helen De Cieri, Dana Minbaeva, Alain Verbeke, Angelika Zimmermann, „ International HRM Insights for Navigating the COVID-19 Pandemic: Implications for Future Research and Practice" *Journal of International Business Studies*, 2020. https://news.ucalgary.ca/news/sites/default/files/teams/80/JIBS-Pandemic-IHRM-2020.pdf.

a remote work environment[37]. Moreover, organizations quite quickly deployed a range of digital infrastructure and tools to ensure continuity of service to their customers[38]. In the event of the COVID-19 pandemic, a wide variety of widely distributed decentralized actors are involved in the process of creating and collecting data. These actors include local and regional authorities, technology developers and providers, healthcare institutions, and private actors. In addition, huge amounts of location-based data are being collected from IoT platforms, social applications, and mobile devices[39].

Competition law has not kept pace with technological progress[40]. Comprehensive and effective competition law is essential for any market economy[41]. It is also good for business. However, this is not an easy task in the age of big tech companies and technologies that are developing and innovating at a rapid pace. European competition authorities should also have a good understanding of how technological innovation works. It is necessary to ensure that the adopted regulations are enforced[42].

---

37 Eva Verbeemen, Salvadore B. D'Amico, *Why Remote Working Will be the New Normal, Even after COVID-19*, 2020. https://www.ey.com/en_be/covid-19/why-remote- working-will-be-the-new-normal-even-after-covid-19. [accessed: 26.12.2022].

38 J. Hines, *HR & Digital Trends. The Workplace after COVID-19: What is Your New Normal?*. https://www.hrdigitaltrends.com/story/14398/workplace-after-covid-19-what-your- new-normal. [accessed: 27.12.2022].

39 Daniel Shu Wei Ting, Lawrence Carin, Victor Dzau, Tien Y. Wong, „ Digital Technology and COVID-19" *Nature Medicine*, No. 26 (2020): 459-461.

40 Katherine Kemp, „Concealed Data Practices and Competition Law: Why Privacy Matters" *European Competition Journal*, No. 2-3 (2020): 628-672; Daniel Sokol, Feng Zhu, „Harming Competition and Consumers under the Guise of Protecting Privacy: An Analysis of Apple's iOS 14 Policy Updates" *USC Law Legal Studies Paper*, No. 21-27 (2021): 23-32; Marco Botta, Klaus Wiedemann, „The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey" *The Antitrust Bulletin*, No. 3 (2019): 428-446.

41 Francisco Costa-Cabral and Orla Lynskey, „Family Ties: The Intersection Between Data Protection and Competition in EU law" *Common Market Law Review*, 54(1) (2017): 11-50.

42 Ibidem; Anthony Reyna, „The Psychology of Privacy – What can Behavioral Economics Contribute to Competition in Digital Markets?" *International Data Privacy Law*, No. 3 (2018): 240-252; Inge Graef, Daiman Clifford, Peggy Valcke, „Fairness and Enforcement: Bridging

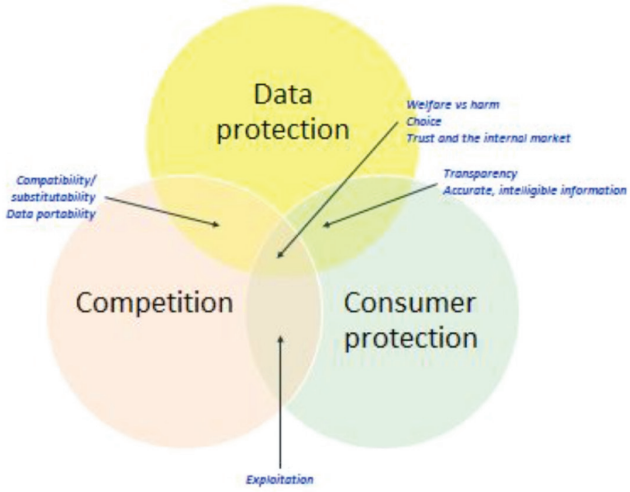

Figure 3: The interplay between data protection, competition law, and consumer protection in the Digital Economy[43]

In view of the above challenges, it is worth considering how individual entrepreneurs should behave. What solutions will the legislator adopt in the field of digital competition law? Competition law in EU countries is highly dependent on regulations at the EU level, and therefore there is also a probability of overlapping competition law provisions across Member States. After all, digital competition law goes beyond national borders. In addition, different national competition authorities take different approaches to enforcing applicable laws. There is also a lack of European Court of Justice jurisprudence, so it is difficult for companies and national competition authorities to act without knowledge of which action is appropriate in specific situations in cases of digital competition.

Competition, Data Protection, and Consumer Law" *International Data Privacy Law*, No. 3 (2018): 200-223.

43 EDPS, *Preliminary Opinion of the European Data Protection Supervisor Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*', March 2014. https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf. [accessed: 29.12.2022].

4.1. Internet platforms and data ecosystems

The dominant approach to competition has long been the consumer welfare standard, based on the measurement of benefit or harm to consumers in the form of lower or higher prices, respectively[44]. Therefore, certain practices of dominant platforms may continue to cause consumer harm in forms other than price. However, this catalogue should be extended to include other criteria, such as the lock-in effect of dominant platforms[45].

Due to the fact that large technology companies create very complex data ecosystems, the relevant competition authorities are now facing the challenge of keeping up with rapid technological changes. It is necessary to adopt regulations that consider the fact that digital competition law refers not only to consumer law and personal data protection but also, *inter alia*, to the protection of entrepreneurs' trade secrets.

The use of cloud storage for corporate data is nothing new. This data storage model, as has remote working, has become even more popular during the pandemic. Organizations were able to quickly deploy a range of digital infrastructure and tools to create a digital workplace. Serving digital customers during an outbreak also prompts organizations to implement tools that closely track customer data. Organizations can use these data to achieve corporate profits, often with scant heed to customer privacy. On the one hand, the use of international digital platforms offers many advantages to entrepreneurs, who benefit from the market traction of an established platform. On the other hand, the operator of such platforms stands to gain control over consumers' data and the customer relationship in general, which yields market power. It also raises concerns about the possibility of gaining an unfair competitive advantage. Platformization affects not only the nature of transactions in certain sectors of the economy but also the ability of firms to scale quickly, thus affecting the structure of particular sectors.

Large technology companies have penetrated many aspects of people's lives, from purchasing to social interactions, but have also become an integral part of the operation of a modern company. The most popular 'platforms' include Amazon, Apple, and Google. The most commonly used platforms that provide file storage and synchronization services are OneDrive, Google

44 Sören Preibusch, Joseph Bonneau, „The Privacy Landscape: Product Differentiation on Data Collection", [in:] *Economics of Information Security and Privacy III*, ed. Bruce Schneier (New York: Springer, 2013), 263-283; Ramon Casadesus-Masanell, Andres Hervas-Drane, „Competing with Privacy" *Management Science*, No. 1 (2015): 229-246.

45 Beatriz Kira, Vikram Sinha, Sharmadha Srinivasan, „Regulating Digital Ecosystems: Bridging the Gap between Competition Policy and Data Protection" *Industrial and Corporate Change*, No. 5 (2021): 1337-1360, https://doi.org/10.1093/icc/dtab053.

Drive, Dropbox, and Amazon Drive. These digital platforms offer many benefits but may gain control over the data of both consumers and entrepreneurs, which provides them a competitive advantage in the marketplace. During the coronavirus pandemic, as the use of cloud disks became even more common, there were concerns about violating fair competition. Antitrust law is not aligned with the regulation of the IT industry and data protection. Nevertheless, more and more attention is paid to the regulation of digital platforms.

The dominant platforms enjoy the benefits of obtaining such large data sets, including trade secrets, and control over this data, creating, in turn, large barriers to entry for potential competitors. For example, Google may use users' search data to improve search engine algorithms, while new entrants do not have this advantage. Entering a market and obtaining comparably huge amounts of data relative to the big players is a serious challenge for new entrants in a market, and many may eventually be taken over by one of the dominant platforms. Huge amounts of data obtained by service providers during the pandemic as a result of, inter alia, the functioning of tracking applications, remote work, and education significantly strengthened the dominant position of a small group of a few global corporations. Monopolization in the digital economy can harm not only economies but also society and democracy[46]. Competition authorities in developed and developing countries should consider this action and respond if necessary. Digitization will continue and will penetrate all sectors of the economy. As digital platforms are global, cooperation between competition authorities at the regional and international levels is essential. This is essential to meet the challenges of the digital economy and the negative impacts that can arise from the use of digital platforms by entrepreneurs.

4.2. Competition law in a pandemic world

The pandemic has proved that the antitrust framework must be adapted to the new digital challenges. The rapid pace of technological development has changed the nature of markets and business models. The challenges competition law needs to be adapted to new market realities and business models[47]. It is crucial to ensure fair competition and a properly functioning competitive market.

---

46 United Nations Conference on Trade and Development, Geneva, 10–12 July 2019, Competition issues in the digital economy. https://unctad.org/meetings/en/SessionalDocuments/ciclpd54_en.pdf. [accessed: 29.12.2022].

47 Michael Jacobides, Maartin Bruncko, Rene Langen. *Regulating Big Tech in Europe: why, so what, and how understanding their business models*

Table 1. Relationship between data protection and competition

	Positive competitive outcomes	Negative competitive outcomes
Positive data protection outcomes	Companies compete on data protection, and the extent to which companies protect users' data can be a competitive advantage. There are incentives for companies to invest in products and policies that offer greater levels of protection to users' data (e.g. privacy by design)	Lack of data can prevent companies from building a critical database or from offering goods and services at competitive levels. This makes these companies less likely to survive in data-driven markets, leading to a decrease in competition
Negative data protection outcomes	In competitive markets, companies compete fiercely for data, employing invasive techniques to gather large amounts of users' data. However, this information can be used to improve the quality and efficiency of goods and services, leading to a drop in costs	Intrusive data collection techniques might lead to data concentration. Data monopolies have fewer incentives to compete on privacy and are able to use market power in new anticompetitive ways. Data concentration can also increase the risks of surveillance and security breaches

Table 1. Relationship between data protection and competition (Kira, Sinha, Srinivasan, „Regulating digital ecosystems", 1337-1360).

The pandemic has shown that a new approach to competition research is needed, including a focus on the anti-competitive effects of platforms gaining control of collected data. A change to competition law appears desirable, given the relationship between market share and control over the data collected, including trade secrets. Adopting such an approach to digital platforms that focuses on barriers to entry, conflicts of interest, data use, and control is essential. Access to and control of data is critical and provides market power, and network effects further enhance this function[48].

and ecosystems can make a difference (London: London Business School, 2020). https://ssrn.com/abstract=3765324. [accessed: 30.12.2022].

48 Michal Gal, Oshrit Aviv, „The Unintended Competitive Consequences of the GDPR" *Journal of Competition Law and Economics*, No. 3 (2020): 349-391; Michael Jacobides, Martin Bruncko, Rene Langen, *Regulating Big Tech in Europe: why, so what, and how understanding their business models and ecosystems can make a difference* (London: London Business School, 2020). https://ssrn.com/abstract=3765324. [accessed: 14.12.2022].
Damien Geradin „What is a Digital Gatekeeper? Which Platforms Should be Captured by the EC Proposal for a Digital Market Act?", 18 February 2021. 10.2139/ssrn.3788152. [accessed: 14.11.2022]. Michael Jacobides Ioannis Lianos, „Ecosystems and competition law in theory

Platforms with a dominant position are constantly expanding their activities, which further increases their ability to collect more data, including trade secrets, all of which increase their dominant position. Such a situation may lead to serious abuses, such as the cloning of companies. In the digital economy, data collection and processing are closely related to economic activity that is very important to competition. Access to data, primarily in the case of online platforms and networks, is an important factor in market dominance. It is essential to ensure that the specificities of digital platforms are reflected in competition law and taken into account in competition law enforcement. Competition law and its enforcement must take into account both consumer/business protection and data protection. These areas have become more interconnected due to the market power they acquired data provides to digital platforms, including the trade secrets of potential competitors. It is also worth reconsidering the approach to the abuse of dominant positions in the data-driven digital economy and creating a stimulus for data-sharing business models[49]. There are even more concerns about the abuse of a dominant position by a few owners of key platforms, the scope of their control over the obtained data, and possible damage to consumers, entrepreneurs, and the entire society. Some platforms are dominant, and their services are difficult to replace.

---

and practice" *Centre for Law, Economics and Society. Research* Paper, No. 1 (2021). https://www.ucl.ac.uk/cles/sites/cles/files/cles-1-2021.pdf. [accessed: 16.11.2022]. David S. Evans, „The Antitrust Economics of Two-sided Markets" *Yale Journal on Regulation*, No. 2 (2003): 325-381. doi: 10.2139/ssrn.332022. Maurice Stucke, Grunes Allen P., *Big Data and Competition Policy*. Oxford: Oxford University Press (2016). https://www.researchgate.net/publication/308970973_Big_Data_and_Competition_Policy.

49 Graef Inge, Thomas Tombal, Alexandre De Streel, „Limits and Enablers of Data Sharing. An Analytical Framework for EU Competition, Data Protection and Consumer Law" *TILEC Discussion Paper* (2021); Thomas Tombal, „GDPR as shield to a data sharing remedy", [w:] *Deep Diving into Data Protection: 1979–2019: Celebrating 40 Years of Research on Privacy Data Protection at the CRIDS* (Brussels: Larcier, 2019), 67-93; Jenny Frédéric, „Competition Law Enforcement and Regulation for Digital Platforms and Ecosystems: Understanding the Issues, Facing the Challenges and Moving Forward" *Industrial and Corporate Change*, No. 5 (2021): 38-62; Darryl Biggar, Alberto Heimler, „Digital platforms and the transactions cost approach to competition law, [Digital platforms inquiry: Final report, Technical report, Australian Competition and Consumer Commission]" *Industrial and Corporate Change*, No. 5 (2021): 1230-1258.

5. Discussion

The COVID-19 pandemic popularized new digital surveillance technologies, such as facial recognition and cell phone location tracking, to monitor citizens' traffic and track infected populations in real-time. Unfortunately, it is unclear how these systems are useful in containing the spread of COVID-19. Ethical issues related to using digital surveillance technologies and examining the boundary between necessary supervision and the protection of personal data constitute separate research areas[50]. Currently, individual tracking applications are being analyzed for compliance with the requirements resulting from legal regulations in personal data protection. Considering the fact that tracking applications implemented in EU Member States should comply with the regulations at the EU level in the field of personal data protection, the question arises as to whether it might be advisable to develop one application, fully compliant with legal regulations, which would be implemented in all EU countries. This would avoid doubts about the scope of the fulfilled data protection requirements. It is essential to explore the legal boundary between protecting public health and protecting personal data and privacy.

The 2020 Sustainable Development Goals report contains information showing that progress was uneven before the COVID-19 pandemic and that it was unlikely that the goals would be achieved by 2030[51]. Now, because of the health crisis, it has become even more difficult to achieve these goals. In view of this change, it is necessary to adapt the legal regulations to the

50 Urs Gasser, Marcello Ienca, James Scheibner, Joanna Sleigh, Effy Vayena, „Digital Tools Against COVID-19: Taxonomy, Ethical Challenges, and Navigation Aid" *Lancet Digit Health*, No. 8 (2020): e425–e434. doi: 10.1016/S2589-7500(20)30137-0; Bernard Lo, Ida Sim, „ Ethical Framework for Assessing Manual and Digital Contact Tracing for COVID-19" *Annals of Internal Medicine*, No. 3 (2021): 395-400. doi: 10.7326/M20-5834; Robert Ranisch, Niels Nijsingh, Angela van Ballantyne, Anne van Bergen, Alena Buyx, Orsolya Friedrich, Tereza Hendl, Georg Marckmann, Christian Munthe, Verina Wild, „ Digital Contact Tracing and Exposure Notification: Ethical Guidance for Trustworthy Pandemic Management" *Ethics and Information of Technology*, (2020): 1-10. doi: 10.1007/s10676-020-09566-8; Federica Lucivero, Nina Hallowell, Stephanie Johnson, Barbara Prainsack, Gabrielle Samuel, Tamar Sharon, „COVID-19 and Contact Tracing Apps: Ethical Challenges for a Social Experiment on a Global Scale" *Journal of Bioethical Inquiry*, No. 4 (2020): 835-839. doi: 10.1007/s11673-020-10016-9.

51 The Sustainable Development Goals Report 2020, https://unstats.un.org/sdgs/report/2020/The-Sustainable-Development-Goals-Report-2020.pdf. [accessed: 26.12.2022].

new reality so that each country achieves the best possible results in terms of sustainable development, including environmental protection.

Although the pandemic has shown that we need fewer things, some new technology platforms that creatively address our needs when locked at home also entail serious threats. Trade secrets are of great value to entrepreneurs because they convey a competitive advantage over others. Due to the fact that entrepreneurs more and more often use the services of platforms that have access to their trade secrets and other data, it seems necessary to research how to secure the interests of the owners of these secrets and how to establish control mechanisms that prevent abuse by any platform owners privy to them.

6. Conclusion

The implementation of new technologies is a catalyst for more effective business. However, an appropriate level of protection of personal data and trade secrets would increase the level of trust and would encourage the wider use of tracking applications and cloud disk services. This trust should also improve the quality of the data collected, with users being more willing to provide complete and accurate information without fearing its unlawful use. The legal framework in operation in this regard seems to encourage the development of applications to protect privacy. In the present COVID-19 pandemic, the aim should be to use technology to provide truly effective measures to combat the spread of the virus and disease while ensuring adequate privacy protection. Experiences from the COVID-19 crisis are likely to accelerate efforts to achieve the SDGs after the pandemic ends. The pandemic has shown that effective and ethically acceptable global health security is only possible when sustainability is taken into account. Management of environmental issues means planning, coordinating, monitoring, and improving activities related to environmental protection based on the obligations resulting from legal regulations. Transformation towards such an economy poses specific challenges for producers, creators of innovative technology and business solutions, and bodies implementing regulations and legal solutions. Still, it will not be successful without the involvement of entrepreneurs, consumers, and relevant supervisory authorities.

In today's economy, access to data and how it is used determine one's competitive advantage and market success. Knowledge and information are key assets requiring special protection and safeguarding. This need applies to entrepreneurs as well as academic and research units. Adequate legal protection of trade secrets prevents unfair action on the part of competitors. Due to the development of new technologies and the functioning of data ecosystems, concluding even a 'good' contract is no longer sufficient. Further analysis of legal regulations regarding their adequacy to the technologies implemented will allow assessment of the extent to which EU regulations require change.

Bibliography

Agarwal Yuvraj, Michael Hall, „Protect My Privacy: Detecting and Mitigating Privacy Leaks on iOS Devices Using Crowdsourcing", [w:] *Proceedings of the 11th Annual International Conference on Mobile Systems, Applications, and Services*. Taipei, Taiwan, 2013.

Alamri Hamad, Carsten Maple, Mohamad Saad, Gregory Epiphaniou, *Do the Right Thing: A Privacy Policy Adherence Analysis of over Two Million Apps in Apple iOS App Store*. Basel: Sensors, 2022.

Anglemyer Andrew, Theresa Hm Moore, Lisa Parker, Timothy Chambers, Alice Grady, Kellia Chiu, Matthew Parry, Magdalena Wilczynska, Ella Flemyng, Lisa Bero, „Digital Contact Tracing Technologies in Epidemics: A Rapid Review" *Cochrane Database of Systematic Reviews*, No. 8 (2020): CD013699.

Balebako Rebecca, Jaeyeon Jung, Wei Lu, Faith Lorrie Cranor, Carolyn Nguyen, *Little Brothers Watching You Raising Awareness of Data Leaks on Smartphones*. Proceedings of the Ninth Symposium on Usable Privacy and Security; Newcastle, UK, 24-26 July 2013.

Banasiak Julia, „Application ProteGo Stop Covid – Could it have been an Opportunity to Prevent Covid-19 Spreading?" *Political Preferences*, No. 29 (2021): 47-59.

Bardus Marco, Melodie Al Daccache, Noel Maalouf, Rayan Al Sarih, Imad H Elhajj, „Data Management and Privacy Policy of COVID-19 Contact-Tracing Apps: Systematic Review and Content Analysis" *JMIR Mhealth Uhealth*, No. 7 (2022): e35195.

Beccia Flavia, Andrea Di Pilla, Francesco Andrea Causio, Bruno Federico, Maria Lucia Specchia, Carlo Favaretti, Stefania Boccia, Gianfranco Damiani, „Narrative Review of the COVID-19 Pandemic's First Two Years in Italy" *International Journal of Environmental Research Public Health*, No. 19 (2022): 15443.

Bennett Belinda, „Legal Rights During Pandemics: Federalism, Rights and Public Health Laws – a View from Australia" *Public Health* (2006): 232-236.

Blom Annelies G., Alexander Wenz, Carina Cornesse, Tobias Rettig, Marina Fikel, Sabine Friedel, Katja Möhring, Elias Naumann, Maximiliane Reifenscheid, Ulrich Krieger, „Barriers to the Large-scale Adoption of a COVID-19 Contact Tracing App in Germany: Survey Study" *Journal of Medical Internet Research*, No. 3 (2021): e23362.

Botta Marco, Klaus Wiedemann, „The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey" *The Antitrust Bulletin*, No. 3 (2019): 428-446.

Bradford Laura, Mateo Aboy, Kathleen Liddell, „COVID-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR, and Data Protection Regimes" *Journal of Law and the Biosciences*, No. 1 (2020): 1021.

Buhr Lorina, Silke Schicktanz, Eike Nordmeyer, „Attitudes Toward Mobile Apps for Pandemic Research Among Smartphone Users in Germany: National Survey" *JMIR Mhealth Uhealth*, No. 1 (2022): e31857.

Burns Jacob, Ani Movsisyan, Jan M. Stratil, Renke Lars Biallas, Michaela Coenen, Karl Mf Emmert-Fees, Karin Geffert, Sabine Hoffmann, Olaf Horstick, Michael Laxy, Carmen Klinger, Suzie Kratzer, Tim Litwin, Susan Norris, Lisa M. Pfadenhauer, Peter von Philipsborn, Kerstin Sell, Julia Stadelmaier, Ben Verboom, Stephan Voss, Katharina Wabnitz, Eva Rehfuess, „International Travel-related Control Measures to Contain the COVID-19 Pandemic: A Rapid Review" *Cochrane Database of Systematic Reviews*, No. 3 (2021): CD013717.

Caligiuri Paula, Helen De Cieri, Dana Minbaeva, Alain Verbeke, Angelika Zimmermann, „International HRM Insights for Navigating the COVID-19 Pandemic: Implications for Future Research and Practice" *Journal of International Business Studies* (2020).

Casadesus-Masanell Ramon, Andres Hervas-Drane, „Competing with Privacy" *Management Science*, No. 1 (2015): 229-246.

Chang Ji E, Alden Yuanhong Lai, Avni Gupta, Ann M. Nguyen, Carolyn A. Berry, Donna R. Shelley, „Rapid Transition to Telehealth and the Digital Divide: Implications for Primary Care Access and Equity in a Post-COVID Era" *Milbank Quarterly*, No. 2 (2021): 340-368.

Cohen Glenn, Lawrence O. Gostin, Daniel J. Weitzner, „Digital Smartphone Tracking for COVID-19: Public Health and Civil Liberties in Tension" *JAMA*, No. 23 (2020): 2371-2372.

Cohen Glenn, Sara Gerke, Daniel B. Kramer, „Ethical and Legal Implications of Remote Monitoring of Medical Devices" *Milbank Quarterly*, No. 4 (2020): 1257.

Costa-Cabral Francisco, Orla Lynskey, „Family Ties: The Intersection Between Data Protection and Competition in EU law" *Common Market Law Review*, No.1 (2017): 11-50.

Davison Robert M., „The transformative potential of disruptions: A viewpoint" *International Journal of Information Management* (2020): 226.

Downes John, Jordan Goodman, *Dictionary of Finance and Investment Terms*. NY: Deakin University, 1991.

El-Sadr Wafaa M., Joey Platt, Melanie Bernitz, Melissa Reyes, „Contact Tracing: Barriers and Facilitators" *American Journal of Public Health*, No. 7 (2021): 1025-1033.

Elkhodr Mahmoud, Omar Mubin, Zainab Iftikhar, Maleeha Masood, Belal Alsinglawi, Suleman Shahid, Fady Alnajjar, „Technology, Privacy, and User Opinions of COVID-19 Mobile Apps for Contact Tracing:

Systematic Search and Content Analysis" *Journal of Medical Internet Research*, No. 2 (2021): e23467.

Ellmann Stephan, Markus Maryschok, Oliver Schöffski, Martin Emmert, „The German COVID-19 Digital Contact Tracing App: A Socioeconomic Evaluation" *International Journal of Environmental Research Public Health*, No. 21 (2022): 14318.

Evans David S., „The Antitrust Economics of Two-sided Markets" *Yale Journal on Regulation*, No. 2 (2003): 325-381.

Frédéric Jenny, „Competition Law Enforcement and Regulation for Digital Platforms and Ecosystems: Understanding the Issues, Facing the Challenges and Moving Forward" *Industrial and Corporate Change*, No. 5 (2021): 38-62.

Gal Michal, Aviv Oshrit, „The Unintended Competitive Consequences of the GDPR" *Journal of Competition Law and Economics*, No. 3 (2020): 349-391.

Gasser Urs, Marcello Ienca, James Scheibner, Joanna Sleigh, Effy Vayena, „Digital Tools Against COVID-19: Taxonomy, Ethical Challenges, and Navigation Aid" *Lancet Digit Health*, No. 8 (2020): e425-e434.

Geradin Damien, *What is a Digital Gatekeeper? Which Platforms Should be Captured by the EC Proposal for a Digital Market Act?*. 18 February 2021.

Graef Inge, Thomas Tombal, Alexandre De Streel „Limits and Enablers of Data Sharing. An Analytical Framework for EU Competition, Data Protection, and Consumer Law" *TILEC Discussion Paper* (2019).

Graef Inge, Damian Clifford, Peggy Valcke, „Fairness and Enforcement: Bridging Competition, Data Protection, and Consumer Law" *International Data Privacy Law*, No. 3 (2018): 200-223.

Hatamian Majid, Samuel Wairimu, Nurul Momen, Lothar Fritsch, „A Privacy and Security Analysis of Early-deployed COVID-19 Contact Tracing Android Apps" *Empirical Software Engineering*, No. 26 (2021): 36.

Heinsohn Torben, Berit Lange, Patrizio Vanella, Isti Rodiah, Stephan Glöckner, Alexander Joachim, Dennis Becker, Tobias Brändle, Stefan Dhein, Stefan Ehehalt, Mira Fries, Annette Galante-Gottschalk, Stefanie Jehnichen, Sarah Kolkmann, Annelene Kossow, Martin Hellmich, Jörg Dötsch, Gérard Krause, „Infection and Transmission Risks of COVID-19 in Schools and their Contribution to Population Infections in Germany: A Retrospective Observational Study Using Nationwide and Regional Health and Education Agency Notification data" *PLOS Medicine*, No. 12 (2022): e1003913.

Hines J., *HR & Digital Trends. The Workplace after COVID-19: What is Your New Normal?*. 2020.

Horstmann Kai T., Susanne Buecker, Julia Krasko, Sarah Kritzler, Sophia Terwiel, „Who does or does not Use the »Corona-Warn-App« and Why" *European Journal of Public Health*, No. 1 (2021): 49-51.

Jacobides Michael, Martin Bruncko, Rene Langen, *Regulating Big Tech in Europe: Why, so what, and how Understanding Their Business Models and Ecosystems can Make a Difference*. London: London Business School, 2020.

Kahnbach Leonie, Dirk Lehr, Jessica Brandenburger, Tim Mallwitz, Sophie Jent, Sandy Hannibal, Burkhardt Funk, Monique Janneck, „Quality and Adoption of COVID-19 Tracing Apps and Recommendations for Development: Systematic Interdisciplinary Review of European Apps" *J Med* (2021): e27989.

Kemp Katherine, „Concealed Data Practices and Competition Law: Why Privacy Matters" *European Competition Journal*, No. 2-3 (2020): 628-672.

Kira Beatriz, Vikram Sinha, Sharmadha Srinivasan, „Regulating Digital Ecosystems: Bridging the Gap between Competition Policy and Data Protection" *Industrial and Corporate Change*, No. 5 (2021): 1337-1360.

Kleinman Robert A., Colin Merkel, „Digital Contact Tracing for COVID-19" *Canadian Medical Association Journal*, No. 24 (2020): E653--E656.

Knierim Kyle, Christina Palmer, Erik Seth Kramer, Rachel S. Rodriguez, Jill Van Wyk, Alison Shmerling, Peter Smith, Heather Holmstrom, Brian S. Bacak, Shandra M. Brown, Elizabeth W. Staton, Jodi Summers Holtrop, „Lessons Learned During COVID-19 That Can Move Telehealth in Primary Care Forward" *Journal of the American Board of Family Medicine*, 34(Suppl) (2021): 196-202.

Kolasa Katarzyna, Francesca Mazzi, Ewa Leszczuk-Czubkowska, Zsombor Zrubka, Márta Péntek, „State of the Art in Adoption of Contact Tracing Apps and Recommendations Regarding Privacy Protection and Public Health: Systematic Review" *MIR Mhealth Uhealth*, No. 6 (2021): e23250.

Li Hui, Yifel Zhu, Yi Niu, „Contact Tracing Research: A Literature Review Based on Scientific Collaboration Network" *International Journal of Environmental Research Public Health*, No. 15 (2022): 9311.

Lo Bernard, Ida Sim, „Ethical Framework for Assessing Manual and Digital Contact Tracing for COVID-19" *Annals of Internal Medicine*, No. 3 (2021): 395-400.

Lucivero Federica, Luca Marelli, Nora Hangel, Bettina Maria Zimmermann, Barbara Prainsack, Ilaria Galasso, Ruth Horn, Katharina Kieslich, Marjolein Lanzing, Elisa Lievevrouw, Fernandos Ongolly, Gabrielle Samuel, Tamar Sharon, Lotje Siffels, Emma Stendahl, Ine Van Hoyweghen, „Normative Positions towards COVID-19 Contact-tracing Apps: Findings from a Large-scale Qualitative Study in Nine European Countries" *Critical Public Health* (2021): 5-18.

Lucivero Federica, Nina Hallowell, Stephanie Johnson, Barbara Prainsack, Gabrielle Samuel, Tamar Sharon, „COVID-19 and Contact Tracing Apps: Ethical Challenges for a Social Experiment on a Global Scale" *Journal of Bioethical Inquiry*, No. 4 (2020): 835-839.

Martinez-Martin Nicole, Sarah Wieten, David Magnus, Mildred K. Cho, „Digital Contact Tracing, Privacy, and Public Health" *Hastings Center Report*, No. 3 (2020): 43-46.

Montanari Vergallo G., Simona Zaami, Enrico Marinelli, „The COVID-19 Pandemic and Contact Tracing Technologies, between Upholding the Right to Health and Personal Data Protection" *European Review for Medical and Pharmacological Sciences*, No. 5 (2021): 2449-2456.

Moritz, Esdar, Ursula Hübner, „Analyzing the Essential Attributes of Nationally Issued COVID-19 Contact Tracing Apps: Open-Source Intelligence Approach and Content Analysis" *JMIR Mhealth Uhealth*, No. 3 (2021): 1-14.

Nicholas Jennifer, Katie Shilton, Stephen M. Schueller, Elizabeth L. Gray, Mary J. Kwasny, David C. Mohr, „The Role of Data Type and Recipient in Individuals' Perspectives on Sharing Passively Collected Smartphone Data for Mental Health: Cross-sectional Questionnaire Study" *JMIR Mhealth Uhealth*, No. 4 (2019): e12578.

Nussbaumer-Streit Barbara, Verena Mayr, Andreea Iulia Dobrescu, Andrea Chapman, Emma Persad, Irma Klerings, Gernot Wagner, Uwe Siebert, Dominic Ledinger, Casey Zachariah, Gerald Gartlehner, „Quarantine Alone or in Combination with Other Public Health Measures to Control COVID-19: A Rapid Review" *Cochrane Database Systematic Reviews*, No. 9 (2020): CD013574.

O'Connell James, Manzar Abbas, Sarah Beecham, Jim Buckley, Muslim Chochlov, Brian Fitzgerald, Liam Glynn, Kevin Johnson, John Laffey, Bairbre McNicholas, Bashar Nuseibeh, Michael O'Callaghan, Ian O'Keeffe, Abdul Razzaq, Kaavya Rekanar, Ita Richardson, Andrew Simpkin, Cristiano Storni, Damyanka Tsvyatkova, Jane Walsh, Thomas Welsh, Derek O'Keeffe, „Best Practice Guidance for Digital Contact Tracing Apps: A Cross-disciplinary Review of the Literature" *JMIR Mhealth Uhealth*, No. 6 (2021): e27753.

Papageorgiou Achilleas, Michael Strigkos, Eugenia Politou, Efthimios Alepis, Agusti Solanas, Constantinos Patsakis, „Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice" *IEEE Access*, No. 6 (2018): 9390-9403.

Pratt Bridget, Michael Parker, Susan Bull, „Equitable Design and Use of Digital Surveillance Technologies During COVID-19: Norms and Concerns" *The Journal of Empirical Research on Human Research Ethics*, No. 5 (2022): 573-586.

Pratt Bridget, Susan Bull, „Equitable Data Sharing in Epidemics and Pandemics" *BMC Medical Ethics*, No. 1 (2021): 136.

Preibusch Sören, Joseph Bonneau, „The Privacy Landscape: Product Differentiation on Data Collection", [in:] *Economics of Information Security and Privacy III*, ed. Bruce Schneier. 263-283. Springer: New York, 2013.

Ranisch Robert, Niels Nijsingh, Angela van Ballantyne, Anne van Bergen, Alena Buyx, Orsolya Friedrich, Tereza Hendl, Georg Marckmann, Christian Munthe, Verina Wild, „Digital Contact Tracing and Exposure Notification: Ethical Guidance for Trustworthy Pandemic Management" *Ethics and Information of Technology*, (2020): 1-10.

Reyna Anthony, „The Psychology of Privacy – What can Behavioral Economics Contribute to Competition in Digital Markets?" *International Data Privacy Law*, No. 3 (2018): 240-252.

Schwartz Adam, Andrew Crocker, *Electronic Frontier Foundation. Governments Haven't Shown Location Surveillance Would Help Contain COVID-19*, 2020. https://www.eff.org/deeplinks/2020/03/governments-havent-shown-location-surveillance- would-help-contain-COVID-19.

Scrivano Noemi, Rosario Alfio Gulin, Daniele Giansanti, „Digital Contact Tracing and COVID-19: Design, Deployment, and Current Use in Italy" *Healthcare*, No. 1 (2021): 67.

Sharon Tamar, „Blind-sided by Privacy? Digital Contact Tracing, the Apple/Google API and Big Tech's Newfound Role as Global Health Policy Makers" *Ethics and Information Technology*, No. 23 (2020): 45-57. doi: 10.1007/s10676-020-09547-x.

Sheng Jie, Joseph Amankwah-Amoah, Zaheer Khan, Xiaojun Wang, „COVID-19 Pandemic in the New Era of Big Data Analytics: Methodological Innovations and Future Research Directions" *British Journal of Management*, No. 4 (2021): 1164-1183.

Sokol Daniel, Feng Zhu, „Harming Competition and Consumers under the Guise of Protecting Privacy: An Analysis of Apple's iOS 14 Policy Updates" *USC Law Legal Studies Paper* No. 21-27 (2021): 23-32.

Stucke Maurice E., Allen P. Grunes, *Big Data, and Competition Policy*. Oxford: Oxford University Press, 2016.

Tombal Thomas, „GDPR as shield to a data sharing remedy", [w:] *Deep Diving into Data Protection: 1979–2019: Celebrating 40 Years of Research on Privacy Data Protection at the CRIDS*. 67-93. Brussels: Larcier, 2019.

Ussai Silvia, Marco Pistis, Eduardo Missoni, Beatrice Formenti, Benedetta Armocida, Tatiana Pedrazzi, Francesco Castelli, Lorenzo Monasta, Baldassare Lauria, Ilaria Mariani, „»Immuni« and the National Health System: Lessons Learnt from the COVID-19 Digital Contact Tracing in Italy" *International Journal of Environmental Research Public Health*, No. 12 (2022): 7529.

Verbeemen Eva, Salvadore B. D'Amico, *Why Remote Working Will be the New Normal, Even after COVID-19*, 2020. https://www.ey.com/en_be/covid-19/why-remote- working-will-be-the-new-normal-even-after-covid-19.

Wachter Sandra, Brent Mittelstadt, „A Right to Reasonable Inferences: Rethinking Data Protection Law in the Age of Big Data and AI" *Columbia Business Law Review*, No. 2 (2019): 443-493.

Wei Ting Daniel Shu, Lawrence Carin, Victor Dzau, Tien Y. Wong, „Digital Technology and COVID-19" *Nature Medicine*, No. 26 (2020): 459-461.

Weill Peter, Sinan Aral, „Generating Premium Returns on Your IT Investments" *MIT Sloan Management Review*, No. 2 (2006): 39.

Weiß Bardus, Daccache Marco, Al. Melodie, Noel Maalouf, Rayan Al Sarih, Imad H. Elhajj, „Data Management and Privacy Policy of COVID-19 Contact-Tracing Apps: Systematic Review and Content Analysis" *JMIR Mhealth Uhealth*, No. 7 (2022): e35195.

Winter Michael, Harald Baumeister, Ulrich Frick, Miles Tallon, Manfred Reichert, Rudiger Pryss, *Exploring the Usability of the German COVID-19 Contact Tracing App in a Combined Eye Tracking and Retrospective Think Aloud Study*. Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2021.