MASARYK UNIVERSITY JOURNAL OF LAW AND TECHNOLOGY

VOLUME **19** | NUMBER **1** | SUMMER **2025** | ISSN **1802-5943**

PEER REVIEWED



CONTENTS:

MORBEL | CARUANA | BORG | WISZNIEWSKA | BAGNATO | MÜLLER-TÖRÖK | PROSSER | STEIN

www.mujlt.law.muni.cz

Masaryk University Journal of Law and Technology
issued by Institute of Law and Technology
Faculty of Law, Masaryk University
www.mujlt.law.muni.cz

Editor-in-Chief
Jakub Harašta, Masaryk University, Brno

Deputy Editor-in-Chief
Ondřej Böhm, Masaryk University, Brno

Founding Editor
Radim Polčák, Masaryk University, Brno

Editorial Board
Tomáš Abelovský, Swiss Re, Zurich
Zsolt Balogh, Corvinus University, Budapest
Michael Bogdan, University of Lund
Joseph A. Cannataci, University of Malta | University of Groningen
Josef Donát, ROWAN LEGAL, Prague
Julia Hörnle, Queen Mary University of London
Josef Kotásek, Masaryk University, Brno
Leonhard Reis, University of Vienna
Naděžda Rozehnalová, Masaryk University, Brno
Vladimír Smejkal, Brno University of Technology
Martin Škop, Masaryk University, Brno
Dan Jerker B. Svantesson, Bond University, Gold Coast
Markéta Trimble, UNLV William S. Boyd School of Law
Andreas Wiebe, Georg-August-Universität Göttingen
Aleš Završnik, University of Ljubljana

Editors
Tina Mizerová, Andrej Krištofík

Official Partner (Czech Republic)
ROWAN LEGAL, advokátní kancelář s.r.o. (https://rowan.legal)
Na Pankráci 127, 14000 Praha 4

Subscriptions, Enquiries, Permissions
Institute of Law and Technology, Faculty of Law, MU (cyber.law.muni.cz)

listed in HeinOnline (www.heinonline.org)
listed in Scopus (www.scopus.com)
reg. no. MK ČR E 17653

MASARYK UNIVERSITY JOURNAL OF
LAW AND TECHNOLOGY

VOLUME **19** | NUMBER **1** | SUMMER **2025**

LIST OF ARTICLES

Fatma Ceren Morbel: Network Effects and the Dynamics of Digital Markets in the Data Economy……..**3**

Mireille Martine Caruana, Roxanne Meilak Borg: Assessing Pandemic Measures: The Impact of Digital Technologies on Fundamental Rights…..…….**27**

Joanna Wiszniewska: Influencer Marketing – Do We Need a New Law or a New Approach? Few Remarks From the European and Polish Perspective…..**57**

Domenica Bagnato, Robert Müller-Török, Alexander Prosser, Robert Stein: Evoting at the German Social Elections – Lessons Learnt……..….**75**

DOI 10.5817/MUJLT2025-1-1

NETWORK EFFECTS AND THE DYNAMICS OF DIGITAL MARKETS IN THE DATA ECONOMY

by

FATMA CEREN MORBEL *

With the advent of the digital age, data has become one of the most powerful tools shaping markets. The article examines how data is crucial for online platforms in gaining dominance, as well as several characteristics of online markets that play a role in competitiveness. Throughout the article, network effects, multi-sided markets, switching costs, and lock-in effects are discussed as examples of how these factors might affect innovation and restrict competition. The purpose of the article is to provide an overview of digital markets' challenges and highlights recent regulations intended to promote a competitive digital markets.

KEY WORDS

Data, Data Economy, Digital Markets, Network Effects, Competition Law

1. INTRODUCTION

Recent technological developments have revolutionised the markets and business models. Digital markets and platforms are of particular importance in this regard. As digital markets become more relevant and the economics behind them become more complex, competition law and authorities face new challenges. Network externalities might make markets highly concentrated. Therefore, such markets become less competitive if potential competitors face high barriers to entry due to structural disadvantages, compared to early market entrants. Several characteristics of online markets may allow for business practices that prevent fair competition.[1] The article aims to show the use of data in the digital age, along with the main

* Ph.D. Candidate, Faculty of Law, Károli Gáspár University of the Reformed Church, Budapest, Hungary, e-mail: fcerenmorbel@gmail.com

1 Brühl, V. (2023) Big Tech, the platform economy and the European digital markets. *Center for Financial Studies, CFS Working Paper Series*, 711, p. 3

characteristics of digital platforms and the problems they pose in the competitive environment. In this regard, Section 2 analyses the power of data after defining data and Big Data. Afterwards, Section 3 describes the main elements of online platforms and the problems associated with them, including multi-sidedness, network effects, economies of scale and scope, multi-homing, switching costs, and lock-in effects. Finally, Section 4 presents some current efforts to regulate digital markets and minimise online platform challenges as well as concerns regarding their success.

2. DEFINITION AND POWER OF DATA

Data has become more important than ever before, with the Economist referring to it as the new oil.[2]

The importance of data comes from the fact that it is not only collected and stored but also analysed and utilised. After companies discovered the value of data in the establishment of market power, they evolved their business models to emphasise the collection and use of data. Data refers to information that can be factual or digital in form and transmitted or processed, as well as information generated by a sensing device or organ that includes useful and redundant information and which must be processed to provide information that is meaningful. Data can be used to detect someone's behaviours, wishes, traits etc. This type of data is considered personal data, which is protected by data protection laws that set limits on the collection and usage of that data to ensure the privacy of consumers and users. Specifically, personal data is any information pertaining to a data subject. Examples of personal data include names and surnames, home addresses, e-mail addresses, an Internet Protocol (IP) address, and a cookie ID. However, it is not considered personal data if the data has been anonymised in such a way that it no longer identifies the individual.[3]

It is possible to categorise data as quantitative or qualitative, depending on the answer to the question, "how much/many" and "why". Quantitative data refers to statistical data that is expressed in numbers and values, and is therefore more easily processed and suitable for commercial use. However, qualitative data does not possess a statistical structure and is either unstructured or semi-structured in nature. Hence, it cannot be processed

[2] The Economist. (2017) *The world's most valuable resource is no longer oil, but data*. [online] London Available from: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data [Accessed 12 March 2025]

[3] European Commission. Data protection explained. Available from: https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en [Accessed 12 March 2025]

directly or easily by machine language, which means it requires an algorithm to make it profitable.

A data subject may provide voluntarily or the platform may infer a data subject's data using artificial intelligence, thus, data can be volunteered, observed or inferred. Users may provide voluntarily data through platforms they use, such as setting up an account on a website or sharing their personal data with an online shopping site. Observed data may be collected as a result of individuals' activities, such as tracking web users' browsing history or location data provided by mobile devices. Analysing observed data yields inferred data.[4]

Data collected by a company itself from its own sources is referred to as "first-party data". The company collects this data through its websites, apps, social media accounts or surveys. For instance, when a company collects information about its customers' demographics, purchase history and time spent on its website, all of this information is considered first-party data. However, if a company purchases data collected by another entity, it is considered third-party information. Contrary to first-party data, third-party data is not free. As well as collecting first-party data, companies can also buy third-party data for better efficiency.[5]

Big Data differs from data in that it has 5 Vs, including volume, velocity, value, variety and veracity. When most people think of Big Data, they think of the "Volume", which represents the enormous amount of data. "Velocity" refers to the rate at which this data is collected, processed, stored and analysed. "Variety" relates to all types of data generated by humans or machines; structured, semi-structured and unstructured. "Veracity" of the source data is the result of the data accuracy of analysis. As a final and most important aspect of Big Data, "Value" is what companies strive to achieve and in which they gain the market power.[6]

Data has become increasingly vital in recent years and it is not a myth that it can be utilised to gain an economic advantage and enhance an undertaking's position in the market. Analysis of data can be used by companies to better target users that may create an advantageous feedback loop, a mutually beneficial system that will make it possible for the company to gain access to a greater amount of data. As users demand more, the

[4] International Competition Network. (2024) Control of Data, Market Power, and Potential Competition in Merger Reviews. *Merger Working Group*, p. 17.

[5] European Data Protection Board. (2024) *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*. p. 11.

[6] Ishwarappa, K. and Anuradha, J. (2015) A Brief Introduction on Big Data 5Vs Characteristics and Hadoop Technology. *Procedia Computer Science*, 48, pp. 320-321.

company would be able to gather more data, improving user experiences and attracting more consumers.[7]

Refusal to access to data may be seen as anti-competitive if we consider data as an essential facility in terms of competition law. In addition to access to data, its accumulation can be a key indicator of a high entry barrier in a market, as well as the amount of data a company has that is likely to contribute to dominance. This is notably evident when a dominant company serves both as a marketplace and as a seller of its own products.[8]

A further anti-competitive scenario would be the use of algorithms to discriminate against prices. In many sectors, companies discriminate against customers and offer prices that reflect their willingness-to-pay for a specific product or service. As a result of data-based price discrimination, some consumers would pay higher prices, while others would pay lower prices. In light of this, it is difficult to assess the effects of price discrimination based on the facilitation of data.[9]

Through data, dominant firms can detect and acquire potential rivals early, before they become an actual threat. This strategy is often called "killer acquisitions", in which established firms purchase emerging competitors to eliminate future competition, rather than improving innovation and efficiency. These acquisitions are typically outside of the notification thresholds set by traditional merger control regimes, particularly those that rely on turnover as a key criteria. The enforcement authorities may be unable to identify these acquisitions as anti-competitive since they could lack access to this information or fail to comprehend its significance.[10] This creates an enforcement gap in the digital economy, as competitive threats are not always apparent in financial statements. Moreover, the merger of two companies that have already established strong positions in separate upstream and downstream markets may prevent new competitors from entering those markets.[11]

---

7 U.S. Subcommittee on Antitrust Commercial and Administrative Law of the Committee on the Judiciary. (2020) Investigation of Competition in Digital Markets. *Majority Staff Report and Recommendations*, p. 42.

8 Ibid.

9 Autorité de la concurrence, Bundeskartellamt. (2016) *Joint Paper on Data and Its Implications for Competition Law*. [press release] 10 May. p. 21. Available from: `https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/10_05_2016_Big\%20Data\%20Papier.html`

10 U.S. Subcommittee on Antitrust Commercial and Administrative Law of the Committee on the Judiciary. (2020) Investigation of Competition in Digital Markets. *Majority Staff Report and Recommendations*, p. 44.

11 Autorité de la concurrence, Bundeskartellamt. (2016) Joint Paper on Data and Its Implications for Competition Law. *Op. cit.* p. 17.

Lastly, massive collection of data can bring privacy and data protection concerns as firms can use market power to acquire more data from users to strengthen their position in the market.

3. CHARACTERISTICS OF DIGITAL PLATFORMS

Digital platforms are places where users are brought together for a particular purpose such as exchange of information, commercial transactions by a platform operator.[12]

Digital platforms can be described as digital services that facilitate communication between different but interdependent groups of users that can be firms or individuals via the Internet.[13] As Geradin and Katsifis point out, digital markets share certain economic characteristics, such as extreme returns to scale, network externalities, the importance of data and ecosystems, by emphasising that these characteristics are not unique to online platforms, but they are exhibited in such a manner that has never been seen before.[14] Even though these characteristics can be found in old industries, including electricity, gas and railway, new industries, including search engines, e-commerce platforms and social networks, are certainly likely to experience rapid change and disruptive innovation, resulting in the emergence of these features at an increasingly rapid rate.[15]

In this regard, this article examines the main characteristics of digital platforms, such as multi-sidedness, network effects, economies of scale and scope, single and multi-homing, switching costs, and lock-in effects.

3.1.MULTI-SIDED MARKETS AND AD-FUNDED BUSINESS MODEL

Multi-sided markets, or more specifically two-sided markets, are not new terms and can be seen even in newspapers where advertisers and readers interact.[16] In a two-sided market, two sets of agents interact through an intermediary or platform and their decisions have an impact on the outcomes of the other set of agents, usually due to externalities.[17]

---

[12] European Commission (2016a). *Communication Online Platforms and the Digital Single Market Opportunities and Challenges for Europe*, 25 May 2016, COM(2016) 288 final.

[13] OECD. (2019) *An Introduction to Online Platforms and Their Role in the Digital Transformation*. p. 21.

[14] Geradin, D. and Katsifis, D. (2022) Strengthening effective antitrust enforcement in digital platform markets. *European Competition Journal*, 18 (2), p. 362.

[15] Graef, I. (2016) EU competition law, data protection and online platforms: Data as essential facility. *International Competition Law Series, Kluwer Law International*, 68, p. 43.

[16] Eriksson, C. I., Åkesson, M. and Lund, J. (2016) Designing Ubiquitous Media Services - Exploring the Two-Sided Market of Newspapers. *Journal of Theoretical and Applied Electronic Commerce Research*, 11 (3), pp. 1-19.

[17] Rysman, M. (2009) The Economics of Two-Sided Markets. *Journal of Economic Perspectives*, 23 (3), p. 125.

Accordingly, platform effects describe the feedback loops created by a platform when users produce value for other users, which attracts more users, who in turn produce more value, which attracts yet more users.[18] As there is no clear consensus on the definition of a two-sided market, and some definitions are rather broad, it may be difficult to show that a market is not two-sided. However, according to Rysman, markets with positive feedback loops would be two-sided under any definition.[19]

In the age of digitalisation, the nature of two-sided markets has not changed but evolved into digital platforms, such as Facebook. The German Competition Authority defined Facebook as a multi-sided market in its decision, expressing that "the service Facebook offers to its advertising customers becomes more attractive the more the quality and quantity of the data it provides to these customers increase."[20]

Despite Facebook being "free", as it is financed by advertising, in this instance, the currency is data rather than money. This model can be seen by the fact that users will see advertisements related to certain products when they like them. As long as users are active on Facebook, the platform collects more data about them. Since Facebook's strong user lock-in prevents users from easily multi-homing when family and friends use the platform as well, the platform creates a natural monopoly.

When data is being used as a currency, online platforms within an attention market can aim to capture as much attention as possible from users. In this manner, platforms can collect more personal data, enabling them to provide advertisers and users with more valuable services. However, platforms can also misuse personal data to gain more attention from individuals and to influence their thinking.[21]

On the basis of the above, even though some online platforms appear to be free, data is being exchanged for currency, and this can result in market disruptions.

---

[18] Van Alstyne, M. (2019) The opportunity and challenge of platforms, Platforms and Ecosystems: Enabling the Digital Economy Briefing Paper. *World Economic Forum*, p. 8.

[19] Rysman, M. (2007) The Empirics of Antitrust in Two-Sided Markets. *Competition Policy International Journal*, 3 (1), p. 198.

[20] Judgment of 23 June 2020, Facebook, KVR 69/19, ECLI:DE:BGH:2020:230620BKVR69.19.0, paragraph 43.

[21] Tóth, A. (2023) Strengthening of EU Regulatory Intervention Against Data Exploitations By Online Platforms with a Zero-Price Business Model. *Masaryk University Journal of Law and Technology*, 17 (1), p. 115.

3.2.NETWORK EFFECTS

Interrelation between customer groups often affects the demand for many products, that gives rise to network effects, that is one of the characteristics of online platforms. Network externatility or effect is defined by McKnight and Bailey as *"the benefit gained by incumbent users of a group when an additional user joins the group. The group can be thought of as a 'network' of users, hence the term network externality."*[22] According to Liebowitz and Margolis, the value that results from consumers' increased use of the product or service can be divided into two categories: its intrinsic value when used alone (autarky value) and the added value from interacting with other users (synchronisation value), with the latter being key to network effects.[23]

Network effects may appear advantageous to consumers since they increase the utility of their consumption through the synchronisation value, but they can also serve as a source of dominance for undertakings and a barrier to entry for new entrants.[24] This was also emphasised by the European Commission in *Whatsapp/Facebook* case as "The existence of network effects as such does not a priori indicate a competition problem in the market affected by a merger. Such effects may however raise competition concerns in particular if they allow the merged entity to foreclose competitors and make more difficult for competing providers to expand their customer base."[25]

Moreover, in 2021 Compendium of approaches to improving competition in digital markets it was stated that network effects may impact competition in several ways. Platform businesses may benefit from them and may invest and compete aggressively to acquire scale, or they may act as a deterrent to entry that insulates market power from competing firms.[26]

Based on the above, it is possible that network effects can have both beneficial and detrimental effects on competition. On the one hand, network effects may be beneficial to emerging market participants. For instance, a new entrant with an innovative feature or unique value proposition can attract a significant user base. As a result, it will be able to gain more users due

---

[22] McKnight, L. W. and Bailey, J. P. (eds.) (1997) Internet Economics. Cambridge: MIT Press, p. 6, note 3.

[23] Liebowitz, S. J. and Margolis, S. E. (2002) Network Externalities (Effects). In: Newman, P. (ed.) The New Palgrave Dictionary of Economics and the Law. London: Palgrave Macmillan.

[24] Graef, I. (2016) EU competition law, data protection and online platforms: Data as essential facility. *International Competition Law Series, Kluwer Law International*, 68, p. 44.

[25] COMISSION DECISION of 3 October 2014 declaring a concentration to be compatible with the common market, Facebook/WhatsApp, COMP/M.7217, paragraph 130

[26] G7 Competition Authorities (2021) *Compendium of approaches to improving competition in digital markets*. Available from: `https://assets.publishing.service.gov.uk/media/61d6cef9d3bf7f054798bbe5/Compendium_of_approachess_to_improving_competition_in_digital_markets_publication.pdf` [Accessed 12 March 2025].

to network effects. This can result in rapid growth of market share and enable challengers to disrupt established market players. Hence, network effects can facilitate competitive dynamics by helping new entrants to gain a competitive advantage quickly if they provide a unique advantage to the user. However, this dynamic can result in what is known as "tipping" which means the market shifts strongly in favor of one firm, possibly leading to long-term dominance.[27]

On the other hand, network effects can act as a barrier to entry, limiting competition by reinforcing established firms' dominance. As a company's user base expands, it gains access to more user data, which can be leveraged to enhance product or service quality. Providing an improved product and service will further attract users, creating a feedback loop that will strengthen the incumbent's position in the market. As a consequence, it would be difficult for new entrants to compete effectively.[28]

Network effects can be a a possible indicator of market power and act as significant barriers for new entrants. In these instances, network effects can raise switching costs, leading to consumer lock-in and limiting options for multi-homing strategies.[29] Although network effects may exist on one side of the market, they are not sufficient to demonstrate market power. Therefore, authorities should consider other factors that indicate market power in their market analysis.

3.2.1 Positive and Negative Network Effects

Network effects can be positive or negative depending on the circumstances. For instance, social media platforms can result in a positive network effect, as the value of a platform increases for each individual as more users join, since more people are available to connect with.

Belleflamme and Peitz illustrate negative network effects with the example of road congestion and traffic jams. In this case, as more drivers use a particular road at the same time, the traffic flow slows down, decreasing the overall benefit for each driver.[30] Similarly, advertisers can be subject to negative network effects on online platforms. Advertisers do not benefit from new advertisers. As additional advertisements are displayed, existing advertisers face greater competition for user attention, thereby reducing the

[27] Autorité de la concurrence, Bundeskartellamt. (2016) Joint Paper on Data and Its Implications for Competition Law. *Op. cit*. p. 28.

[28] Ibid.

[29] International Competition Network. (2024) Control of Data, Market Power, and Potential Competition in Merger Reviews. *Merger Working Group*, p. 47.

[30] Belleflamme, P. and Peitz, M. (2016) Platforms and Network Effects. *Working Paper Series*, 16-14, p. 2.

effectiveness of each advertisement. The platform may also raise prices as demand for ad space increases, which further increases costs for advertisers.[31] However, network effects may not be symmetrical since advertisers may suffer from increased advertising on the platform, but they may also benefit from an increase in users.[32]

3.2.2 Direct and Indirect Network Effects

In Katz and Shapiro's widely accepted definition of network effects, they state that: *"There are many products for which the utility that a user derives from consumption of the good increases with the number of other agents consuming the good."*[33] In the same paper, they also differentiate between direct and indirect network effects.

They explain that direct network effects occur when the quality of a product improves as more people purchase it, illustrating this with the example of a telephone, which becomes more valuable as more households and businesses join the telephone network. In our current age, direct network effects can be observed in social media platforms such as Facebook or Instagram, where as more users join these platforms, the value for each individual user increases as more people are available to interact with, follow and share content with.

This also creates a powerful growth cycle across digital platforms. In social media and messaging apps, the more people who join, the richer the experience becomes, as people are able to connect with a broader network of friends, colleagues or new contacts. Similarly, as search engines gain more users, their algorithms improve, producing better, more relevant results. Network effects can also enhance a platform's competitiveness, creating entry barriers for newcomers by increasing user loyalty and utility. However, these effects do not affect all platforms equally, for instance, dating apps can experience negative effects if growth becomes excessive and matching becomes less effective. As a result, positive direct network effects are critical for platforms aiming to scale quickly, since the continuous increase in users can lead to exponential growth and value.[34]

---

[31] Graef, I. (2016) EU competition law, data protection and online platforms: Data as essential facility. *International Competition Law Series, Kluwer Law International*, 68, p. 45.

[32] OECD (2017) *Network Effects and Efficiencies in Multisided Markets*. Shelanski, H., Knox, S. and Dhilla, A. Paris: OECD, p. 3.

[33] Katz, M. L. and Shapiro, C. (1985) Network Externalities, Competition, and Compatibility. *The American Economic Review*, 75 (3), pp. 424-440.

[34] OECD (2019) *An Introduction to Online Platforms and Their Role in the Digital Transformation*. Paris: OECD, p. 22. Available from: `https://doi.org/10.1787/53e5f593-en` [Accessed 12 March 2025].

On the other hand, indirect network effects arise when the value a consumer gains from a product or service grows as more people use compatible or complementary products.

Positive indirect network effects can be achieved by platforms in two-sided markets. When a platform provides better service for one side, it attracts more users to that side, which in turn increases the platform's appeal to the other user groups, creating a mutually reinforcing cycle of growth. This dynamic facilitates interaction between different user groups which benefit from each other's presence on the platform, thus solving a coordination problem. A platform with positive indirect network effects may be able to profit from this coordination.[35]

A computer operating system can be considered an example of indirect network effects since if only a few people use a given operating system, there would be a limited number of programs and applications developed for that operating system. However, as more users adopt the system, developers create more compatible software, which in turn attracts even more users. Also, in the case of marketplaces such as Amazon or eBay or app stores such as Google Play or AppStore, the number and identity of sellers and app developers affect the value of the platform.

In their paper, Evan and Schmalensee used YouTube as an example to show how indirect network effects can be effective for digital platforms since the platform did not succeed by being first to market. Instead, it navigated a challenging startup phase to identify effective strategies for encouraging users to upload and view videos, since users on the platform fulfill different roles, therefore, platforms can attract both types of users.[36]

Direct and indirect network effects can coexist in certain cases. For example, the value of a social network for an individual user grows as more people are involved (direct network effects). At the same time, a larger user base also increases network value for advertisers (indirect network effects).[37]

---

[35] OECD (2019) An Introduction to Online Platforms and Their Role in the Digital Transformation. *Op. cit.*

[36] Evans, D. and Schmalensee, R. (2017) Debunking the 'Network Effects' Bogeyman. *Regulation*, Winter 2017-2018, p. 38. Available from: `https://object.cato.org/sites/cato.org/files/serials/files/regulation/2017/12/regulation-v40n4-1.pdf?utm_source=Cato+Institute+E-mails&utm_campaign=9f32909490-regulation-winter-20172018&utm_medium=email&utm_term=0_395878584c-9f32909490-141199901&mc_cid=9f3` [Accessed 12 March 2025].

[37] Autorité de la concurrence, Bundeskartellamt. (2016) Joint Paper on Data and Its Implications for Competition Law. *Op. cit.* p. 27.

3.2.3 Scale and Scope Induced Network Effects

It is also possible to distinguish network effects as scale and scope induced. Scale-induced network effects result from increasing the value of a product or service as its production volume or user base increases, often resulting in lower costs and better service. An example of scale-induced network effects would be a ride-sharing service such as Uber, whose drivers are able to experience a better experience as the number of riders grows. Because of an increased number of users, the service becomes more efficient and appealing to both drivers and passengers. Moreover, as more users perform searches, a search engine such as Google is able to display more accurate and relevant search results, which enables it to collect and analyse more data. Likewise, the larger user base enables Google to target its advertising more precisely, which increases the platform's value and attracts additional advertisers.

In 2010, Microsoft and Yahoo! decided to merge their search operations in order to better compete with Google by taking advantage of scale-induced network effects.[38] Microsoft argued that the main purpose of optimising algorithmic relevance is to increase user engagement, which is aligned with the company's incentives to maximise paid advertisement revenue.[39] As a result of combining resources, user bases and datasets, both companies sought to improve the accuracy and relevance of their search results, thereby increasing the value of their services. The Commission also noted that the merger would allow the merging parties to provide greater relevance through greater scale.[40]

Scope-induced network effects occur when a business expands its range of offerings, products, or services, creating a broader ecosystem that adds value through diversity and complementarity. For instance, Google provides scope-induced network effects through its Google Search, Google Maps, Gmail and YouTube products. Users are attracted to each additional service, creating a network where the combined offerings are more valuable than individual services.

[38] COMISSION DECISION of 18 February 2010, Microsoft/Yahoo! Search Business, COMP/M.5727
[39] Ibid. para. 211.
[40] Ibid. para. 225.

3.3.COSTS AND ECONOMIES OF SCALE AND SCOPE

Besides network effects, digital markets can be described as having high fixed costs, low marginal costs.

Companies entering such markets often face substantial fixed costs related to research and development and the establishment of a network infrastructure to deliver products and services.[41] These upfront investments are essential for companies to establish themselves on the market, which requires advanced technological tools and reliable connectivity. However, once they are established, producing additional units or servicing more users has a relatively low incremental cost, often approaching zero.[42]

Microsoft's software development process is an example of high fixed costs and low marginal costs. For Microsoft to develop products such as Microsoft Word or Microsoft Excel, substantial investment must be made in both human resources and development efforts. These are the high fixed costs associated with the development of the software. However, once the software is developed and the code is written, additional copies can be produced and distributed at a low cost.[43]

Both economies of scale and economies of scope contribute to the competitive advantage of digital platforms. A company enjoys economies of scale in product production or distribution when its average costs fall as output increases.[44] On digital platforms, after the initial infrastructure is built, adding more units or serving additional users is relatively low-cost, allowing platforms to expand their user bases at a minimal cost. This scaling advantage, combined with network effects, enables platforms to grow rapidly. Platforms that offer multiple services or products are also subject to economies of scope. An economy of scope occurs when a firm produces two or more products that are cheaper to produce together than separately.[45] For instance, platforms such as Google and Amazon share data, infrastructure, and users across multiple services, making each additional service more cost-effective compared to providing each service on its own.

---

[41] Van Uytsel, S. and Uemura, Y. (2017) Competition Law Interference Prior to the Formation of a Digital Market: The JFTC's Enforcement Action Against DeNA. *SSRN*. Available from: http://dx.doi.org/10.2139/ssrn.3086449

[42] Ekingen, E. (2022) An Overview of the Concepts of 'Digital Economy' and 'Digital Markets' as Ongoing Trends in EU Competition Law. *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, 30 (4), p. 1947.

[43] Hovenkamp, H. (2017) Antitrust and Information Technologies. *Florida Law Review*, 68 (2), Article 9, p. 425.

[44] European Commission (n.d.) *Glossary of Terms Used in EU Competition Policy: Antitrust and Control of Concentrations*, p. 15.

[45] Ibid.

Combined with economies of scale, the low marginal cost advantage enables firms to scale efficiently, which is particularly advantageous in digital markets in which the costs of adding users or distributing additional units are minimal.[46]

In digital markets, economies of scale can create high barriers to entry, making it difficult for new companies to compete. Markets with increasing returns to scale tend to favour large firms since the cost per unit decreases with increasing output, which allows existing firms to dominate the market. Especially in digital markets, where high upfront fixed costs are required for infrastructure, research and development, these costs can serve as a barrier to entry for potential competitors.[47] Furthermore, established firms can become more competitive by adding more users and producing more units at a minimal cost, which makes it harder for new entrants to compete. Consequently, competition in such markets shifts from competition in the market to competition for the market, resulting in highly concentrated industries dominated by a few or a single company.[48]

3.4.SINGLE-HOMING AND MULTI-HOMING

Single-homing and multi-homing are two other characteristics of online platforms that are usually taken into account by competition authorities when describing market power.

The term "single-homing" refers to the use of only one single platform or network by users. Single-homing occurs when both users and providers of a platform market choose one platform exclusively.[49]

Business that sells an item that is unique and fits best on its own dedicated platform such as handmade items and artcrafts on Etsy is more likely to single-homing. Also, the majority of app developers are prone to single-homing, due to the complexity of developing apps for different platforms.[50]

On the other hand, "multi-homing" occurs when users use numerous platforms or networks on the market. Multi-homing on competing platforms is generally seen as a factor likely to reduce market power since it disrupts the self-reinforcing feedback loop effect by allowing users to use multiple

[46] Ekingen, E. (2022) An Overview of the Concepts of 'Digital Economy' and 'Digital Markets' as Ongoing Trends in EU Competition Law. *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, 30 (4), p. 1947.

[47] International Competition Network. (2024) Control of Data, Market Power, and Potential Competition in Merger Reviews. *Merger Working Group*, p. 53.

[48] Van Uytsel, S. and Uemura, Y. (2017) Competition Law Interference Prior to the Formation of a Digital Market: The JFTC's Enforcement Action Against DeNA. *Op. cit.*

[49] Bundeskartellamt (2016) *The Market Power of Platforms and Networks: Executive Summary*, p. 14.

[50] Barcevičius, E., Caturianas, D., Leming, A. and Skardžiūtė, G. (2021) Multi-homing: Obstacles, Opportunities, Facilitating Factors. *European Commission Analytical Paper*, 7, p. 8.

different platforms. In this way, network effects are less likely to lock-in users.[51]

Payment cards can be considered as an example of multi-homing in non-digital markets, which occurs when users engage with multiple platforms or networks. Many merchants accept various credit and debit card brands like Visa, Mastercard and American Express. Additionally, consumers tend to carry several payment cards even when they favour one payment card the most.[52]

According to Rysman, while some cardholders may concentrate their spending on a single card network, they maintain flexibility by holding cards from various networks. This allows consumers to easily switch between their preferred card networks if necessary.[53]

Furthermore, multi-homing can be seen in the online platforms where business users use several platforms to interact with their customers in order to provide goods, services, apps. For example, online travel agencies are a market type that multi-homing can be observed from the perspective of renters as they usually consider several options prior to making a reservation. Additionally, hotels and property owners can list their properties on multiple platforms so that renters can browse and reserve accommodations.[54]

Another most common example of multi-homing would be social media platforms. According to a report published in 2018 by the Pew Research Center, social media users are increasingly using multiple social media platforms. Based on the results of this survey, there is substantial overlap between social media users. For example, significant majority of users of social media platforms use both YouTube and Facebook, while about three-quarters of Twitter and Snapchat users indicate that they also use Instagram.[55]

---

[51] Bundeskartellamt (2016) *The Market Power of Platforms and Networks: Executive Summary*, p. 14.

[52] Evans, D. S. and Schmalensee, R. (2007) The Industrial Organization of Markets with Two-Sided Platforms. *Competition Policy International*, 3 (1), p. 166.

[53] Rysman, M. (2006) An Empirical Analysis of Payment Card Usage. *Boston University - Department of Economics - Working Papers Series*, p. 14.

[54] Barcevičius, E., Caturianas, D., Leming, A. and Skardžiūtė, G. (2021) Multi-homing: Obstacles, Opportunities, Facilitating Factors. *European Commission Analytical Paper*, 7, p. 8.

[55] Smith, A. and Anderson, M. (2018) *Social Media Use in 2018*. Pew Research Centre, pp. 1-4. Available from: `https://www.pewresearch.org/internet/2018/03/01/social-media-use-in-2018/` [Accessed 12 March 2025]

3.5.SWITCHING COSTS AND LOCK-IN EFFECTS

Another characteristics of digital platforms that affect market power are switching costs and lock-in effects. Switching costs can be defined as the costs associated with changing from one supplier to another, which can be monetary as well as non-monetary.[56] Switching costs refer to the expenses users incur when switching suppliers, such as information, learning or transaction costs, often influenced by existing suppliers' technological or commercial strategies.[57]

Although users wish to change products or services they use, switching costs will prevent them from making the switch. The more switching costs are incurred, the greater the degree of lock-in. Due to their ability to lock-in users, switching costs represent an effective barrier to entry for companies. Switching costs may eventually contribute to a more difficult entry into established markets, and result in reduced competition.[58]

A lock-in strategy might negatively impact society by preventing the adoption of more advanced technologies, as illustrated by the continued use of the QWERTY keyboard. Although the QWERTY layout was originally designed in the 1870s in order to slow down typists and prevent mechanical jams, it has remained dominant even after the Dvorak layout was introduced in 1932. Although Dvorak allows faster typing, high switching costs and the challenges of coordination at large have kept QWERTY in use, even with computer keyboards.[59]

A more recent example would be the switch between Apple and Google mobile device ecosystems, which could result in the loss of purchased apps and subscription-based services. Furthermore, switching may result in the loss of access to applications and hardware that are not interoperable, which will further reinforce a user's loyalty to a particular digital ecosystem.

As stated before, switching costs can also arise from the learning process. For instance, according to the survey conducted in 2022 by Competition Markets Authority ("CMA"), 31% of iOS Marginal Users and 21% of Android Marginal Users stated that they did not want to spend time learning how

---

[56] Hernandez Perez, A. and Gonzalez, A. (n.d.) Switching Costs. *Global Dictionary of Competition Law*, Concurrences, Art. N° 117837. Available from: `https://www.concurrences.com/en/dictionary/switching-costs` [Accessed 12 March 2025]

[57] Avgeropoulos, S. and Sammut-Bonnici, T. (2014) Switching Costs. In: *Wiley Encyclopedia of Management*. John Wiley & Sons. Available from: `https://www.researchgate.net/publication/272353027_Switching_Costs` [Accessed 12 March 2025]

[58] OECD (2022) *The Evolving Concept of Market Power in the Digital Economy – Background Note*, DAF/COMP(2022) 5 May, p. 16.

[59] Sammut-Bonnici, T. and McGee, J. (2002) Network Strategies for the New Economy. *European Business Journal*, pp. 183-184.

to use a new operating system as one of reasons why they did not switch device.[60]

The same challenge can be faced if a property owner rents through AirBnB and decides to switch platforms, as AirBnB will increase its fees and if the owner has a well-established reputation with AirBnB, it will be necessary for him or her to begin building a reputation on a new platform from the beginning.[61]

Aside from technical difficulties, users can encounter lock-in effects as a result of social factors. Even though Facebook accounts can be deactivated, it would be difficult for someone whose entire family and friends are currently active on the platform. This will result in users feeling as though they are locked into the platform.[62]

Similar social factors can be found in the situation where Whatsapp forced Turkish users to share their data with other Meta (formerly known as "Facebook") platforms, as in the famous Bundeskartellamt v. Meta case.[63] In January 2021, Whatsapp announced a change in its data privacy policy for end users in Turkey. When users opened the application, a pop-up message prompted them to approve this change by February 2021, in order to continue using the application. The new policy eliminated the option for users to choose not to share their Whatsapp account information with Meta, thus requiring the sharing of data. Following this move, there was a significant backlash, and users began considering alternative social communication apps like Signal, Telegram and BiP (Turkish alternative). However, lock-in effects hindered the switch. Due to Whatsapp's dominance and established network effects, switching to another platform was difficult.

Following the announcement of Whatsapp's new policy, the Turkish Competition Authority initiated an ex officio investigation into Meta and Whatsapp for the possible abuse of the dominant position. Whatsapp was also ordered to notify its Turkish users that its new policy would not be enforced as of February 2021, pending the outcome of the ongoing investigation at the Authority. As a result of Meta's substantial market share in consumer communications, social networking and online advertising

[60] CMA (n.d.) *Appendix D: Barriers to Switching Between Mobile Operating Systems*, p. 7. Available from: `https://assets.publishing.service.gov.uk/media/62a22d5bd3bf7f036750b0d8/Appendix_D__002_.pdf` [Accessed 12 March 2025]

[61] Hernandez Perez, A. and Gonzalez, A. (n.d.) Switching Costs. *Global Dictionary of Competition Law*, Concurrences, Art. N° 117837. Available from: `https://www.concurrences.com/en/dictionary/switching-costs` [Accessed 12 March 2025]

[62] Waller, S. W. (2012) Antitrust and Social Networking. *North Carolina Law Review*, 90 (5), p. 1789.

[63] Judgment of 4 July 2023, Meta Platforms Inc and Others v Bundeskartellamt, Case C-252/21, ECLI:EU:C:2023:537

sectors, the Authority has decided on 11 January 2021 that this may result in exploitative and exclusionary consequences, which could lead to irreparable harm to consumers. In May 2021, the Turkish Competition Authority announced that Whatsapp had informed them that the updated terms, under which user data could have been shared with other Meta companies, would not apply to Turkish users, even if they already agreed to them.[64]

Both examples demonstrate that most users would not choose a social networking platform solely based on functionality or privacy enhancements, but rather based on their family and friends' involvement in the platform, which causes switching costs and lock-in effects.

4. THE EU'S EFFORTS TO REGULATE DIGITAL PLATFORMS

As discussed in the previous chapter, online platforms are likely to pose significant risks by distorting competition and stifling innovation as a result of their characteristics. Therefore, the EU's recent effort to address these concerns is the Digital Markets Act ("DMA"), which was entered into force in 2022 and became effective in May 2023, thus making it relatively new.[65]

The main aims of the DMA are "contestability" and "fairness". In order to achieve these objectives, the DMA introduces a number of measures aimed at addressing the challenges posed by dominant online platforms who are deemed as "gatekeepers" in the DMA, especially those that leverage strong network effects and have entrenched market positions. For instance, the DMA has a measure relating to multi-homing that ensures that users and businesses can connect to multiple platforms at the same time, thereby minimising lock-in effects and increasing competition. Additionally, interoperability encourages large platforms to make their services compatible with competitors, fostering innovation and consumer choice. Through the DMA, measures are intended to mitigate digital platforms' anti-competitive characteristics and their exclusionary effects, in an effort to make digital markets more fair and contestable.

[64] Paksoy (2021) *Client Briefing*. Available from: https://paksoy.av.tr/en/2021/06/whatsapp-notifies-turkish-competition-authority-that-new-conditions-on-user-data-sharing-will-not-apply-in-turkey/ [Accessed 12 March 2025]

[65] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

Along with the DMA, the Digital Services Act ("DSA") is a key element of the Digital Strategy and the Digital Decade policy programme 2030.[66] The DSA, which came into force in 2022 and became effective in 2024, sets out clear guidelines and obligations for online platforms in order to ensure a secure, credible and reliable environment for online services.[67]

The DMA and DSA are landmark efforts taken by the EU to regulate digital markets and constrain gatekeeper power, but questions remain regarding whether they are sufficient to address network effects. Due to the DMA's focus on specific anti-competitive acts based largely on prior competition law cases, such as self-preferencing, which was central to the EU's enforcement actions against Google[68], it mostly offers behavioural remedies rather than structural ones.

Abuse of dominance remedies fall into two categories: behavioural and structural. Through behavioural remedies, dominant businesses are required to cease certain practices or take affirmative steps, such as combining data or enabling interoperability. On the other hand, structural remedies are forms of intervention that directly impact and alter market structures. As a result, they may intervene in the undertaking by requiring the divestiture of specific assets or business units.[69]

Although the DMA focuses primarily on behavioural remedies, structural remedies are designated as a last resort under Article 18. Thus, the DMA may not be able to significantly disrupt self-reinforcing network effects and ecosystem lock-ins that entrench gatekeeper power.

Also, the European Commission's decision to designate ByteDance, the operator of TikTok, as a gatekeeper under the DMA brought concerns regarding the coherence and proportionality of gatekeeper designations under the DMA. ByteDance challenged this designation before the General Court, seeking interim measures to suspend the obligations. According to ByteDance, TikTok lacks the entrenched network effects and ecosystem lock-in typically associated with gatekeeper status, and users engage in

[66] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)

[67] Brühl, V. (2023) Big Tech, the platform economy and the European digital markets. *Center for Financial Studies, CFS Working Paper Series*, 711, p. 4.

[68] COMMISSION DECISION of 27.6.2017 relating to proceedings under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the Agreement on the European Economic Area (AT.39740 - Google Search (Shopping). *Official Journal of the European Union* (C(2017) 4444) 27 June. Available from: `https://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_14996_3.pdf`

[69] Mandrescu, D. (2024) Designing (restorative) remedies for abuses of dominance by online platforms. *Journal of Antitrust Enforcement*, p. 9.

multi-homing across platforms. It further emphasised the platform's limited role as a critical gateway for business users.[70]

Nevertheless, the General Court upheld the Commission's designation, clarifying that in the absence of long-standing dominance, a platform may qualify as a gatekeeper under the DMA if it meets the quantitative thresholds and exhibits characteristics that justify qualitative assessment. As a result, the Court appeared to adopt a proactive approach, accepting that TikTok's fast growth and potential market influence were suitable grounds for regulatory analysis.[71] Consequently, it appears to suggest a broad and flexible interpretation of the DMA's designation framework that may raise questions regarding the clarity of the gatekeeper concept.

As a result, the DMA and the DSA represent major developments in digital regulation, but their ultimate success in reducing network effects and enabling sustainable market competition may depend on greater legal clarity.

5. CONCLUSION

In the digital economy, data has become a crucial source of power which empowers those who control it. Because digital platforms possess unique characteristics, they often create complex market dynamics that reinforce dominance and limit competition. Network effects, which result in a platform becoming more valuable as more users join, give established players such as "GAMAM" (namely Google, Amazon, Meta, Apple and Microsoft) an advantage in attracting users, making it difficult for new competitors to compete. Additionally, users and businesses are discouraged from leaving dominant platforms due to high switching costs and lock-in effects. For example, App Store and Play Store impose restrictions that make it difficult for developers to distribute their apps outside of these ecosystems. The problem often results in fewer consumer choices, reduced innovation and an imbalance in the digital market as a result.

Because of the challenges presented by these platforms, more effective regulation has become necessary to ensure a more contestable and fair environment in the digital economy. The DMA and the DSA can be viewed as an effort to address these challenges and reduce their network effects.

Although the DMA and the DSA are a significant evolution in the EU's digital regulatory approach, they are complementary instruments rather than serving as the sole solution. Achieving success depends not only on

[70] Judgement of 17 July 2024, ByteDance v Commission, T-1077/23, ECLI:EU:T:2024:478

[71] Court of Justice Of the European Union (2024). *Judgment of the General Court in Case T-1077/23 Bytedance v Commission*, 114/24, [Press Release] 17 July 2024. Available from: https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-07/cp240114en.pdf

enforcement, but also on whether EU institutions and courts are prepared to engage in an ambitious agenda that directly addresses the economic infrastructures that enable dominance. Thus, these efforts should be read in conjunction with other tools that focus on merger control, data sharing, and economic analysis. Even though the DMA aims to facilitate enforcement by limiting economic analysis, it will still be useful for the designation process and effective evaluation.[72]

LIST OF REFERENCES

[1] Autorité de la concurrence, Bundeskartellamt. (2016) Joint Paper on Data and Its Implications for Competition Law. [press release] 10 May. p. 21. Available from: https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/10_05_2016_Big\%20Data\%20Papier.htmlpp.21-28.

[2] Avgeropoulos, S. and Sammut-Bonnici, T. (2014) Switching Costs. In: *Wiley Encyclopedia of Management*. John Wiley & Sons. Available from: https://www.researchgate.net/publication/272353027_Switching_Costs [Accessed 12 March 2025].

[3] Barcevičius, E., Caturianas, D., Leming, A. and Skardžiūtė, G. (2021) Multi-homing: Obstacles, Opportunities, Facilitating Factors. *European Commission Analytical Paper*, 7, p. 8.

[4] Belleflamme, P. and Peitz, M. (2016) Platforms and Network Effects. *Working Paper Series*, 16-14, p. 2.

[5] Brühl, V. (2023) Big Tech, the platform economy and the European digital markets. *Center for Financial Studies, CFS Working Paper Series*, 711, pp. 3-4.

[6] Bundeskartellamt (2016) *The Market Power of Platforms and Networks: Executive Summary*, p. 14.

[7] COMMISSION DECISION of 27 June 2017 relating to proceedings under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the Agreement on the European Economic Area (AT.39740 - Google Search (Shopping). *Official Journal of the European Union* (C(2017) 4444) 27 June. Available from: https://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_14996_3.pdf

[8] Judgement of 17 July 2024, ByteDance v Commission, T-1077/23, ECLI:EU:T:2024:478.

[9] CMA (n.d.) *Appendix D: Barriers to Switching Between Mobile Operating Systems*, p. 7. Available from: https://assets.publishing.service.

[72] Guimarães, G. (2024) A comment on ByteDance v Commission: the General Court's take on gatekeeper designation. *JusGov Research Paper Series*, p. 10.

gov.uk/media/62a22d5bd3bf7f036750b0d8/Appendix_D__002_.pdf [Accessed 12 March 2025].

[10] Ekingen, E. (2022) An Overview of the Concepts of 'Digital Economy' and 'Digital Markets' as Ongoing Trends in EU Competition Law. *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, 30 (4), p. 1947.

[11] Eriksson, C. I., Åkesson, M. and Lund, J. (2016) Designing Ubiquitous Media Services - Exploring the Two-Sided Market of Newspapers. *Journal of Theoretical and Applied Electronic Commerce Research*, 11 (3), pp. 1-19.

[12] European Commission (2016a). *Communication Online Platforms and the Digital Single Market Opportunities and Challenges for Europe*, 25 May 2016, COM(2016) 288 final.

[13] European Commission (n.d.) Glossary of Terms Used in EU Competition Policy: Antitrust and Control of Concentrations, p. 15.

[14] European Commission. *Data protection explained*. Available from: https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en [Accessed 12 March 2025].

[15] European Data Protection Board. (2024) *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*. p. 11.

[16] Evans, D. and Schmalensee, R. (2017) Debunking the 'Network Effects' Bogeyman. *Regulation*, Winter 2017-2018, p. 38. Available from: https://object.cato.org/sites/cato.org/files/serials/files/regulation/2017/12/regulation-v40n4-1.pdf?utm_source=Cato+Institute+E-mails&utm_campaign=9f32909490-regulation-winter-20172018&utm_medium=email&utm_term=0_395878584c-9f32909490-141199901&mc_cid=9f3 [Accessed 12 March 2025].

[17] Evans, D. S. and Schmalensee, R. (2007) The Industrial Organization of Markets with Two-Sided Platforms. *Competition Policy International*, 3 (1), p. 166.

[18] G7 Competition Authorities (2021) *Compendium of approaches to improving competition in digital markets*. Available from: https://assets.publishing.service.gov.uk/media/61d6cef9d3bf7f054798bbe5/Compendium_of_approachess_to_improving_competition_in_digital_markets_publication.pdf [Accessed 12 March 2025].

[19] Geradin, D. and Katsifis, D. (2022) Strengthening effective antitrust enforcement in digital platform markets. *European Competition Journal*, 18 (2), p. 362.

[20] Graef, I. (2016) EU competition law, data protection and online platforms: Data as essential facility. *International Competition Law Series, Kluwer Law International*, 68, pp. 43-45.

[21] Guimarães, G. (2024) A comment on ByteDance v Commission: the General Court's take on gatekeeper designation. *JusGov Research Paper Series*, p. 10.

[22] Hernandez Perez, A. and Gonzalez, A. (n.d.) Switching Costs. *Global Dictionary of Competition Law*, Concurrences, Art. N° 117837. Available from: https://www.concurrences.com/en/dictionary/switching-costs [Accessed 12 March 2025]

[23] Hovenkamp, H. (2017) Antitrust and Information Technologies. *Florida Law Review*, 68 (2), Article 9, p. 425.

[24] International Competition Network. (2024) Control of Data, Market Power, and Potential Competition in Merger Reviews. *Merger Working Group*, pp. 17-53.

[25] Ishwarappa, K. and Anuradha, J. (2015) A Brief Introduction on Big Data 5Vs Characteristics and Hadoop Technology. *Procedia Computer Science*, 48, pp. 320-321.

[26] COMISSION DECISION of 18 February 2010, Microsoft/Yahoo! Search Business, COMP/M.5727.

[27] Judgment of 23 June 2020, Facebook, KVR 69/19, ECLI:DE:BGH:2020:230620BK-VR69.19.0, paragraph 43.

[28] COMISSION DECISION of 3 October 2014 declaring a concentration to be compatible with the common market, Facebook/WhatsApp, COMP/M.7217, paragraph 130.

[29] Judgment of 4 July 2023, Meta Platforms Inc and Others v Bundeskartellamt, C-252/21, ECLI:EU:C:2023:537.

[30] Katz, M. L. and Shapiro, C. (1985) Network Externalities, Competition, and Compatibility. *The American Economic Review*, 75 (3), pp. 424-440.

[31] Liebowitz, S. J. and Margolis, S. E. (2002) Network Externalities (Effects). In: Newman, P. (ed.) *The New Palgrave Dictionary of Economics and the Law*. London: Palgrave Macmillan.

[32] Mandrescu, D. (2024) Designing (restorative) remedies for abuses of dominance by online platforms. *Journal of Antitrust Enforcement*, p. 9.

[33] McKnight, L. W. and Bailey, J. P. (eds.) (1997) Internet Economics. Cambridge: MIT Press, p. 6, note 3.

[34] OECD (2017) *Network Effects and Efficiencies in Multisided Markets*. Note by Shelanski, H., Knox, S. and Dhilla, A. Paris: OECD, p. 3.

[35] OECD (2019) *An Introduction to Online Platforms and Their Role in the Digital Transformation*. Paris: OECD, p. 22. Available from: https://doi.org/10.1787/53e5f593-en [Accessed 12 March 2025].

[36] OECD (2022) *The Evolving Concept of Market Power in the Digital Economy – Background Note*, DAF/COMP(2022)5, p. 16.

[37] OECD. (2019) *An Introduction to Online Platforms and Their Role in the Digital Transformation*. p. 21.

[38] Paksoy (2021) Client Briefing. Available from: https://paksoy.av.tr/en/2021/06/whatsapp-notifies-turkish-competition-authority-that-new-conditions-on-user-data-sharing-will-not-apply-in-turkey/ [Accessed 12 March 2025].

[39] Press Release No 114/24, Judgment of the General Court in Case T-1077/23 Bytedance v Commission, 17 July 2024.

[40] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

[41] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

[42] Rysman, M. (2009) The Economics of Two-Sided Markets. *Journal of Economic Perspectives*, 23 (3), p. 125.

[43] Rysman, M. (2006) An Empirical Analysis of Payment Card Usage. *Boston University - Department of Economics - Working Papers Series*, p. 14.

[44] Rysman, M. (2007) The Empirics of Antitrust in Two-Sided Markets. *Competition Policy International Journal*, 3 (1), p. 198.

[45] Sammut-Bonnici, T. and McGee, J. (2002) Network Strategies for the New Economy. *European Business Journal*, pp. 183-184.

[46] Smith, A. and Anderson, M. (2018) *Social Media Use in 2018*. Pew Research Centre, pp. 1-4. Available from: https://www.pewresearch.org/internet/2018/03/01/social-media-use-in-2018/ [Accessed 12 March 2025].

[47] The Economist. (2017) *The world's most valuable resource is no longer oil, but data*. [online] London Available from: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data [Accessed 12 March 2025].

[48] Tóth, A. (2023) Strengthening of EU Regulatory Intervention Against Data Exploitations By Online Platforms with a Zero-Price Business Model. *Masaryk University Journal of Law and Technology*, 17 (1), p. 115.

[49] U.S. Subcommittee on Antitrust Commercial and Administrative Law of the Committee on the Judiciary. (2020) Investigation of Competition in Digital Markets. *Majority Staff Report and Recommendations*, pp. 42-44.

[50] Van Alstyne, M. (2019) The opportunity and challenge of platforms, Platforms and Ecosystems: Enabling the Digital Economy Briefing Paper. *World Economic Forum*, p. 8.

[51] Van Uytsel, S. and Uemura, Y. (2017) Competition Law Interference Prior to the Formation of a Digital Market: The JFTC's Enforcement Action Against DeNA. *SSRN*. Available from: `http://dx.doi.org/10.2139/ssrn.3086449`

[52] Waller, S. W. (2012) Antitrust and Social Networking. *North Carolina Law Review*, 90 (5), p. 1789.

DOI 10.5817/MUJLT2025-1-2

ASSESSING PANDEMIC MEASURES: THE IMPACT OF DIGITAL TECHNOLOGIES ON FUNDAMENTAL RIGHTS

by

MIREILLE MARTINE CARUANA * ROXANNE MEILAK BORG †

The European Union's response to the COVID-19 pandemic relied heavily on creating, deploying and using digital technologies. This article focuses on the implications of two such measures - digital contact tracing and digital vaccine certificates. Much of the academic response to these has focused on data protection law, the preservation of privacy and the reluctance to build surveillance infrastructures that would empower states with tracking capabilities. This contribution tackles these digital initiatives from another angle. It examines their deployment through a broader human rights lens, and explores whether the EU, in mobilising these measures to curb the pandemic and reinstate free movement during these times, complied with its international obligations to protect human rights, particularly those enshrined in the European Convention on Human Rights and the EU Charter of Fundamental Rights. This paper argues that in urgent and extraordinary contexts where knowledge and understanding of health threats are limited, such as was the COVID-19 pandemic, it remains essential to be prudent if and when overstating the primacy of one or more rights over others. Human rights instruments include provisions on emergency contexts, and laws implementing fundamental rights, such as the GDPR, allow for the deployment of measures to help protect against threats to public health. It is essential in such contexts to strive for an

* Mireille M Caruana, B.A., LL.D. (Melit.), LL.M. (Lond.), Ph.D. (Bristol), is Senior Lecturer and Head of the Department of Media, Communications and Technology Law within the Faculty of Laws at the University of Malta. e-mail: mireille.caruana@um.edu.mt

† Roxanne Meilak Borg, LL.B. (Melit.), LL.D. (Melit.), M.A. (Melit.), is a Research Support Officer at the Department of Media, Communications and Technology Law within the Faculty of Laws and former Data Protection Officer of the University of Malta. e-mail: roxanne.meilak@um.edu.mt.

appropriate balance which ensures a sustained role for protective mechanisms such as lawfulness, proportionality, and legal and technical safeguards, in light of public interest goals and without undue deference to state interests which may have serious implications - such as, in this case, unjustified mass surveillance.

KEY WORDS

Human Rights, ECHR, EU Charter of Fundamental Rights, GDPR, COVID-19, digital technologies, pandemic technology, contact tracing, Digital Certificates

1. INTRODUCTION

The outbreak of the novel coronavirus SARS-CoV-2 ('COVID-19') was declared a Public Health Emergency of International Concern ('PHEIC') by the World Health Organisation ('WHO') on 30 January 2020 and classified as a pandemic less than two months later. COVID-19 retained PHEIC status until May 2023.[1] During this period, governments across the world took various diverse measures to contain the rapidly-spreading virus and to prevent and limit the consequences of the public health threat. By their nature, these measures engaged individual human rights, raising controversy regarding whether they constituted a lawful restriction of human rights in extraordinary circumstances, or whether governments were riding roughshod over and violating such rights.

Core measures implemented during the COVID-19 pandemic were either technological in nature or implemented through technological means. This contribution explores whether measures implemented by EU countries to curb the pandemic and reinstate free movement during these times complied with international obligations to protect human rights, particularly those enshrined in the European Convention on Human Rights ('ECHR') and the EU Charter of Fundamental Rights. In the context of a discussion on the balancing of civil liberties with security, American judge Richard Posner has written: 'In times of danger, the weight of concerns for public safety increases relative to that of liberty concerns, and civil liberties are narrowed. In safer times, the balance shifts the other way and civil liberties are broadened.'[2] This view indicates that values and principles can change depending on how we view threats. In light of this consideration, our article first outlines the digital technologies supporting pandemic measures that were commonly

[1] WHO. (2023) *Statement on the fifteenth meeting of the IHR (2005) Emergency Committee on the COVID-19 pandemic*. 5 May. Available from: `https://www.who.int/news/item/05-05-2023-statement-on-the-fifteenth-meeting-of-the-international-health-regulations-(2005)-emergency-committee-regarding-the-coronavirus-disease-(covid-19)-pandemic` [Accessed 26 January 2024].

[2] Posner, R. (2006) *Not a Suicide Pact: The Constitution in A Time of National Emergency*. Oxford University Press, p. 9.

deployed by a majority of European countries during the pandemic as part of a pan-European response aimed at reopening borders while still limiting the spread of the virus. It then examines human rights protection (and limitations) under extraordinary circumstances in light of the ECHR, relevant jurisprudence of the European Court of Human Rights ('ECtHR'), and the EU Charter. Finally, it considers the deployment of pandemic-related technologies, in particular digital contact tracing ('DCT') and the EU's Digital COVID Certificates, in light of the obligations under the above-mentioned legal instruments. The paper's conclusion assesses the suitability of human rights to protect all citizens during a public health emergency.

2. DIGITAL TECHNOLOGIES SUPPORTING PANDEMIC MEASURES

Measures taken by governments to help limit the spread of COVID-19 varied from contact tracing to lockdowns and other rules on physical distancing, isolation, quarantine, restricting the movement of people and the prohibition of mass gatherings. Once a vaccine became available, a further measure was the imposition of so-called 'vaccine mandates' or compulsory vaccination. This article focuses on two measures that were supplemented or enforced through digital technology: digital contact tracing ('DCT'), implemented by means of contact tracing mobile applications, and digital vaccine certificates, as the principal pandemic-related technologies that were deployed in a coordinated manner across the EU and that benefitted from interoperability across the EU Member States ('MS').

2.1.DIGITAL CONTACT TRACING AND CROSS-BORDER INTEROPERABILITY

Contact tracing ('CT') is an effective 'time-tested'[3] technique which aims to identify individuals who have come into contact with other individuals infected by a communicable disease, in order to isolate cases and stop the spread of disease. Traditionally, CT has been carried out manually, with the relevant information obtained through interviews conducted in person or over the phone.[4] Over the past century, contact tracing programmes have gained traction as a means of responding to and controlling epidemics.[5]

[3] Shahroz, M. et al. (2021) COVID-19 digital contact tracing applications and techniques: A review post initial deployments. *Transportation Engineering*, 5 (100072), p. 2.

[4] Ibid. See also: Hui, L. et al. (2022) Contact Tracing Research: A Literature Review Based on Scientific Collaboration Network. *International Journal of Environmental Research and Public Health*, 19 (15), p. 2; Nabeel, A. et al. (2022) Digital Contact Tracing Applications against COVID-19: A Systematic Review. *Medical Principles and Practice*, 31 (5), p. 429.

[5] Brandt, A. M. (2022) The History of Contact Tracing and the Future of Public Health. *American Journal of Public Health*, 112 (8), p. 1.

Nevertheless, the CT exercise is not without its challenges. Firstly, manual CT requires a substantial workforce to carry out the required interviews, particularly in fast-spreading epidemics and/or pandemics. Secondly, it is hard to trace disease transmission in contexts such as supermarkets or churches, where people are in contact with others they do not know and are thus unable to identify. Thirdly, the success of the CT exercise depends on the concerned disease: diseases that spread before individuals begin to show symptoms are harder to control and reduce, since the disease will have spread before relevant cases are identified.[6] In this latter case in particular, time is thus greatly of the essence.

In the context of the rapidly-spreading SARS-CoV-2, technology provided a way to relieve the growing burden on the individuals undertaking this manual exercise and foster a timelier response.[7] DCT, which entails the use of smartphones to register close contact with other devices running the same CT app, either through Bluetooth or GPS,[8] is faster, and supports more time-efficient tracing of disease transmission if implemented properly. In fact, research has shown that DCT 'typically averts more cases during the supercritical phase of an epidemic when case counts are rising and the measured efficacy therefore depends on the time of evaluation.'[9] DCT also solves the problem of identifying individuals crossing paths who do not know each other. However, unless mandated by the State, the success of DCT depends on individuals and their willingness to participate in the contact tracing exercise: As a matter of fact, the contact tracing mobile applications launched in most of the EU MS, first as national initiatives and later extended to include cross-border interoperability, were of a voluntary nature[10]

Thus, both manual and digital CT techniques are intrinsically valuable, but both have their drawbacks. In fact, even in the COVID-19 context, manual CT techniques were not disregarded, but were rather supplemented with DCT.[11]

---

6 Eames, K. T. D. and Keeling, M. J. (2003) Contact tracing and disease control. *Proceedings of the Royal Society B*, 270 (1533), p. 2570.

7 See: Nabeel, A. et al (2022) Digital Contact Tracing Applications against COVID-19: A Systematic Review. *Medical Principles and Practice*, 31 (5), p. 429.

8 Ibid.

9 Burdinski, A., Brockmann, D. and Maier, B. F. (2022) Understanding the impact of digital contact tracing during the Covid-19 pandemic. *PLOS Digital Health*, 1 (12), p. 1.

10 European Commission. (June 2020) *Progress Report: Mobile applications to support contact tracing in the EU's fight against COVID-19*. Available from: `https://health.ec.europa.eu/document/download/70c9e921-4930-4dbc-925e-d5a38ec393b8_en`. [Accessed 24 October 2024], p. 5

11 Shahro. (2021), *op. cit*.

2.2.DIGITAL COVID CERTIFICATES

In an attempt to encourage safe movement during the pandemic, the EU further established the Digital Covid Certificate,[12] a form of digital proof of vaccination, test results and recovery from COVID-19. Individuals in possession of a valid Certificate were in principle exempted from free movement restrictions and could travel freely within the EU.[13] Such certificates are now set to outlive the COVID-19 crisis: the concept of digital certification as a tool to protect individuals from ongoing and future health threats has in fact been taken up by the WHO and included as a first building block of the Global Digital Health Certification Network.[14]

In practice, the precursor to - and obvious requirement for - digital certification is vaccination, which is itself an integral part of managing disease.[15] Vaccination programmes aim towards reaching the public health concept of 'herd immunity', loosely framed as the proportion of individuals in a particular territory that need to be immune in order for new infections to decline.[16] Herd immunity is achieved if and when a sufficiently large percentage of the population gets vaccinated voluntarily, or through so-called 'vaccine mandates', which may involve direct or indirect coercion (for example by imposing sanctions for not getting vaccinated, or by restricting access to selected venues or restricting travel to the non-vaccinated).

---

[12] By virtue of: Regulation (EU) 2021/953 of the European Parliament and of the Council of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic. *Official Journal of the European Union* (OJ L 211/1) 14 June. Available from: `http://data.europa.eu/eli/reg/2021/953/2022-06-30` [Accessed 26 January 2024]

[13] Ibid, Art. 11.

[14] WHO. *Global Digital Health Certification*. [online] Available from: `https://www.who.int/initiatives/global-digital-health-certification-network` [Accessed 26 January 2024]

[15] Andre F. E. et al. (2007) Vaccination greatly reduces disease, disability, death and inequity worldwide. *Bulletin of the World Health Organisation* 86(2), pp. 140-146.

[16] Mc Dermott, A. (2021) Core Concept: Herd immunity is an important - and often misunderstood - public health phenomenon. *Proceedings of the National Academy of Sciences* 118(21).

3. HUMAN RIGHTS IN EXTRAORDINARY CIRCUMSTANCES

This section examines human rights protection and limitations under extraordinary circumstances in light of the ECHR, relevant ECtHR jurisprudence and the EU Charter of Fundamental Rights ('the Charter').[17] It begins by discussing the critical role of proportionality assessments when it comes to limiting human rights.

3.1. THE ROLE OF PROPORTIONALITY ASSESSMENTS

Human rights and interests often need to be balanced against each other. The COVID-19 context in particular presented the challenge of balancing individual rights against public interests. In such cases, proportionality assessments are crucial. The proportionality analysis involves the State establishing a legitimate and pressing goal – such as protecting a public interest – the achievement of which would trigger rights-infringing measures. It is up to the judiciary, then to assess the legality of any such measures. The COVID-19 pandemic presented unique challenges for courts, as governments enacted urgent and time-sensitive sweeping measures to protect public health. While necessary to combat the pandemic, these measures also severely limited individual freedoms, prompting requests to courts to reassess the proportionality of such limitations.

Vyhnanek et al.[18] explore the dynamic nature of proportionality assessments during crises like pandemics, where traditional approaches face significant limitations. They outline the standard three-step proportionality test used by courts globally: (i) Suitability (rationality), where courts assess whether the measures taken by the government are suitable for achieving their intended goal. For COVID-19, this typically involved evaluating whether restrictions were rational means of protecting public health; (ii) Necessity: This step examines whether less restrictive alternatives exist that could achieve the same objective; (iii) Proportionality in the narrow sense (balancing): Finally, courts conduct a 'cost-benefit analysis' to determine if the benefits of the restrictive measures outweigh the harm to individual rights. This was particularly challenging during COVID-19, as courts had to weigh the public interest in saving lives against the severe social and economic costs of imposed restrictions.

Vyhnanek et al. argue that courts faced a dilemma during the pandemic between adopting a 'substantive proportionality assessment' (alternatively

[17] *Charter of Fundamental Rights of the European Union*, 18 December 2000 (C 83/02). Available from: `https://www.europarl.europa.eu/charter/pdf/text_en.pdf` [Accessed 26 January 2024]

[18] Vyhnánek, L. et al. (2024). The Dynamics of Proportionality: Constitutional Courts and the Review of COVID-19 Regulations. *German Law Journal 25*, pp. 386–406.

termed 'strict substantive review'), or maintaining a deferential approach. A substantive proportionality assessment would involve closely scrutinising the government's actions and demanding strong justification for every measure taken. This approach, though protective of individual rights, risked slowing down the rapid response needed to control the pandemic. On the other hand, substantive deference allowed courts to give governments more leeway, acknowledging the complex, rapidly evolving nature of the pandemic and the high stakes involved in public health allowed courts to give governments more leeway. Most courts, during the pandemic, opted for the deferential approach, acknowledging the need for quick and decisive government action amid scientific uncertainty and time constraints.[19]

Vyhnanek et al. propose a third approach, which they call 'semiprocedural review'. This approach does not focus solely on substantive proportionality, nor does it fully defer to the government's decisions. Instead, it emphasises reviewing the rationality of the decision-making process. Courts using semiprocedural review assess whether the government followed a rational and transparent process in making decisions, considering the available evidence and weighing alternatives carefully. This approach, they argue, is particularly suited to dynamic and uncertain situations like a pandemic. It allows courts to ensure that governments act responsibly without overstepping their constitutional boundaries, while still respecting the need for swift action in emergencies.

Finally, and as a related aside, it is pertinent to note that proportionality is also a general principle of EU law, where it is recognised as having three prongs: suitability, necessity and non-excessiveness (or proportionality stricto sensu). In other words, when assessing whether there is proportionality in the context of EU law, one would ask the following questions: (i) is the measure concerned suitable for realising the goals it is aimed at meeting; (ii) is the measure concerned required for realising the goals it is aimed at meeting; and (iii) does the measure go further than is necessary to realise the goals it is aimed at meeting. Furthermore, proportionality has emerged as a data privacy principle in its own right,[20] and is an intrinsic requirement of the EU General Data Protection Regulation ('GDPR').[21]

---

[19] Vyhnánek, L. et al. (2024). The Dynamics of Proportionality: Constitutional Courts and the Review of COVID-19 Regulations. *Op. cit.*

[20] Bygrave, L. A. *Data Privacy Law: An International Perspective*, OUP 2014.

[21] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union* (2016/L-119/1) 4 May.

3.2.THE EUROPEAN CONVENTION ON HUMAN RIGHTS

The measures mentioned in section 2 impact various human rights protected under international laws such as the European Convention on Human Rights.[22] Lockdowns and other free movement restrictions affect the right to liberty[23] and the freedom of assembly and association,[24] while digital measures such as compulsory contact tracing apps and vaccine certificates impinge specifically on individuals' right to a private life[25] and raise concerns about possible discrimination.[26]

Still, States must act to manage extraordinary circumstances, and human rights instruments thus provide mechanisms for the lawful restriction of so-called 'qualified' human rights in such circumstances. For instance, the ECHR provisions pertaining to qualified rights include the conditions under which restrictions may be made, and the ECHR also provides an alternative option for states to derogate from certain human rights obligations 'in times of war or other public emergency threatening the life of the nation' by declaring a state of emergency.[27]

Restrictions must be justified. The ECHR lays down a three-part test in this regard, of lawfulness, legitimate aim, and proportionality ('necessary in a democratic society'). For example, in terms of Article 8 (2) ECHR, any interference with the right to a private life must be 'in accordance with the law' and 'necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.' Furthermore, in terms of established jurisprudence, any law restricting rights and freedoms must be 'accessible to the person concerned and foreseeable as to its effects';[28] limitations should be in response to a 'pressing social need' and not merely 'useful', 'reasonable' or 'desirable' in a democratic society;[29] and states must demonstrate a legitimate aim for the concerned interference[30] and show that they employed the least restrictive method to achieve their stated aim.

Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

22 Council of Europe. (1950) *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*. 4 November (ETS 5).

23 Ibid., Art. 5.

24 Ibid. Art. 11

25 ECHR, *op. cit.*, Art. 8.

26 ECHR, *op. cit.*, Art. 14.

27 ECHR, *op. cit.*, Art. 15.

28 *Kudrevičius and Others v. Lithuania [GC]* (2015). No. 37553/05, paras 108-110

29 *Dudgeon v. the United Kingdom* (1981). No. 752576, para 51.

30 *S.A.S v. France* (2014). Np. 43835/11

3.3.JURISPRUDENCE OF THE ECTHR

The ECtHR carries out assessments of the legality of measures that limit human rights, and through its jurisprudence, offers insight into the balancing exercise that must be undertaken when limiting a human right to pursue a public interest such as public health. The authors are not aware of any ECtHR judgments to date that specifically address the implications of tech measures deployed by states to aid with combatting the COVID-19 pandemic on fundamental rights. Furthermore, although numerous other pandemic-related complaints were brought before the ECtHR, this Court has not ruled on the substance in the majority of such complaints, but has rather declared these inadmissible on procedural grounds. Thus, established parameters on justified restrictions of human rights in circumstances such as those of the COVID-19 pandemic are limited. Nevertheless, in reaching its verdicts of inadmissibility, the Court shed light on how this context could eventually be substantively considered.

To exemplify the above, this section first considers pertinent COVID-19 cases relating to the right to liberty, the freedom of assembly and association, and the right to private life, respectively, that were deemed inadmissible by the Court. It then analyses a recent COVID-19 case on the right to private life where the ECtHR delivered a substantive ruling. Rather than focusing on whether the Court's approach to fundamental rights differs pre- and post-COVID-19, this article aims to elucidate the Court's approach in the pandemic-related cases, with a view to shedding light on whether such approach would also be reflected in judgments relating to pandemic tech measures.

The complainant in Terhes v. Romania[31] alleged that a lockdown imposed during the pandemic breached his right to liberty. The ECtHR dismissed the case on the grounds that this measure had not targeted the applicant individually. It considered that while the lockdown did not amount to a deprivation of the applicant's liberty (since he had been "free to leave his home for various reasons and could go to various destinations, at whatever time of day it was necessary to do so" and he "was not individually monitored by the authorities"), it did constitute a restriction to the applicant's freedom of movement as protected by Article 2 of Protocol No. 4 ECHR.[32] Nonetheless, the ECtHR did not proceed to examine whether such restriction was a permitted interference since the applicant did not invoke Protocol No. 4 in his complaint, and in any case, Romania had already previously declared an Art. 15 state of emergency and its intention to derogate from such Protocol.

[31] *Terhes v. Romania* (2021). No. 49933/20
[32] Ibid., paras 43, 45.

In CGAS v. Switzerland,[33] the ECtHR considered whether a ban on public and private events imposed by Switzerland at the onset of the pandemic was a legitimate interference with the right to freedom of assembly and association in terms of Art. 11(2) ECHR. The ECtHR initially ruled on the merits of the complaint, holding that the blanket ban was 'not proportionate to the aims pursued', that 'the domestic courts did not conduct an effective review of the measures at issue during the relevant period' and that thus, in implementing such a measure, Switzerland had 'overstepped the margin of appreciation afforded to it.'[34] The Court declared that it was 'not persuaded that the applicant enjoyed at the time of the application an effective remedy'[35] and thus dismissed the Swiss government's objection of non-exhaustion of domestic remedies.[36] This judgment would have been one of the few substantive rulings on a pandemic-related complaint; however, the case was later referred to the Grand Chamber, which, contrary to the earlier judgement, held that domestic remedies had been available to CGAS and deemed the application inadmissible precisely on the grounds of failure to exhaust such remedies.[37] In what may be described as a deferential approach, the Grand Chamber affirmed in its decision of inadmissibility that it 'cannot ignore the exceptional nature of the [COVID-19] context'[38] and that it was 'all the more important that the national authorities were first given the opportunity to strike a balance between competing private and public interests or between different rights protected by the Convention, taking into consideration local needs and conditions and the public-health situation as it stood at the relevant time.'[39]

The applicant in Piperea v. Romania[40] complained that the state had infringed on his right to privacy when, during the pandemic, it imposed a requirement on individuals leaving their homes to fill out a document stating where they were going, why, and for how long, together with other personal information. The ECtHR dismissed the case on the grounds that the applicant did not explain how the measures affected him personally. In this case too, the Court may be said to have opted for the deferential approach, as it stated in its inadmissibility decision that 'the measures had been imposed on the entire population in response to what competent national authorities

[33] *Communauté Genevoise d'Action Syndicale (CGAS) v. Switzerland* (2022). No. 21881/20
[34] *CGAS v. Switzerland (2022), op. cit.*, para 91.
[35] *CGAS v. Switzerland (2022), op. cit.*, para 59.
[36] *CGAS v. Switzerland (2022), op. cit.*, para 60.
[37] *Communauté Genevoise d'Action Syndicale (CGAS) v. Switzerland* (2023). No. 21881/20
[38] Ibid., para 162
[39] Ibid., para 163
[40] *Piperea v. Romania* (2022). No. 24183/21

had determined to be a serious public health situation' and acknowledged that 'the situation had to be characterised as 'unforeseeable exceptional circumstances.'[41]

The right to a private life has also been invoked in complaints pertaining to compulsory COVID-19 vaccination. In Thevenon v. France,[42] the complainant alleged that the requirement of vaccination based on his occupation as a firefighter breached his right to a private life and was discriminatory and in breach of Art. 14 ECHR. The ECtHR dismissed this application on the grounds that the applicant had not exhausted domestic remedies available to him prior to seeking recourse to it. It also reached a similar decision in Zambrano v. France,[43] concerning the so-called 'health pass' implemented by French authorities, by virtue of which individuals could show proof of vaccination to be allowed into places hosting large numbers of people, such as cinemas, museums and trade fairs. The applicant contended that this measure was intended to 'compel individuals to consent to vaccination' and that the laws establishing the health pass amount to a 'discriminatory interference with the right to respect for private life.'[44] This case was also dismissed on the basis that the applicant had failed to exhaust all domestic remedies available to him.

In the case of Pasquinelli and Others v. San Marino,[45] decided in August 2024, the Court finally pronounced itself on the merits of a COVID-19 related complaint. This case involved twenty-six healthcare personnel who refused to get vaccinated against COVID-19 and who were consequently affected by several measures relating to their employment - such as suspension without pay and relocation to vacant posts - under a 2021 law regulating the vaccination of healthcare workers. The Court held that this law did not constitute a violation of the right to a private life, that 'restrictive measures in the health sector adapted to the constant evolution of the COVID-19

[41] Registrar of the European Court of Human Rights. (2022) *Complaint against Romanian COVID-19 measures inadequately substantiated, inadmissible.* [press release] 1 September. Available from: `https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=003-7416653-10152416&filename=Decision\%20Piperea\%20v.\%20Romania\%20-\%20Complaint\%20against\%20Romanian\%20COVID-19\%20measures\%20inadmissible.pdf` [Accessed 26 January 2024]

[42] *Thevenon v. France* (2022). No. 46061/21

[43] *Zambrano v. France* (2021). No. 41994/21

[44] Registrar of the European Court of Human Rights. (2021) *The European Court of Human Rights declares inadmissible an application contesting the French "health pass"*. [press release] 7 October. Available from: `https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=003-7145978-9686694&filename=Decision\%20Zambrano\%20v.\%20France\%20-\%20application\%20which\%20was\%20challenging\%20the\%20French\%20\%E2\%80\%9Chealth\%20pass\%E2\%80\%9D.pdf` [Accessed 26 January 2024]

[45] *Pasquinelli and Others v. San Marino* (2024). No. 24622/22

pandemic … pursued the legitimate aim of the protection of health and the protection of the rights and freedoms of others'[46] and that such measures 'stood in a reasonable relationship of proportionality to the legitimate aims pursued by the State', which had as such not 'exceeded its wide margin of appreciation in health care policy matters.'[47] It re-confirmed the COVID-19 context as 'exceptional and unforeseeable'[48] and endorsed the measures taken by the concerned State in this case.

Barring the exceptional decision in CGAS, which was in any case later overturned by the Grand Chamber, the ECtHR appears reticent to call into question measures adopted by States at such an extraordinary time as was the onset and duration of the COVID-19 pandemic, or indeed, to pronounce itself on whether an appropriate balance was struck between the taking of appropriate measures and respect for human rights. The ECtHR has dismissed numerous complaints relating to general and/or nation-wide measures, and in most cases, appears to at least implicitly reaffirm the severity of the COVID-19 context in particular as perceived at the time the events were unfolding.

It is in light of the stance seemingly adopted by the ECtHR that the above-mentioned CGAS decisions merit further attention in the present discussion. The decisions of both the ECtHR Third Section and the Grand Chamber include an opinion of dissenting judges. Broadly speaking, there were those who felt that a limitation of the freedom of peaceful assembly should fall within the wide margin of appreciation generally afforded to States in healthcare matters,[49] and those who, while acknowledging that 'the Court must respect the member States' margin of appreciation in weighing up the requirements of combatting a pandemic on the one hand and fundamental freedoms on the other', nevertheless argued that 'no such margin of appreciation exists with regard to the availability of judicial remedies' and that the Grand Chamber had failed to sufficiently

[46] Ibid., para 96

[47] *Pasquinelli and Others v. San Marino* (2024), *op. cit.*, para 108. Note that the ECtHR had previously and outside the COVID-19 context, ruled on the issue of compulsory vaccination in the context of Art. 8 ECHR, also finding in that case that there was no violation of this provision. In the case of *Vavřička and others v. Czech Republic* (2021), Nos. 47621/13, 3867/14, 73094/14, 19298/15, 19306/15 and 43883/15, the Court held that while the duty to vaccinate children (subject to a sanction/fine on parents) and the direct consequences of non compliance with such duty (exclusion of children from preschool or nursery) amounted to an interference with Art. 8, this interference was lawful and pursued the legitimate aim of protecting the health and the rights of others. In this assessment, the Court considered the State's margin of appreciation, the pressing social need and relevant and sufficient reasons, and proportionality

[48] *Pasquinelli and Others v. San Marino* (2024), *op. cit.*, para 19

[49] *CGAS v. Switzerland* (2022), *op. cit.*, Joint Dissenting Opinion of Judges Ravarani, Seibert-Fohr and Roosma, para 13

recognise that 'the principles which are at the heart of a democratic society are "vulnerable" in times of crisis, in terms both of procedure and of substance'.[50]

The former judges supported their position by referring to the fact that, although there was no parliamentary debate regarding the introduction of health measures in Switzerland, the federal authorities had the support of the people as evidenced by two referenda, held in June and November 2021. On both occasions, a majority of more than 60% of the electorate rejected initiatives to force the lifting of the relevant restrictive measures.[51] Insofar as the latter judges' opinion is concerned, pre-eminence is placed on the 'guardian' role of the Court even in times of crisis. In their view (i) Switzerland had not provided a readily available judicial remedy, thus the applicants had in fact exhausted domestic remedies and the ECtHR was properly seized of the case; and (ii) on the substantive merits of the case Switzerland had in fact infringed human rights. While these authors are in agreement with the majority opinion of the Grand Chamber, we do not deny that judicial remedies that need strengthening should be strengthened, while the legality of measures allegedly infringing human rights should (always) be assessed in light of the relevant contextual factors.

Finally, although there is no specific ECtHR ruling on the compatibility with human rights of digital measures deployed to manage the pandemic, it is arguable that this court will continue to pursue the stance elucidated above in this regard too, and attach greater importance to state discretion (within the 'margin of appreciation') with regard to such measures employed temporarily at a time of emergency. This is also in line with what is being observed elsewhere in the literature, that, as the ECtHR appears to be increasingly inclined to permit mass surveillance, it is also 'likely to agree with most of the [technological] measures that states have introduced to prevent the COVID-19.'[52]

---

[50] *CGAS v. Switzerland* (2023), *op. cit.*, Joint Dissenting Opinion of Judges Bošnjak, Wojtyczek, Mourou-Vikstrőm, Ktistakis and Zűnd, paras 9, 10.

[51] Joint Dissenting Opinion of Judges Ravarani, Seibert-Fohr and Roosma (2022), para 13, *op. cit.*

[52] Vardanyan, L. and Stehlik, V. (2022) Is the Case Law of the ECtHR Ready to Prevent the Expansion of Mass Surveillance in Post-Covid Europe? *Sciendo*, 7 (2020), p. 253.

3.4.FUNDAMENTAL RIGHTS WITHIN THE EUROPEAN UNION

3.4.1 The EU Charter of Fundamental Rights

In addition to their obligations under the ECHR, EU MS must abide by the EU's Charter of Fundamental Rights,[53] which is primary EU law and legally binding on such MS,[54] but only applicable when these States are 'implementing Union law'[55] and thus covering 'all situations where member states fulfil their obligations under the treaties as well as under secondary EU law (adopted pursuant to the treaties)'.[56]

The EU Charter contains a general 'horizontal' provision which sets out the conditions that every limitation on a fundamental right set out in the Charter must comply with in order to be compliant with EU law. Article 52(1) states that any such limitation must be 'provided for by law', and must 'respect the essence' of those rights and freedoms recognised by the Charter. Furthermore, such limitations must be compliant with the principle of proportionality, and 'may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others'. The 'objectives of general interest recognised by the Union' include the protection of public health.[57] Lenaerts notes that the wording of Article 52(1) of the Charter is largely inspired by CJEU jurisprudence on the protection of fundamental rights, which, in turn, draws on the jurisprudence of the ECtHR.[58]

As primary EU law, the Charter serves as an aid to the interpretation of both secondary EU legislation and national legislation falling within the scope of EU law, which must therefore be interpreted in light of the Charter.[59] Moreover, the Charter may provide grounds for judicial review, as EU law that violates Charter rights will be declared void by the CJEU, and national legislation that falls within the scope of EU law and violates the Charter must be set aside. The scope of application of EU fundamental rights with regard to MS' actions, or in other words, the circumstances in which these rights apply to MS actions, is also determinative of the cases where, in principle, the CJEU

---

53 EU Charter (2000), *op. cit.*

54 *Consolidated Version of the Treaty on the European Union*, 26 October 2012 (C 326/13). Available from: https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF [Accessed 26 January 2024], Art. 6 (1).

55 EU Charter (2000), *op. cit.*, Art. 51 (1)

56 Lenaerts, K. (2012) Exploring the Limits of the EU Charter of Fundamental Rights. *European Constitutional Law Review*, 8 (3), pp. 375–403

57 Judgment of 29 April 1999, Standley and Others, C-293/97, ECLI:EU:C:1999:215

58 Lenaerts (2012), *op. cit.*, p. 388.

59 Ibid.

has the final word on fundamental rights protection in the EU in the event of an allegation that a MS failed to comply with them.[60]

3.4.2 The EU Charter and the ECHR

The EU framework also gives due importance to the ECHR. Fundamental rights as guaranteed by the ECHR constitute general principles of EU law,[61] although the EU has itself to date refrained from acceding to the ECHR[62] and thus the Convention does not constitute a legal instrument which has been formally incorporated into the EU legal order.[63]

The EU Charter itself provides that, in so far as the Charter contains rights which correspond to rights guaranteed by the ECHR, the meaning and scope of those rights shall be the same as those laid down by the Convention. Furthermore, EU law may 'provide more extensive protection.'[64] For instance, the right to a private life enshrined in Art. 8 ECHR is mirrored in Art. 7 of the Charter. The meaning and scope of both rights are the same.[65] Consequently, limitations which may be legitimately imposed on these rights are also the same as those allowed by Article 8 of the ECHR.[66] Notably, 'it seems clear that the level of protection afforded by the Charter may not be lower than that guaranteed by the Convention as interpreted by the Human Rights Court.'[67]

ECtHR jurisprudence is clearly relevant within the EU context. The CJEU has explicitly declared that EU courts must take such jurisprudence into account in interpreting fundamental rights; for example, in the Abdida case[68] the CJEU stated that in accordance with Art. 52(3) of the Charter, ECtHR jurisprudence must be taken into account for the purpose of interpreting

[60] Kokott, J. and Sobotta, C. (2015) Protection of Fundamental Rights in the EU: On the Relationship between EU Fundamental Rights, the European Convention and National Standards of Protection, *Yearbook of European Law*, 34 (1), pp. 60-73.

[61] Article 6(3) TFEU

[62] Advocate General Kokott. (2014) *Opinion procedure 2/13 initiated following a request made by the European Commission*. (ECLI:EU:C:2014:2454) 7 June. Available from: https://curia.europa.eu/juris/document/document.jsf;jsessionid=6580258E3F20CFA2CB5CAB5DCC17936E?text=&docid=160929&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=145338 [Accessed 26 January 2024]

[63] Kokott, J. and Sobotta, C. (2015), *op. cit*

[64] EU Charter (2000), *op. cit.*, Article 52(3).

[65] Ibid.

[66] Explanations relating to the Charter of Fundamental Rights. *Official Journal of the European Union* (2007/C 303/02) 14 December. Available from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0017:0035:en:PDF [Accessed 26 January 2024]

[67] Kokott, J. and Sobotta, C. (2015), *op. cit.*, p. 64.

[68] Judgment of 18 December 2014, Abdida, C-562/13, ECLI:EU:C:2014:2453

Charter provisions,[69] although the CJEU retains the final word on the interpretation of EU fundamental rights.[70]

Of relevance to the present discussion, the Charter has elevated to fundamental right status the right to protection of personal data.[71] The significance or added value of affirming data protection as a fundamental right, separate from the right to privacy, has been explored in the literature.[72] It is pertinent to note that this 'new' right as enshrined in the Charter constitutes the normative foundation for the secondary data privacy legislation in the EU, in particular, the General Data Protection Regulation ('GDPR'). It is the GDPR that implements the substantive aspect of this right, providing conditions and limitations for the exercise of the right to the protection of personal data (within the scope of that legislative instrument, that for example excludes processing by law enforcement authorities for law enforcement purposes.[73])

The deployment and use of pandemic tech engage privacy and data protection rights above all. Thus, within the EU, they fall within the scope of the Charter and are subject to the GDPR.

3.4.3 The GDPR

As aforementioned, the provisions of the GDPR implement the fundamental right to protection of personal data guaranteed by Art. 8 Charter, and must be interpreted in light of such Charter. The processing of personal data for the management of the COVID-19 pandemic – including the processing of health data by contact tracing mobile apps and for the purposes of digital health certificates – is subject to the GDPR, which lays down rules regarding lawfulness and proportionality of processing, but also envisages extraordinary circumstances.

The GDPR requires any processing operation involving so-called 'special categories of personal data' (which include 'data concerning health') to have a lawful basis under Article 6 and to be exempt from the general prohibition on processing of special categories of personal data under one of the conditions listed in Article 9(2).[74] Thus, data processing undertaken during emergency circumstances such as a pandemic, for purposes such as contact tracing,

[69] Judgment of 18 December 2014, Abdida. *Op.cit.* para 47
[70] See Opinion of Advocate General Kokott (2014), *op. cit.*, para 170
[71] EU Charter (2000), *op. cit.*, Art. 8.
[72] Mifsud Bonnici, J. P. (2013). Exploring the non-absolute nature of the right to data protection. *International Review of Law, Computers & Technology*. 28 (2)
[73] GDPR, *op. cit.*, Art. 2 (2)
[74] Judgement of 21 December 2023, Medizinischer Dienst der Krankenversicherung Nordrhein, Körperschaft des öffentlichen Rechts, C 667/21, ECLI:EU:C:2023:1022

must be provided for by law, where such processing is not based on the individuals' consent. In terms of Art. 9 (2), in fact, the general prohibition against the processing of special categories of data such as health data in Art. 9 (1) can be lifted in the context of public health emergencies where 'necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health ... on the basis of Union or MS law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject'.[75]

The GDPR's recitals provide further guidance about the changing role of the data protection framework during emergencies, noting in particular that data subject consent is not needed during public health emergencies: 'the processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject.'[76] Furthermore, '[s]uch processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons.'[77] Thus, apart from other general qualities that an implementing law should have, such as foreseeability and publicity requirements, it should provide for legal and other organisational and technological safeguards, such as encryption of data, the latter as recalled throughout the text of the GDPR and particularly in its provisions on data protection by design. Such safeguards would normally be implemented in light of risks of varying levels identified in data protection impact assessments ('DPIAs'), themselves mandated by the GDPR in such 'likely to result in a high risk' circumstances.

[75] GDPR, *op. cit.*, Art. 9 (2) (i)

[76] GDPR, *op. cit.*, Recital 54

[77] Ibid. For further discussion, see Leiser, M. R. and Caruana, M. M. (2020) *Some Contrarian Thoughts on the Deployment of Contact-Tracing Apps.* Available from `https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3608677`. [Accessed 15 February 2024]

4. TECHNOLOGICAL INITIATIVES IN EXTRAORDINARY CIRCUMSTANCES

This section considers the deployment of pandemic-related technologies, in particular, digital contact tracing and digital vaccine certificates as the principal pandemic-related technologies deployed in a coordinated manner across the EU, in light of the obligations emanating from the legal instruments discussed in the previous section.

4.1.DIGITAL CONTACT TRACING

A face value reading of the justifications and limitations permissible to qualified human rights and the conditions and requirements under which they may be applied or availed of during times of crisis leads one to conclude that, at least in Europe, this legal framework is relatively robust; It offers flexibility to States to act as may be required to manage extraordinary events, whilst still providing for the upholding of human rights.

In practice, however, it appears that in the context of the COVID-19 pandemic, countries generally either proceeded as they deemed fit, or erred on the side of caution and subjected all relevant data processing to their citizens' consent. Many countries around the world implemented a form of DCT. Some, such as Russia and Armenia, made it compulsory for their citizens to download the relevant CT apps.[78] In the EU, individuals were free to choose whether or not to do so.[79] Furthermore, EU DCT apps only measured the Bluetooth signal strength between devices and the length of time of exposure, meaning that actual location data was not stored, but merely the relevance of the proximity in terms of likely contagion, which was notified to the individual via the app; no public or other central authority was permitted to check for compliance and/or enforce the notifications sent to users that recommended that they isolated, self-quarantined, or got tested.

Deployment of DCT apps in the EU required compliance with the EU Charter of Fundamental Rights and the GDPR. Nevertheless, it may be questioned on a preliminary basis whether DCT apps deployed in certain EU Member States were actually processing personal data - and thus fell within the material scope of the GDPR - at all, since the issue of when data can be considered anonymous and therefore, outside the scope of the GDPR, remains contentious.[80] It is nevertheless worth noting that where data

[78] Vardanyan, L. and Stehlik, V. (2022), *op. cit.*, p. 256.

[79] European Commission. (2022) *Digital Contact Tracing Study*. Luxembourg: Publications Office of the European Union, p. 7

[80] cf. the contested interpretation of the 'means reasonably likely to be used ... either by the controller or by another person to identify the natural person directly or indirectly': Judgment of 19 October 2016, Patrick Breyer v Bundesrepublik Deutschland, C-582/14,

undergoing processing does not relate to an identifiable individual and thus does not constitute 'personal data' as per the GDPR, the right to privacy may still be engaged.

In any case, a genuine choice not to download and use DCT apps was offered to EU citizens and thus, in GDPR terms, consent remained a viable and indeed the commonly chosen option for processing.[81] Some MS adopted specific legislation to ensure an appropriate legal basis for the relevant data processing;[82] a case in point, the authors' home country of Malta based its processing of data for the purposes of the CT app on the legal basis of public interest and implemented safeguards such as purpose specification and limitation, and non-discrimination in specific legislation.[83]

In this context, were EU MS legally obliged to rely on data subject consent for the deployment and use of CT apps? Russia and Armenia have been criticised for imposing such apps on their citizens.[84] In the EU, such a notion was condemned at the outset, when CT apps began to be developed,[85] even though the legal framework appears to provide an alternative option for processing that does not involve individuals' consent. One must of course acknowledge that, beyond privacy and data protection related concerns, it may in practice be hard to enforce the use of compulsory apps and/or smartphones, as such an exercise would surely entail challenges of its own, particularly in respect of individuals who can or do not use smartphones at all.

Practical issues aside, however, the question arises: in the context of digital contact tracing, can there be no restriction of the fundamental rights

ECLI:EU:C:2016:779; Judgment of 26 April 2023, Single Resolution Board v. European Data Protection Supervisor, T-557/20, ECLI:EU:T:2023:219, under appeal brought by the EDPS (C-413/23 P)

81 European Commission, *Digital Contact Tracing Study: Study on lessons learned, best practices and epidemiological impact of the common European approach on digital contact tracing to combat and exit the COVID-19 pandemic*, p.7 ('All apps were made available on a voluntary basis.')

82 European Commission. (2020) *Mobile applications to support contact tracing in the EU's fight against COVID-19 Progress*. Available from: `https://health.ec.europa.eu/document/download/70c9e921-4930-4dbc-925e-d5a38ec393b8_en` [Accessed 29 December 2024]

83 S.L. 465.52 *Malta Contact Tracing and Alerting Mobile Application Order, Subsidiary Legislation 465.52, adopted by Legal Notice 379 of 2020 as amended by Legal Notice 128 of 2021*. In: English. The government of Malta took this approach on the legal advice provided by the first author of this contribution (relative documentation on file with the author)

84 Vardanyan, L. and Stehlik, V. (2022), *op. cit.*, p. 256.

85 European Data Protection Board. *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, Adopted on 21 April 2020. Available from: `https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf` [Accessed 26 January 2024]; and Ventrella, E. (2020) Privacy in emergency circumstances: data protection and the COVID-19 pandemic. *ERA Forum*, 21 (3), p. 385

to privacy and data protection except for that explicitly consented to by the individuals concerned, even in the context of a public health emergency such as was that of the Covid context? If on the contrary, any such restrictions are indeed justified in a democratic society in the context of crises, could and should EU MS have been able to do better than they actually did with the technological solutions they were able to deploy in the face of resistance from privacy advocates and lobbyists?[86]

The obligation towards the State is not one reasonably based on consent as defined by the GDPR. The State processes personal data on legal bases other than consent for a variety of purposes, such as to provide social services and for taxation purposes. It would be meaningless for the state to claim to be processing such data on the basis of citizens' consent, since the citizen cannot reasonably deny or withhold their consent in such contexts. Moreover, the state has an obligation to carry out its tasks in this regard, and can and should not be hindered in doing so by the withholding of the individual's consent.

However, as elucidated in section 3, in restricting a fundamental right on a basis other than consent, a state must assess the suitability, necessity and proportionality of the relevant measure, and then also ensure appropriate safeguards. Akinsanmi and Salami highlight the importance of elements such as lawfulness, fairness and transparency, accountability and public trust in balancing competing rights and interests.[87] Indeed, to deploy a CT system that does not rely on citizen collaboration expressed through such individuals' consent, a state must pass a law that provides both for data processing for specific purposes and other suitable and specific safeguarding measures to be implemented in respect of it.

A law intended to safeguard the rights and freedoms of concerned individuals in this regard should define who the controller/s is/are, specify the purpose of processing and lay down explicit limitations regarding further use, identify the categories of data as well as the entities to, and purposes for which the personal data may be disclosed, and enact additional meaningful safeguards as appropriate, including a specific reference to the voluntary nature of the application, and providing specific rules for non-discriminatory protection. Laws enacted in extraordinary circumstances should importantly include a time limit or 'sunset clause' – in the sense that measures should be

[86] For more discussion on this see Litan, R. E. and Lowy, M. (2020) *Freedom and privacy in the time of coronavirus*. [online]. Washington DC: Brookings. Available from: `https://www.brookings.edu/articles/freedom-and-privacy-in-the-time-of-coronavirus/` [Accessed 26 January 2024]

[87] Akinsanmi, T. and Salami, A. (2021) Evaluating the trade-off between privacy, public health safety, and digital security in a pandemic. *Data & Policy 3*, e27. `https://doi.org/10.1017/dap.2021.24`

temporary and rolled back once the crisis is over. A time limit should also be applied to the retention period of all collected personal data. Measures and penalties for non-compliance could also be integrated into the law. Even where States deploy systems that do rely on citizens' consent, it is advisable to base any human rights restrictions on a law. In such cases, a specific reference to the voluntary nature of the application, providing specific rules for non-discriminatory protection, may be included in such law. For example, in line with the approach taken throughout the rest of the EU, Maltese law also stipulated that 'the use of the application shall be on a voluntary basis and no person shall suffer from any form of disadvantage or discriminatory action for refusing or for being unable to use the application.[88]

Beyond legal safeguards, throughout the pandemic much emphasis was placed on implementing safeguards 'by design' in contact-tracing apps.[89] Indeed in practice, and also for the sake of achieving interoperability across the Member States, most EU Member States deployed decentralised applications based on the Google and Apple Exposure Notification Framework, using Bluetooth technology to enable digital proximity tracing,[90] and following the DP-3T (Decentralised Privacy-Preserving Proximity Tracing) data protection solution developed by a group of European academics.[91] The use of decentralised contact-tracing apps used in combating Covid-19 was, for example, 'applauded' by Akinsanmi and Salami 'for minimising privacy risks while ensuring the digital security and health safety of people'.[92] While not discounting the importance of 'by design' strategies, the first author of this piece has argued elsewhere that 'trust-building elements can come about on the front end at the expense of functionality, or on the back end through strong safeguards as required under Article

[88] S.L. 465.52 (2021), *op. cit.*, Art. 6.

[89] See Li, J., Guo, X., (2020). COVID-19 Contact-tracing Apps: a Survey on the Global Deployment and Challenges. *arXiv*. Available form: https://doi.org/10.48550/arXiv.2005.03599

[90] European Commission: Directorate-General for Communications Networks, C. and T., Prodan, A., Birov, S., Wyl, V., Ebbers, W., Schulz, C., Hentges, M., Tariq, S., Stroetmann, V., (2022). *Digital contact tracing study – Study on lessons learned, best practices and epidemiological impact of the common European approach on digital contact tracing to combat and exit the COVID-19 pandemic*. Publications Office of the European Union. Available from: https://doi.org/10.2759/146050

[91] Troncoso, C et al. *Decentralised Privacy-Preserving Proximity Tracing (DP-3T) White Paper*. [GitHub] 25 May. Available from: https://github.com/DP-3T/documents/blob/master/DP3T\%20White\%20Paper.pdf [Accessed 14 October 2024]. See also: Troncoso, C. et al. (2020). Decentralized Privacy-Preserving Proximity Tracing. *arXiv*. Available from: https://doi.org/10.48550/arXiv.2005.12273

[92] Akinsanmi, T. and Salami, A. (2021), *op. cit.*

9(2)(i)'[93] and further that 'there is more than one means to achieve [trust] and there is more than one way to ensure privacy: put effective functionality first (trusting that the app has worthwhile utility to justify the interference with privacy), ensure the user interface is friendly and understandable second (by ensuring the app is friendly and easy to navigate, users trust what is going on inside the environment), design apps for compliance with the GDPR's principles third, while ensuring strong privacy and data protection safeguards are put on a lawful basis.'[94]

However, the functionality of technological solutions should not be undermined in light of privacy and/or data protection concerns. Thus, understanding the purpose that a tech solution is intended for is central to the legal consideration of whether such solution passes the necessity and proportionality tests set out in the relevant human rights frameworks and the GDPR. It is often claimed that necessity must be born out of effectiveness: however, at the onset of the pandemic, there were many unknowns about the way COVID-19 spreads. Moreover, there was no conclusive evidence available to States regarding how effective the deployment of a DCT app would be at the time they were being called upon to carry out their duties and take necessary actions to contain the crisis. Thus, the status of the threat must be taken into account as understood and given the scientific evidence available at the time when the action was taken and the proposed tech solution deployed, and not with the benefit of hindsight.

The question of necessity is not one that can be answered conclusively in the abstract, as proportionality is contextual upon the ongoing current status of the threat. Thus, a technology that is deployed and that is proportionate at one point in time may need to be decommissioned/withdrawn at a later time when the extent of the threat has diminished or is no longer extant – for example after a vaccine has been developed and administered to a sufficiently large percentage of the population. As mentioned, such 'sunset clauses' should also be included as a safeguard in the relevant legislation.

---

[93] Leiser, M.R., Caruana, M.M., (2020). Some Contrarian Thoughts on the Deployment of Contact-Tracing Apps. *SSRN*. Available from: https://dx.doi.org/10.2139/ssrn.3608677

[94] Ibid.

4.2.DIGITAL VACCINE CERTIFICATES

Like contact tracing, digital vaccine certificates were deployed with the ultimate aim of limiting the spread of the virus. Their deployment happened hand in hand with the introduction of vaccine mandates, meaning that some countries chose to restrict access to workplaces and other publicly accessible places such as museums and cinemas, or to international travellers to enter the country, based on whether the individual could produce such a certificate of vaccination.[95] This led to allegations of unfair discrimination, as the unvaccinated suffered the consequences of their choice not to get vaccinated in terms of the restriction of their ability to go to work, other selected venues, and to travel.

The EU's vaccine certificates, called Digital COVID Certificates, were praised for being established by and grounded in primary EU law, as well as for being more 'privacy-preserving' than other technological solutions such as the blockchain-based IATA Travel Pass deployed by some airlines.[96] Nevertheless, the introduction of these certificates gave rise to much controversy, centering around concerns relating to social exclusion and inequality.[97]

In terms of human rights, digital certificates and corresponding vaccine mandates must also be considered in light of the principle of non-discrimination, enshrined in Art. 14 ECHR. Notably, the ECtHR has always examined this right in conjunction with another substantive ECHR provision, such, for instance, as Art. 8, although it has held that there may be a breach of Art. 14 even if there was no breach of the associated substantive right.[98] In the early stages of the pandemic, the Council of Europe called for emergency measures to be amongst others non-discriminatory.[99] However,

---

[95] European Commission. (2022) *Report from the Commission to the European Parliament and the Council pursuant to Article 16(3) of Regulation (EU) 2021/953 of the European Parliament and of the Council on the Framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic.* 22 December. Available from `https://commission.europa.eu/publications/key-documents-related-digital-covid-19-certificate_en` [Accessed 27 February 2024], p. 11.

[96] Halpin, H. (2022) A Critique of EU Digital COVID-19 Certificates: Do Vaccine Passports Endanger Privacy? *The 17th International Conference on Availability, Reliability and Security*. Vienna, Austria. Available from: `https://dl.acm.org/doi/10.1145/3538969.3544459` [Accessed 26 January 2024], p. 7.

[97] See Mohapatra, S. (2020) Passports of Privilege. *American University Law Review*, 70, pp. 1729-1763 and Halpin, H. (2022) A Critique of EU Digital COVID-19 Certificates: Do Vaccine Passports Endanger Privacy? *op.cit.*

[98] ECtHR (2022). *Guide on Article 14 of the European Convention of Human Rights and on Article 1 of Protocol No. 12 to the Convention. Prohibition of Discrimination*. 31 August, p. 9 para 19

[99] CoE Steering Committee on Anti-Discrimination, Diversity and Inclusion. (2020) *COVID-19: an analysis of the anti-discrimination, diversity and inclusion dimensions in Council of Europe*

even in this regard, one should not be too quick in presuming unlawfulness. As has been pointed out in literature, 'unequal treatment of people who belong to different groups… does not necessarily constitute discrimination that is morally objectionable, and hence, prohibited by law – that is, wrongfully imposed disadvantageous treatment – because the distinction is not arbitrarily related to a characteristic the person does not control.'[100] While, as discussed above, the ECtHR has recently declared allegations of discrimination in relation to COVID-19 vaccination inadmissible and dismissed these, it remains to be seen whether these would be declared discriminatory in a substantive ruling, particularly in light of the fact that the notion of vaccination passports has also now been taken up by the WHO with a view to applying it on a global level.

5. CONCLUSION

Human rights laws do not exist or purport to exist in isolation. They often permit flexibility in extraordinary circumstances, and themselves provide mechanisms for states to manage such circumstances lawfully. For instance, the ECHR sets out permitted limitations to qualified rights in its substantive provisions, and permits an alternative course of action under Art. 15 in the event of war or other public dangers threatening the life of the nation, whereby states may derogate from qualified rights and freedoms by declaring a state of emergency. Within the EU, substantive laws that implement fundamental rights – like the GDPR – also envisage and provide for such circumstances. Furthermore, the EU Charter of Fundamental Rights does not preclude EU MS from declaring a state of emergency in terms of Art. 15 ECHR.[101]

COVID-19 presented an extraordinary scenario involving a highly infectious and potentially life-threatening disease. Governments rushed to implement measures in an attempt to halt or limit contagion, with the legitimate aim of saving lives, in the face of limited knowledge and understanding of the virus itself. Such measures did not come without a cost, both in terms of restricting and potentially violating human rights, but also severely affecting national and global economies.

These exceptional circumstances have even been acknowledged by the ECtHR. Although there is limited guidance from this court on the human

Member States. 11 November. Available from: `https://edoc.coe.int/en/living-together-diversity-and-freedom-in-europe/9741-covid-19-an-analysis-of-the-anti-discrimination-diversity-and-inclusion-dimensions-in-council-of-europe-member-states.html` [Accessed 26 January 2024], p. 11.

[100] Smith, M. J. and Emanuel, E. J. (2023) Learning from five bad arguments against mandatory vaccination. *Vaccine*, 41 (21), p. 3302.

[101] Explanations relating to the Charter of Fundamental Rights (2000), *op. cit.*

rights compatibility of the specific technological measures deployed in the context of the Covid pandemic, the analysis shows that the ECtHR attaches importance to a State's flexibility or 'margin of discretion' in times of crisis.

Notably, the current legal framework within the EU and the broader European context permits States to legitimately restrict or derogate from human rights in extraordinary circumstances, in order to protect and uphold other fundamental rights and interests such as public health or human life. In the EU in particular, MS do not have to base the relevant data processing on their citizens' consent as long as they ensure lawfulness, proportionality and appropriate safeguards for such processing. Nevertheless, many EU MS opted for consent in the context of the deployment and use of pandemic tech such as digital contact tracing, with the consequence that the functionality of such technologies may have been compromised, and the knock on effect of potentially compromising the health of other citizens.

The use of digital certificates also impinges on fundamental rights, in particular privacy and data protection, and raises concerns about possible discrimination. However, such discriminatory measures may in fact be socially justifiable, and it remains to be seen how the ECtHR would rule in a specific case scenario.

The present analysis aims to bolster future pandemic preparedness and responses. European human rights legal frameworks would appear to stand us in good stead, but this effectiveness can be compromised in contexts which are extraordinary and where knowledge and understanding of the health threat posed is limited. In such circumstances it is important to resist overstating the primacy of certain rights over others, in the face of an important or even essential public interest, such as public health. This is not to say that this paper advocates for undue deference to State interests or going down the slippery slope towards a totalitarian surveillance regime, but it rather advocates for ensuring a sustained role for protective mechanisms such as lawfulness (including legal guarantees or safeguards), proportionality, and judicial review, while keeping public interest goals squarely in focus.

LIST OF REFERENCES

[1] Advocate General Kokott. (2014) *Opinion procedure 2/13 initiated following a request made by the European Commission*. (ECLI:EU:C: 2014:2454) 7 June.

[2] Akinsanmi, T. and Salami, A. (2021) Evaluating the trade-off between privacy, public health safety, and digital security in a pandemic. *Data & Policy 3*, e27. Available from: https://doi.org/10.1017/dap.2021.24

[3] Burdinski, A., Brockmann, D. and Maier, B. F. (2022) Understanding the impact of digital contact tracing during the Covid-19 pandemic. *1*PLOS Digital Health, 1 (12).

[4] *Charter of Fundamental Rights of the European Union*, 18 December 2000 (C 83/02). Available from: https://www.europarl.europa.eu/charter/pdf/text_en.pdf [Accessed 26 January 2024].

[5] CoE Steering Committee on Anti-Discrimination, Diversity and Inclusion. (2020) *COVID-19: an analysis of the anti-discrimination, diversity and inclusion dimensions in Council of Europe Member States*. 11 November. Available from: https://edoc.coe.int/en/living-together-diversity-and-freedom-in-europe/9741-covid-19-an-analysis-of-the-anti-discrimination-diversity-and-inclusion-dimensions-in-council-of-europe-member-states.html [Accessed 26 January 2024]

[6] *Communauté Genevoise d'Action Syndicale (CGAS) v. Switzerland* (2022). No. 21881/20.

[7] *Consolidated Version of the Treaty on the European Union*, 26 October 2012 (C 326/13). Available from: https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF [Accessed 26 January 2024]

[8] Council of Europe. (1950) *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*. 4 November (ETS 5).

[9] *Dudgeon v. the United Kingdom* (1981). No. 752576.

[10] ECtHR (2022). *Guide on Article 14 of the European Convention of Human Rights and on Article 1 of Protocol No. 12 to the Convention. Prohibition of Discrimination*. 31 August.

[11] European Commission. (2022) *Digital Contact Tracing Study*. Luxembourg: Publications Office of the European Union. Available from: https://doi.org/10.2759/146050

[12] European Commission. (2022) *Report from the Commission to the European Parliament and the Council pursuant to Article 16(3) of Regulation (EU)*

2021/953 of the European Parliament and of the Council on the Framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certfication) to facilitate free movement during the COVID-19 pandemic. 22 December. Available from https://commission.europa.eu/publications/key-documents-related-digital-covid-19-certificate_en

[13] European Data Protection Board, *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, Adopted on 21 April 2020. Available from: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf [Accessed 26 January 2024].

[14] Explanations relating to the Charter of Fundamental Rights. *Official Journal of the European Union* (2007/C 303/02) 14 December. Available from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0017:0035:en:PDF [Accessed 26 January 2024].

[15] Halpin, H. (2022) A Critique of EU Digital COVID-19 Certificates: Do Vaccine Passports Endanger Privacy? *The 17th International Conference on Availability, Reliability and Security*. Vienna, Austria. Available from: https://dl.acm.org/doi/10.1145/3538969.3544459 [Accessed 26 January 2024].

[16] Judgment of 18 December 2014, Abdida, C-562/13, ECLI:EU:C:2014:2453.

[17] Kokott, J. and Sobotta, C. (2015) Protection of Fundamental Rights in the EU: On the Relationship between EU Fundamental Rights, the European Convention and National Standards of Protection, *Yearbook of European Law*, 34 (1)

[18] *Kudrevičius and Others v. Lithuania [GC]* (2015). No. 37553/05.

[19] Kuner, C., Bygrave L. A., Docksey, C. and Drechsler, L. (eds.) (2021). *The EU General Data Protection Regulation (GDPR), A Commentary*. New York: Oxford University Press.

[20] Leiser, M. R. and Caruana, M. M. (2020) *Some Contrarian Thoughts on the Deployment of Contact-Tracing Apps*. Available from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3608677 [Accessed 15 February 2024].

[21] Lenaerts, K. (2012) Exploring the Limits of the EU Charter of Fundamental Rights. *European Constitutional Law Review*, 8 (3)

[22] Litan, R. E. and Lowy, M. (2020) *Freedom and privacy in the time of coronavirus*. [online]. Washington DC: Brookings. Available from: https://www.brookings.edu/articles/freedom-and-privacy-in-the-time-of-coronavirus/ [Accessed 26 January 2024].

[23] *Malta Contact Tracing and Alerting Mobile Application Order, Subsidiary Legislation 465.52, adopted by Legal Notice 379 of 2020 as amended by Legal Notice 128 of 2021*. In: English

[24] Mifsud Bonnici, J. P. (2013). Exploring the non-absolute nature of the right to data protection. *International Review of Law, Computers & Technology*. 28 (2)

[25] Mohapatra, S. (2020) Passports of Privilege. *American University Law Review*, 70.

[26] *Pasquinelli and Others v. San Marino* (2024). No. 24622/22.

[27] *Piperea v. Romania* (2022). No. 24183/21.

[28] Registrar of the European Court of Human Rights, (2023) *An association's application concerning anti-Covid measures banning public events in Switzerland 2020 is inadmissible*. [press release] 27 November. Available from: [Accessed 26 January 2024].

[29] Registrar of the European Court of Human Rights. (2022) *Complaint against Romanian COVID-19 measures inadequately substantiated, inadmissible*. [press release] 1 September. Available from: `https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=003-7416653-10152416&filename=Decision\%20Piperea\%20v.\%20Romania\%20-\%20Complaint\%20against\%20Romanian\%20COVID-19\%20measures\%20inadmissible.pdf` [Accessed 26 January 2024].

[30] Registrar of the European Court of Human Rights. (2021) *The European Court of Human Rights declares inadmissible an application contesting the French "health pass"*. [press release] 7 October. Available from: `https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=003-7145978-9686694&filename=Decision\%20Zambrano\%20v.\%20France\%20-\%20application\%20which\%20was\%20challenging\%20the\%20French\%20\%E2\%80\%9Chealth\%20pass\%E2\%80\%9D.pdf` [Accessed 26 January 2024].

[31] Regulation (EU) 2021/953 of the European Parliament and of the Council of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic. *Official Journal of the European Union* (OJ L 211/1) 14 June. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02021R0953-20220630` [Accessed 26 January 2024].

[32] *S.A.S v. France* (2014). Np. 43835/11.

[33] Shahroz, M. et al. (2021) COVID-19 digital contact tracing applications and techniques: A review post initial deployments. *Transportation Engineering*, 5 (100072).

[34] Smith, M. J. and Emanuel, E. J. (2023) Learning from five bad arguments against mandatory vaccination. *Vaccine*, 41 (21).

[35] *Terhes v. Romania* (2021). No. 49933/20.

[36] *Thevenon v. France* (2022). No. 46061/21.

[37] Vardanyan, L. and Stehlik, V. (2022) Is the Case Law of the ECtHR Ready to Prevent the Expansion of Mass Surveillance in Post-Covid Europe? *Sciendo*, 7

[38] *Vavřička and others v. the Czech Republic* (2021). Nos. 47621/13, 3867/14, 73094/14, 19298/15, 19306/15 and 43883/15.

[39] Ventrella, E. (2020) Privacy in emergency circumstances: data protection and the COVID-19 pandemic. *ERA Forum*, 21 (3)

[40] Vyhnánek, L., Blechová, A., Bátrla, M., Míšek, J., Novotná, T., Reichman, A., Harašta, J., 2024. The Dynamics of Proportionality: Constitutional Courts and the Review of COVID-19 Regulations. *German Law Journal 25*, pp. 386–406

[41] WHO. *Global Digital Health Certification*. [online] Available from: *https://www.who.int/initiatives/global-digital-health-certification-network* [Accessed 26 January 2024].

[42] WHO. (2023) *Statement on the fifteenth meeting of the IHR (2005) Emergency Committee on the COVID-19 pandemic*. 5 May. Available from: `https://www.who.int/news/item/05-05-2023-statement-on-the-fifteenth-meeting-of-the-international-health-regulations-(2005)-emergency-committee-regarding-the-coronavirus-disease-(covid-19)-pandemic` [Accessed 26 January 2024].

[43] *Zambrano v. France* (2021). No. 41994/21.

DOI 10.5817/MUJLT2025-1-3

INFLUENCER MARKETING – DO WE NEED A NEW LAW OR A NEW APPROACH? FEW REMARKS FROM THE EUROPEAN AND POLISH PERSPECTIVE

by

JOANNA WISZNIEWSKA *

Facebook, Instagram, TikTok - any social media is full of advertising. The history of celebrity endorsement of products is nothing really new, but Internet brought it to the extreme level. A wide range of global population has been relying on influencers for all sorts of information. It creates the great responsibility as influencer marketing may lead to faulty advertising and misinformation, especially among minors and people with low digital literacy. Until recently influencers and their activities were not the subject of particular legal interest. These issues are currently addressed through tailored legislation neither at EU level nor in national regulations. To compensate for it, the last few years have seen a proliferation of soft law (regulatory guidelines) and industry self-regulatory measures to provide greater transparency. But is soft law combined with case law enough to provide the desired standard of consumer protection in the whole Single Market? Since platforms and technologies change at fast pace are we able to create a regulation that will not lag behind the development of the market? The digital environment in which influencer marketing takes place, which can hardly be confined to one country, creates additional challenges for legislators. The objective of the article is twofold: firstly, to present the existing legal framework at the EU and Polish levels; and secondly, to identify potential weaknesses in these regulations in the context of influencer marketing.

* PhD, Chair of Intellectual Property Law, Jagiellonian University, Kraków, Poland, e-mail: joanna.wiszniewska@uj.edu.pl, ORCID: 0000-0003-2970-8005

KEY WORDS
advertisement, influencer marketing, advertisement disclosure, advertisement law, social media

1. INTRODUCTION

It is a common truth that the internet and social media are not the same as they were when they were first introduced. The social media market is changing dynamically, with new successful portals such as the video-sharing platform TikTok, launched in 2016, continuing to emerge. Most of today's largest and most popular platforms and sites were created in the early 2000s and the Internet itself has an even longer history.[1] Nevertheless, the emergence of Web 2.0 and the 'demotic turn' - as Turner terms it - associated with the provision of communication platforms that facilitated two-way interaction between individuals and large audiences is identified as a watershed moment.[2] Another turning point was the introduction of Web 3.0 - the facilitation of access to social media platforms via applications on mobile devices hugely increased the popularity of Facebook, Instagram, etc.[3]

The term 'social media' (understood as a marketing tool) originated in the 1990's and now primarily refers to profile-based everyday communication platforms, such as the aforementioned Facebook and Instagram.[4] The strategic use of influencer marketing (IM) as a marketing tactic has gained extreme popularity over the course of recent years. The global value of the IM market is estimated to have risen from 3 billion to 21,1 billion US dollars between 2017 and 2023.[5] The phenomenon of IM has been extensively discussed in the literature in recent years, with contributions from marketing, psychology and social science perspectives.[6] Despite this, there has been little

[1] The year 1969 is sometimes cited as the beginning of social media, when the US internet provider CompuServe offered the service, or 1979, when the UseNet newsgroup system was made available in the US - for further information, see, McIntyre, K. (2014). The evolution of social media from 1969 to 2013: A change in competition and a trend toward complementary, niche sites. *The Journal of Social Media in Society*, 3(2), p. 8.

[2] Turner, G. (2010). Ordinary People and the Media: The Demotic Turn. *Theory, Culture & Society*. London: SAGE Publications. Available from: https://doi.org/10.4135/9781446269565 [Accessed 14 January 2024].

[3] Leung, F.F., Gu, F.F. and Palmatier, R.W. (2022). Online influencer marketing. *J. of the Acad. Mark. Sci.* 50, pp. 226-251. Available from: https://doi.org/10.1007/s11747-021-00829-4 [Accessed 7 January 2024].

[4] Meikle, G. (2016). *Social Media: Communication, Sharing and Visibility*. [online] New York; London: Routledge, p. 5. Available from: doi.org/10.4324/9781315884172 [Accessed 7 January 2024].

[5] Statista (2023). *Influencer marketing market size worldwide from 2016 to 2023*. Available from: https://www.statista.com/statistics/1092819/global-influencer-market-size/ [Accessed 7 January 2024].

[6] See e.g., Fowler, K., Thomas, V. (2023). Influencer marketing: a scoping review and a look ahead, *Journal of Marketing Management*, 39:11-12, pp. 933-964. available from: doi.org/10.

academic research on current legal issues especially from the perspective of EU law[7], whereas Polish approaches to influencer marketing have not yet been discussed in international journals at all. This article summarises the preliminary findings of a research project and addresses this gap. Presenting the Polish model in the light of European regulation can add value to understanding the complexity of the world of influencer marketing and the regulatory and enforcement strategies in different EU countries. It is a contribution to the wider European debate on consumer protection online, particularly in digital advertising.

The article firstly underscores the distinctiveness of influencer marketing in comparison to alternative forms of advertising. This is followed by an analysis of the relevant EU and Polish law and a discussion of their applicability to influencer marketing. The next section provides comments on the first Polish regulatory guidelines "Recommendations pertaining to the tagging of advertising content by influencers on social media" published on 26 September 2022. The article ends with a conclusion.

2. THE INFLUENCER MARKETING PHENOMENON

The traditional celebrity endorsement model understood as the use of celebrities to promote and endorse products or services is not really new.[8] Indeed, for more than a century actors or athletes have lent their image to promote various goods or services.[9] The Internet has not only taken this phenomenon to a whole new level, but it has also led to the emergence of influencers, a new group that is extremely attractive to advertisers. Leung, Gu and Palmatier define online influencers as "individuals, groups of individuals, or even virtual avatars who have built a network of followers on social media and are regarded as digital opinion leaders with significant

1080/0267257X.2022.2157038 [Accessed 20 November 2023] or Vrontis, D, Makrides, A, Christofi, M, Thrassou, A. (2021) Social media influencer marketing: A systematic review, integrative framework and future research agenda. *Int J Consum Stud*. 45, pp. 617-644. available from: doi.org/10.1111/ijcs.12647 [Accessed 14 January 2024].

7 For general legal remarks see Goanta, C. and Ranchordas, S. (2020). *The Regulation of Social Media Influencers*. Northampton: Edward Elgar Publishing.

8 For more detail, see e.g., Erdogan, B.Z. (1999). Celebrity Endorsement: A Literature Review, *Journal of Marketing Management*, 15:4, pp. 291-314, Available from: doi.org/10.1362/026725799784870379 [Accessed 14 January 2024] or Proctor, T., and Kitchen, P.J. (2019). Celebrity ambassador/celebrity endorsement - takes a licking but keeps on ticking, *Journal of Strategic Marketing*, 27:5, pp. 373-387, Available from: doi.org/10.1080/0965254X.2018.1430059 [Accessed 14 January 2024].

9 Piehler, R., Schade, M., Sinnig, J., Burmann, C. (2022). Traditional or 'instafamous' celebrity? Role of origin of fame in social media influencer marketing, *Journal of Strategic Marketing*, 30(4), p. 409. Available from: doi.org/10.1080/0965254X.2021.1909107 [Accessed 6 January 2025].

social influence on their network of followers."[10] The most significant difference between celebrities and influencers is in the source of their recognisability. Although there are exceptions, most influencers gain popularity and accumulate followers by creating and actively sharing content on social media that purports to represent their everyday lives and opinions.[11] This phenomenon is referred to as the so-called "original influencers."[12]

An increasing number of Internet users search the web for information on any subject, facing both neutral content (information in the strict sense) and content that directly or indirectly encourages the purchase of specific goods or services. If this content is not properly labelled and, for example, profiled based on a person's previous online activities, it is amazingly easy to disseminate misleading information to consumers. This is particularly evident when the content is presented by a person with whom the Internet user has a pre-existing relationship of some kind, as is often the case with influencers.

So-called original influencers are someone between a close friend and an admired celebrity for their social media audience.[13] On the one hand, they may have similar interests, values, or lifestyles, which can be reflected in the language they use, for example. On the other hand, like celebrities they develop their public image.[14] Because of their closer relationship with their audience, influencer content is often not perceived as marketing.[15] The most significant issue arises when the content published by the influencer gives the impression of a neutral sharing of lifestyle, information about products and services used etc. with the audience, whereas it is tailor-made and is a (sometimes essential) part of the marketing strategy. The absence of

[10] Leung, F.F., Gu, F.F. and Palmatier, R.W. (2022). *Op. cit.* p. 228.

[11] Ibid.

[12] Schouten, A. P., Janssen, L. and Verspaget M. (2020). Celebrity vs. Influencer endorsements in advertising: the role of identification, credibility, and Product-Endorser fit, *International Journal of Advertising*, 39(2), pp. 258-281, Available from: doi.org/10.1080/02650487.2019.1634898 [Accessed 14 January 2024].

[13] Balaban, D.C., Szambolics, J., Chiric, M. (2022) Parasocial relations and social media influencers' persuasive power. Exploring the moderating role of product involvement. *Acta Psychologica* 230, 103731, pp.1-3, Available from: doi.org/10.1016/j.actpsy.2022.103731 [Accessed 6 January 2025].

[14] Belanche, D. et. al. (2021). Building influencers' credibility on Instagram: Effects on followers' attitudes and behavioural responses toward the influencer, *Journal of Retailing and Consumer Services*, 61, pp. 1-11, Available from: https://doi.org/10.1016/j.jretconser.2021.102585 [Accessed 7 January 2024].

[15] Farivar, S., Wang, F. and Yuan, Y. (2021), Opinion leadership vs. para-social relationship: Key factors in influencer marketing, *Journal of Retailing and Consumer Services*, 59, Available from: https://doi.org/10.1016/j.jretconser.2020.102371 [Accessed 14 January 2024].

proper labelling of such content, particularly when it is not clearly designated as advertising, can result in a misperception among the audience. This, in turn, can have a heightened impact on the recipients.[16] Consequently, such practices can result in the dissemination of deceptive and misleading advertising, and given the aforementioned factors, this risk is amplified in the context of IM relative to conventional advertising. This aspect should be duly considered in the legal regulations designed to safeguard consumers.

3. THE CURRENT LEGAL FRAMEWORK IN THE EU

Currently, there are no general regulations in either EU or Polish law that directly refer to influencers or their advertising activities. However, this obviously does not mean that influencers operate in a complete legal vacuum.

From a legal perspective, influencers can be considered as advertisers/traders and as sellers/producers. For the purposes of this article, the first of these roles is of particular interest. At least in theory, four pieces of EU legislation may apply to influencers: the Unfair Commercial Practices Directive (UCPD)[17], the e-Commerce Directive[18], the Audiovisual Media Services Directive (AVSMD)[19]and the Digital Services Act (DSA)[20].

---

[16] Interestingly, recent research findings suggest that the provision of correct disclosures does not have a detrimental effect on the level of engagement exhibited by followers. See Bertaglia, T., Goanta, C., Spanakis, G., Iamnitchi, A. (2025) Influencer self-disclosure practices on Instagram: A multi-country longitudinal study, *Online Social Networks and Media*, Volume 45,100298, p.9-12. Available from: https://doi.org/10.1016/j.osnem.2024.100298. 1705267093852. [Accessed 6 January 2025].

[17] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), *Official Journal of the European Union* (2005/L 149) 11 June, pp. 22-39. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005L0029 [Accessed 2 January 2024]

[18] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), *Official Journal of the European Union* (2000/L 178) 17 July, pp. 1-16. Available from: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32000L0031&qid=1705267093852 [Accessed 2 January 2024]

[19] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities, *Official Journal of the European Union* (2018/L 303) 28 November, pp. 69-92. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1808 [Accessed 2 January 2024].

[20] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), Official Journal of the European Union (2022/L 277) 27 October. Available

3.1.THE UNFAIR COMMERCIAL PRACTICES DIRECTIVE

The UCPD provides a legal framework within which misleading advertising and commercial practices are to be addressed. While the law itself does not regulate influencers directly, it should be interpreted in conjunction with the "The European guidance on the interpretation and application of the UCPD" (European Guidance) issued in 2021.[21]

According to the guidelines, the UCPD applies when an influencer acts as a trader, or, alternatively, as a person acting in the name or on behalf of a trader, regardless of the size of the influencer's audience. It is worth noting that the authors of the guidelines have accurately distinguished between the activities of influencers, who are paid to publish their opinions, and the 'ordinary' online expression of opinions about goods or services by consumers.[22] The European Guideance clearly indicates that the failure to properly identify advertising content in social media posts or other influencer practices (e.g., affiliate content, tagging the trader/brand) for which they are paid may constitute a misleading practice under Article 6 and 7 of the UCPD.[23] In addition, the failure to clearly disclose the promotional nature of the content published may violate Annex I, point 11 of the UCPD (prohibition of practices that do not make it clear that a trader has paid for the promotion of a product in editorial content) as well as Annex I, point 22 (prohibition of misrepresenting oneself as a consumer).

Although some influencers may find this counterintuitive, from a legal perspective, it is reasonable to consider the content to be of commercial character whenever the author receives any form of remuneration (discounts, partnership arrangements, percentage from affiliate links, free products - including unsolicited gifts, trips or event invitations etc.) that is not

from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065 [Accessed 2 January 2024].

[21] Commission Notice - Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (Text with EEA relevance), *Official Journal of the European Union* (2021/C 526) 29 December, p. 1-129. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021XC1229(05) [Accessed 2 January 2024]. For a comparison of how the UCPD was interpreted in the context of influencer marketing before the adoption of the European Guidance see Trzaskowski, J. (2018) Identifying the Commercial Nature of 'Influencer Marketing' on the Internet. *Scandinavian Studies in Law*, 65 ('50 Years of Law and IT'), SSRN, pp. 81-100, Available from: https://ssrn.com/abstract=3324103 [Accessed 13 January 2024].

[22] 'The UCPD does not apply to consumers who provide information about their experience with products or services, unless they can be considered as acting "in the name of or on behalf of a trader" see European Guidance, *Op. cit.* p. 94.

[23] Ibid. p. 98.

necessarily a monetary payment.[24] In light of the distinctive character of the relationship between the influencer and his or her audience, as discussed in section 2 of the article, the mislabelling of content by the influencer can also be assessed from the perspective of an aggressive commercial practice through the use of undue influence.[25]

As is apparent from the European Guidance, there is a need for precise application of the UCPD to the sphere of influencer marketing. However, given the directive's requirement for implementation in EU countries, it would be advisable for the act itself to explicitly include any newly emerging forms of marketing. In its current state, there is potential for legal uncertainty regarding the application of the laws, possible gaps in protection in certain areas, and the need for additional guidelines.

3.2.THE E-COMMERCE DIRECTIVE

In accordance with stipulations set out in the e-Commerce Directive, the provision of commercial information, which constitutes an information society service or a part thereof, must be clearly identifiable as such. The Directive defines this term as any form of information designed to promote, directly or indirectly, the goods, services or image of an undertaking, organisation or person engaged in a commercial, business, craft or regulated profession in so far as it is not information relating to the goods, services or image of the undertaking, organisation or person, compiled in an independent manner, in particular where it is given without any financial consideration.[26]

Consequently, the content published by influencers as a result of paid advertising collaborations will be considered commercial information with all the legal consequences that this entails. In the context of influencer marketing, the following information obligations will be primarily relevant: the clear identification of commercial communication, the identifiability of the advertiser, and the clear and unambiguous presentation of the conditions of promotional offers, competitions, or games.[27] It is worth noting that the definition of commercial communication appears to be broad and, unlike the UCPD, includes all forms of 'indirect' advertising.

---

[24] European Guidance, *Op. cit.* p. 98.

[25] Prohibited by Articles 8-9 UCPD.

[26] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). *Official Journal of the European Union* (2013/C-187/08) 8 June. Available from: `http://data.europa.eu/eli/dir/2000/31/2024-02-17`, Article 2(f)

[27] Ibid. Article 6

Nevertheless, it should be emphasized that the regulation adopted in the e-commerce directive is also not comprehensive leaving outside its scope the content published by influencers without remuneration or when it would not be considered an information society service

3.3.THE AUDIOVISUAL MEDIA SERVICES DIRECTIVE

The AVSMD, on the other hand, affects influencers who have 'editorial responsibility' over an 'on-demand audiovisual media service' in relation to user-generated videos disseminated through these platforms, and which may contain commercial communications. The Directive itself introduces specific new rules for 'video-sharing platform services' and regulates three forms of commercial communication (advertising, sponsorship, product placement).[28]

In general, advertising should be recognisable and distinguishable from editorial content and other commercial relationships with traders must not affect the editorial independence or give undue prominence to products.[29]

3.4.THE DIGITAL SERVICES ACT

According to the DSA, illegal content is 'any information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State which is in compliance with Union law, irrespective of the precise subject matter or nature of that law'.[30] Such unlawful content may be advertising disseminated by online intermediaries that is in breach of EU law or the law of a Member State. This results in the possibility to apply to those who publish illegal content, for example, the provisions on liability of intermediaries (Article 6 DSA) or obligation to act upon orders directed against illegal content (Article 9 DSA).[31]

The definition of advertising itself in the DSA differs significantly in scope from the definition of commercial information in the e-commerce Directive. Article 3(r) of the DSA defines advertising as 'information designed to promote the message of a legal or natural person, irrespective of whether to achieve commercial or non-commercial purposes, and presented by an online platform on its online interface against remuneration specifically for promoting that information'. This means that advertising within the meaning

[28] Article 9-11 of the AVSMD.

[29] Trzaskowski, J. (2018), *op.cit.*, p.90.

[30] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). *Official Journal of the European Union* (2022/2065) 27 October, Article 3(h)

[31] Duivenvoorde, B. and Goanta, C. (2023). The regulation of digital advertising under the DSA: A critical assessment. *Computer Law & Security Review*, 51, p. 5. Available from: `https://doi.org/10.1016/j.clsr.2023.105870` [Accessed 15 December 2023].

of the DSA will also include, for example, promotional activities carried out by NGOs which are not intended to be commercial in nature.

However, this broad definition of advertising makes it difficult to apply to influencer marketing. Although influencers mostly use online platforms to publish their content (including marketing materials), the absence of any form of compensation to the platform for the promotion of this content poses a challenge in categorising such actions as advertising under the DSA.

Thus, problems of inappropriate (or non-existent) labelling of advertising content by influencers are not solved by the regulation in Article 26 of the DSA. It requires online platform providers to ensure, inter alia, that for each specific advertisement presented to each individual recipient, it is possible to identify, in a clear, concise and unambiguous manner and in real time, the following: the advertising nature of the content, the entity for which the advertisement is presented and the entity that paid for the advertisement.

These issues, among others, were already highlighted during the work and drafting of the DSA in the Report of the Committee on the Internal Market and Consumer Protection (IMCO) in 2021.[32] This document called for changes by adding content to the preamble with content explicitly covering influencers, broadening the definition of advertising and transparency reporting requirements for intermediary service providers.[33] Unfortunately, these proposals were not adopted. In addition, it should be emphasised that even if influencers were explicitly covered by the DSA as postulated by IMCO, influencers who publish advertising content, e.g., on blogs, that are not part of online platforms, would still remain outside the regulation. Meanwhile, the DSA should be considered to exclude influencer marketing from its material scope.[34]

4. THE ROLE OF MEMBER STATES' LEGISLATION ON THE EXAMPLE OF THE POLISH EXPERIENCE

While, as mentioned above, the general rules on advertising at EU level apply to some extent to influencer advertising, the scope of their application remains problematic. In 2024, the efficacy of the EU consumer law with regard to digital fairness was assessed as limited, primarily due to the existence of legal uncertainty and the risk of regulatory fragmentation

[32] Draft Report on the proposal for a regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM(2020)0825 - C9-0418/2020 - 2020/0361(COD)) (2021) 28 May. Available from: https://www.europarl.europa.eu/doceo/document/IMCO-PR-693594_EN.pdf [Accessed 15 January 2024].

[33] Currently Article 15 DSA - Article 13 in the draft DSA referred to in the report.

[34] Duivenvoorde, B. and Goanta, C. (2023). op. cit. p. 13

resulting from divergent interpretations and implementations.[35] It is important to note that, with the exception of the DSA, all of the aforementioned EU legal acts are directives. Consequently, Member States retain the prerogative to implement their respective regulations concerning the marketing of influencers. . The European Economic and Social Committee (EESC) in its opinion of 2023 lists the following among the possible actions by Member States[36]:

- adopt specific legislation on influencers;
- implement existing consumer protection legislation;
- publish guides and codes of conduct to establish good practices;
- use digital control and enforcement tools;
- provide training and certification for influencers;
- raise awareness and support consumers;
- facilitate compliance on platforms through standardised dissemination tools.

From the perspective of Polish law, the failure to indicate advertising content or its incorrect marking may constitute a misleading omission under the Act of 23 August 2007 on Counteracting Unfair Market Practices.[37] A particularly common misleading omission, which has been observed to be particularly tempting for influencers, is the failure to disclose the commercial purpose of a practice[38], if it is not clear from the circumstances and if it causes or is likely to cause the average consumer to take a contractual decision that he would not have taken otherwise[39] and surreptitious advertising[40]. On the other hand, surreptitious advertising may also constitute an act of unfair

[35] European Commission. (2024) *Staff Working Document Executive Summary of the Fitness Check of EU consumer law on digital fairness (SWD(2024) 231 final).* Available from: `https://ec.europa.eu/f45c3742-d4d5-461f-bfea-3ce3e6bb5d26` [Accessed 6 January 2025]

[36] Hernandez Bataller, B., and Palmieri, S. *Opinion European Economic and Social Committee. Advertising through influencers and its impact on consumers [Exploratory opinion requested by the Spanish presidency].* INT/1026-EESC-2023-01-01-01658-00-01-AC-TRA. Adopted at plenary on 13 July 2023. Available from: `https://webapi2016.eesc.europa.eu/v1/documents/EESC-2023-01658-00-01-AC-TRA-EN.docx/content` [Accessed 10 January 2024].

[37] *Act of 23 August 2007 on Counteracting Unfair Market Practices (item 2070).* Poland. Journal of Laws 2017. In: Polish

[38] This can manifest itself in a complete lack of labelling, insufficient labelling e.g., only "#co-operation" without further explanation, also in a way that is almost invisible to the consumer, or marking posts as advertising only a few days after publication of the material, when many viewers will no longer be familiar with the corrected material.

[39] Articles 6.1 and 6.3.2 Act of 23 August 2007 on Counteracting Unfair Market Practices. *Op. cit.*

[40] Article 7 Act of 23 August 2007 on Counteracting Unfair Market Practices.*Op. cit.*

competition in the field of advertising under the Act of 16 April 1993 on Combating Unfair Competition[41], if it infringes the interests of entrepreneurs whose are activities in competition with those of the advertiser.[42]

In September 2022, in order to prevent inappropriate labelling that may have resulted from a lack of awareness among the influencers and other social media users, the President of the Polish Office for Competition and Consumer Protection (UOKiK) published *Recommendations of the President of UOKiK on the labelling of advertising content by influencers on social media*.[43] It has to be appreciated that the document next to the clearly explained legal background offers a number of practical tips to enable an influencer to determine whether a given collaboration should be assessed as commercial (especially if the influencer receives a material benefit of different kind instead of monetary remuneration). The correct assessment of the collaboration will determine the commercial nature of the publication and then determine the extent to which the content is correctly labelled. It seems particularly valuable to emphasise that content published by an influencer may also constitute advertising, even if the client has no impact on the content of the influencer's opinion.[44] For some influencers, it is not intuitive to classify such communication as commercial.

The forms of labelling recommended in the document differ significantly from those currently used by influencers to date. Among other things, it is recommended to use two levels of labelling (standard labelling of an advertisement provided by a social media platform and own description in the content of the material, e.g., in the description or in the photo).[45] Labelling should be clear, unambiguous, and comprehensible, e.g., it

---

[41] *Act of 16 April 1993 on Combating Unfair Competition (item 1233).* Journal of Laws 2022. In: Polish

[42] Article 16.1.4 Act of 16 April 1993 on Combating Unfair Competition. *Op. cit.*

[43] It is worth noting that the recommendations are part of a trend of similar documents - see Czech *Recommended Rules of Business Collaboration with Influencers* from 2020. (For more on the work on this document: Ortová, N., Hejlová, D. and Weiss, D. (2023) Creation of a Code of Ethics for Influencer Marketing: the Case of the Czech Republic, *Journal of Media Ethics*, 38(2), pp. 65-79, Available from doi.org/10.1080/23736992.2023.2193958, Accessed [13 January 2024] . For regulations in the Nordic countries introduced since 2016 see Abidin, C. et al. (2020) A review of formal and informal regulations in the Nordic influencer industry. *Nordic Journal of Media Studies*, 2, pp. 71-83. Available fromhttps://www.doi.org/10.2478/njms-2020-0007. Accessed [13 January 2024], or UK (2020) *An Influencer's Guide to making clear that ads are ads*. [online] Available from: https://www.asa.org.uk/static/uploaded/3af39c72-76e1-4a59-b2b47e81a034cd1d.pdf Accessed [13 January 2024]

[44] Recommendations of the President of UOKiK pertaining to the tagging of advertising content by influencers on social medias (2022) p.7. Available from https://uokik.gov.pl/download.php?plik=26686.Accessed [5 January 2024].

[45] Recommendations of the President of UOKiK pertaining to the tagging of advertising content by influencers on social medias (2022), *op. cit.* p.16.

is not sufficient to include the hashtag #ad in the post or even a full description in a foreign language (e.g., #advertisement).[46] In the case of advertisements, the options for correct labelling include in Polish: "XYZ brand advertisement" ('reklama marki XYZ'), "#advertisement or [advertisement]" ('#reklama lub [reklama]"),, "#AdvertisingMaterial or [advertising material]" („#MateriałReklamowy lub [materiał reklamowy]"),, "#PostSponsored or [sponsored post]" („#PostSponsorowany lub [post sponsorowany]).[47]

5. CONCLUSION

Influencer marketing is a relatively new phenomenon that is characterised by significant diversity. However, there is no doubt that it is an issue that needs to be addressed from a legal perspective. Until recently, this phenomenon has not been the subject of much interest either at the EU level or in Poland, but this is changing. Nevertheless, it is still unclear to what extent the current general provisions of advertising law can be applied to the activities of influencers. In particular, the DSA has not made the expected breakthrough, as its definition of advertising, does not include influencer marketing in its material scope.

Given the risks to consumers that may arise from mislabelled content, it seems necessary to adopt a flexible approach right now and to apply consumer protection and unfair competition rules to influencer activities as far as possible. In the near future, it will probably be necessary to comprehensively review the advertising and consumer protection rules as a whole and, if not rewrite them, at least clarify them so that there is no doubt that they all apply in both the offline and online world.

The current regulations are dispersed across a variety of legislation, with their scopes not overlapping, a situation that is not favourable to legal certainty. Moreover, there is an absence of sufficient case law to assess their practical functioning. For instance, Polish courts have not yet had the opportunity to analyse unfair practices concerning influencer marketing. It appears that the responsibility for clarifying the regulations has been passively transferred to the Member States, which is likely to result in divergence and regulatory fragmentation. Regulatory guidelines, while valuable and adaptable instruments, should serve as a complement to, rather than a substitute for, the legal framework. As studies demonstrate, the existence of well-defined guidelines is associated with higher levels of

[46] Recommendations of the President of UOKiK pertaining to the tagging of advertising content by influencers on social medias (2022), *op. cit.* p. 18.

[47] Recommendations of the President of UOKiK pertaining to the tagging of advertising content by influencers on social medias (2022), *op. cit.* p. 17.

compliance.[48] Therefore, Polish guidelines can serve as a valuable source of inspiration in the development of regulations at the EU level.

LIST OF REFERENCES

[1] McIntyre, K. (2014). The evolution of social media from 1969 to 2013: A change in competition and a trend toward complementary, niche sites. *The Journal of Social Media in Society*, 3(2), p. 5-25.

[2] Turner, G. (2010). Ordinary People and the Media: The Demotic Turn. *Theory, Culture & Society*. London: SAGE Publications. Available from: https://doi.org/10.4135/9781446269565 [Accessed 14 January 2024].

[3] Leung, F.F., Gu, F.F. and Palmatier, R.W. (2022). *Online influencer marketing. J. of the Acad. Mark. Sci.* 50, pp. 226–251. Available from: https://doi.org/10.1007/s11747-021-00829-4 [Accessed 7 January 2024].

[4] Meikle, G. (2016). *Social Media: Communication, Sharing and Visibility*. [online] New York; London: Routledge, p. 5. Available from: doi.org/10.4324/9781315884172 [Accessed 7 January 2024].

[5] Statista (2023). *Influencer marketing market size worldwide from 2016 to 2023*. Available from: https://www.statista.com/statistics/1092819/global-influencer-market-size/ [Accessed 7 January 2024].

[6] Fowler, K., Thomas, V. (2023). *Influencer marketing: a scoping review and a look ahead, Journal of Marketing Management*, 39:11-12, pp. 933-964. Available from: doi.org/10.1080/0267257X.2022.2157038 [Accessed 20 November 2023]

[7] Vrontis, D, Makrides, A, Christofi, M, Thrassou, A. (2021) *Social media influencer marketing: A systematic review, integrative framework and future research agenda*. Int J Consum Stud. 45, pp. 617–644. Available from: doi.org/10.1111/ijcs.12647 [Accessed 14 January 2024].

[8] Goanta, C. and Ranchordas, S. (2020). *The Regulation of Social Media Influencers*. Northampton: Edward Elgar Publishing.

[9] Erdogan, B.Z. (1999). *Celebrity Endorsement: A Literature Review, Journal of Marketing Management*, 15:4, pp. 291-314, Available from: doi.org/10.1362/026725799784870379 [Accessed 14 January 2024]

[10] Proctor, T., and Kitchen, P.J. (2019). *Celebrity ambassador/celebrity endorsement – takes a licking but keeps on ticking, Journal of Strategic Marketing*, 27:5, pp. 373-387, Available from: doi.org/10.1080/0965254X.2018.1430059 [Accessed 14 January 2024].

[48] Bertaglia, T., Goanta, C., Spanakis, G., Iamnitchi, A., Influencer self-disclosure practices on Instagram: A multi-country longitudinal study, (2025) *Online Social Networks and Media*, Volume 45,100298, p.9-12

[11] Piehler, R., Schade, M., Sinnig, J., Burmann, C. (2022). Traditional or 'instafamous' celebrity? Role of origin of fame in social media influencer marketing, *Journal of Strategic Marketing*, 30(4), p. 409. Available from: doi.org/10.1080/0965254X.2021.1909107 [Accessed 6 January 2025].

[12] Schouten, A. P., Janssen, L. and Verspaget M. (2020). Celebrity vs. Influencer endorsements in advertising: the role of identification, credibility, and Product-Endorser fit, International *Journal of Advertising*, 39(2), pp. 258-281, Available from: doi.org/10.1080/02650487.2019.1634898 [Accessed 14 January 2024].

[13] Balaban, D.C., Szambolics, J., Chiric, M. (2022) Parasocial relations and social media influencers' persuasive power. Exploring the moderating role of product involvement. *Acta Psychologica* 230, 103731, pp. 1-9. Available from: doi.org/10.1016/j.actpsy.2022.103731 [Accessed 6 January 2025].

[14] Belanche, D. et. al. (2021). Building influencers' credibility on Instagram: Effects on followers' attitudes and behavioural responses toward the influencer, *Journal of Retailing and Consumer Services*, 61, pp. 1-11, Available from: https://doi.org/10.1016/j.jretconser.2021.102585 [Accessed 7 January 2024].

[15] Farivar, S., Wang, F. and Yuan, Y. (2021), Opinion leadership vs. para-social relationship: Key factors in influencer marketing, *Journal of Retailing and Consumer Services*, 59, Available from: https://doi.org/10.1016/j.jretconser.2020.102371 [Accessed 14 January 2024].

[16] Bertaglia, T., Goanta, C., Spanakis, G., Iamnitchi, A. (2025), Influencer self-disclosure practices on Instagram: A multi-country longitudinal study, *Online Social Networks and Media*, Volume 45,100298, p.9-12. Available from: https://doi.org/10.1016/j.osnem.2024.100298. 1705267093852. [Accessed 6 January 2025].

[17] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), *Official Journal of the European Union* (2005/L 149) 11 June, pp. 22–39. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005L0029 [Accessed 2 January 2024].

[18] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services,

in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), *Official Journal of the European Union* (2000/L 178) 17 July, pp. 1-16. Available from: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32000L0031&qid=1705267093852 [Accessed 2 January 2024].

[19] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities, *Official Journal of the European Union* (2018/L 303) 28 November, pp. 69–92. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1808 [Accessed 2 January 2024].

[20] Commission Notice – Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (Text with EEA relevance), *Official Journal of the European Union* (2021/C 526) 29 December, p. 1-129. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021XC1229(05) [Accessed 2 January 2024].

[21] Commission Notice – Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (Text with EEA relevance), *Official Journal of the European Union* (2021/C 526) 29 December, p. 1-129. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021XC1229(05) [Accessed 2 January 2024].

[22] Trzaskowski, J. (2018) Identifying the Commercial Nature of 'Influencer Marketing' on the Internet. *Scandinavian Studies in Law*, 65 ('50 Years of Law and IT'), SSRN, pp. 81-100, Available from: https://ssrn.com/abstract=3324103 [Accessed 13 January 2024].

[23] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), *Official Journal of the European Union* (2022/L 277) 27 October. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065 [Accessed 2 January 2024].

[24] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), *Official Journal of the European Union* (2022/L 265) 12 October. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R1925&qid=1705330810771 [Accessed 2 January 2024].

[25] Duivenvoorde, B. and Goanta, C. (2023). The regulation of digital advertising under the DSA: A critical assessment. *Computer Law & Security Review*, 51, p. 5. Available from: https://doi.org/10.1016/j.clsr.2023.105870 [Accessed 15 December 2023].

[26] *Draft Report on the proposal for a regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM(2020)0825 – C9-0418/2020 – 2020/0361(COD))* (2021) 28 May. Available from: https://www.europarl.europa.eu/doceo/document/IMCO-PR-693594_EN.pdf [Accessed 15 January 2024].

[27] European Commission. *Staff Working Document Executive Summary of the Fitness Check of EU consumer law on digital fairness (SWD(2024) 231 final)*. Available from: https://ec.europa.eu/f45c3742-d4d5-461f-bfea-3ce3e6bb5d26 [Accessed 6 January 2025].

[28] Hernandez Bataller, B., and Palmieri, S. *Opinion European Economic and Social Committee. Advertising through influencers and its impact on consumers [Exploratory opinion requested by the Spanish presidency]*. INT/1026-EESC-2023-01-01-01658-00-01-AC-TRA. Adopted at plenary on 13th July 2023. Available from: https://webapi2016.eesc.europa.eu/v1/documents/EESC-2023-01658-00-01-AC-TRA-EN.docx/content [Accessed 10 January 2024].

[29] Ortová, N., Hejlová, D. and Weiss, D. (2023) Creation of a Code of Ethics for Influencer Marketing: The Case of the Czech Republic, *Journal of Media Ethics*, 38(2), pp. 65-79, Available from: doi.org/10.1080/23736992.2023.2193958 Accessed [13 January 2024]

[30] Abidin, C. et al. (2020) A review of formal and informal regulations in the Nordic influencer industry. *Nordic Journal of Media Studies*, 2, pp. 71–83. Available from: https://www.doi.org/10.2478/njms-2020-0007 Accessed [13 January 2024],

[31] (2020) *An Influencer's Guide to making clear that ads are ads*. [online] Available from: https://www.asa.org.uk/static/uploaded/3af39c72-76e1-4a59-b2b47e81a034cd1d.pdf Accessed [13 January 2024].

[32] *Recommendations of the President of UOKiK pertaining to the tagging of advertising content by influencers on social medias* (2022) p.7. Available from: https://uokik.gov.pl/download.php?plik=26686 Accessed [5 January 2024].

DOI 10.5817/MUJLT2025-1-4

EVOTING AT THE GERMAN SOCIAL ELECTIONS – LESSONS LEARNT

by

DOMENICA BAGNATO * ROBERT MÜLLER-TÖRÖK †
ÁLEXANDER PROSSER ‡ ROBERT STEIN §

With an electorate of 52m the German Social Elections (Sozialwahl) is arguably one of the largest single elections in the European Union. It elects representatives of all people under social security and has been conducted through postal voting only for decades. In 2023 eVoting was introduced as an additional voting channel for the first time. This paper focuses specifically on the eVoting part, particularly the technical requirements and the voting protocol used. It analyses them against general voting principles and the relevant Recommendation of the Council of Europe.

KEY WORDS

eVoting, Social Elections, voting principles, envelope protocol, homomorphism, Council of Europe Recommendation.

1. GENERAL FRAMEWORK

The "Sozialwahl" or Social Election is the third-largest election in Germany, about 52m people with either mandatory social security or pensioners elect their representatives in the self-governing bodies of the social security institutions. The voting right is not restricted to German citizens above 18 years of age like in General Elections, but also granted to foreigners who work

* University of Economics and Business, Vienna, email: domenica.bagnato@wu.ac.at
† University of Public Administration and Finance, Ludwigsburg, email: robert.mueller-toeroek@hs-ludwigsburg.de
‡ University of Economics and Business, Vienna, email: alexander.prosser@wu.ac.at
§ Federal Ministry of the Interior, Vienna, email: robert.stein@bmi.gv.at. This paper expresses his private opinion.

and hence pay mandatory social security or are pensioners and the voting right is also granted to working people from 16 years of age on.[1]

These representatives are in the so-called "Social Parliaments", one each in every social security institution. These institutions are the public German Pension Insurance and five health insurance funds (five large out of a total of 95 health insurance funds existing in Germany in 2023).[2] Their actual power and influence is limited to advice and supervision, normally they do not interfere in daily politics and business.[3] So, as compared to General Elections or Elections to Federal State Parliaments, city councils or county councils, the election is of far less significance – despite being an official, nationwide election governed by the law with voter rolls and all the requisites of a "normal" election.

It is regulated in Social Code IV, §§ 43-66.[4] The Federal Minister of Labour and Social Affairs issues the Election Decree, which is rarely changed.[5] The Social Election itself does not attract much public attention, political parties do not stand for this election and it is rarely disputed in the courts, hence it is suitable for an eVoting pilot. Different to other countries and elections, the competent court of appeal for this election is either the Social Court at the location of the German Pension Insurance or of the respective health insurance fund whose election is disputed. So the judicial appeal is not centralized at one single court, but rather spread among up to six out of 68 regional Social Courts at the first level, one or more out of 14 Social Courts of Federal States at the second level and the Federal Social Court at the third level.[6] So a final decision could appear years after the election was originally contested.

---

1 Cf. Bundesregierung (2023) *Wissenswertes zur Sozialwahl 2023*. [online] Berlin. Available: https://www.bundesregierung.de/breg-de/aktuelles/sozialwahl-2023-2188062 [Accessed 20 July 2025]

2 GKV Spitzenverband. *Die gesetzlichen Krankenkassen*. [online] Bonn. Available from: https://www.gkv-spitzenverband.de/krankenversicherung/kv_grundprinzipien/alle_gesetzlichen_krankenkassen/alle_gesetzlichen_krankenkassen.jsp [Accessed 19 June 2025]

3 Ibid.

4 *Sozialgesetzbuch (SGB) Viertes Buch (IV) - Gemeinsame Vorschriften für die Sozialversicherung* - (Artikel I des Gesetzes vom 23. Dezember 1976, BGBl. I S. 3845) (Social Code IV). In German. Available from: https://www.gesetze-im-internet.de/sgb_4/ [Accessed 20 June 2025]

5 Bundesministerium für Arbeit und Sozialordnung (1997). *Wahlordnung für die Sozialversicherung* (Election Decree for the Social Elections). In German. Available from: https://www.gesetze-im-internet.de/svwo_1997/ [Accessed 20 June 2025]

6 Cf. Nakielski, H. (2022). *Gerichte und Richter:innen der Sozialgerichtsbarkeit*. [online]. Available from: https://netzwerk-sozialrecht.net/gerichte-und-richterinnen-der-sozialgerichtsbarkeit/ [Accessed 20 June 2025]

The Social Election was introduced in 1953 and has been postal voting only, ie. pure distance voting. This makes it, at least from a cost perspective, interesting for an eVoting pilot. The participation has been declining for decades; despite the eVoting pilot, participation in the Social Election reached an all time-low in 2023 with a turnout of 22.43 % (30.42 % in 2017, the last election before the COVID-19-Pandemic).[7]

In 2022, it was decided that eVoting shall be offered as an alternative voting channel at the Social Election 2023; hence, the law had to be adapted to enable eVoting. For the purposes of the eVoting pilot, §§ 194a - § 194d were added to the Social Code V[8], empowering the Federal Minister of Health to issue an Online Election Decree to enable this pilot. There are two main documents governing the eVoting part of the Social Election:[9]

- The Online Election Decree (in the following "Decree") by the Federal Ministry of Health[10]
- Federal Office for Information Security BSI (2023) Technical Guideline TR-03162[11]

These two documents should be seen as one, because § 194c (1) requires the Federal Minister of Health to reconcile with BSI, while § 194c (2) required the office to produce the Technical Guideline. Right at the beginning of the Decree in § 1, it is made clear that this eVoting election, even though not a political election, serves as a "model project" for further application

[7] Der Bundeswahlbeauftragte für die Sozialversicherungswahlen (2024). *Schlussbericht des Bundeswahlbeauftragten für die Sozialversicherungswahlen zu den Sozialwahlen 2023*. Final Report of the Federal Election Commissioner for the Social Election. Berlin: Bundesministerium für Arbeit und Soziales. Available from: https://www.bmas.de/SharedDocs/Downloads/DE/Meldungen/2024/bundessozialwahl-2023-schlussbericht.pdf?__blob=publicationFile&v=1 [Accessed 20 June 2025]

[8] *Sozialgesetzbuch (SGB) Fünftes Buch (V) - Gesetzliche Krankenversicherung* - (Artikel 1 des Gesetzes v. 20. Dezember 1988, BGBl. I S. 2477) (Social Code V). In German. Available from: https://www.gesetze-im-internet.de/sgb_5/ [Accessed 20 June 2025]

[9] Note that the provisons of the Social Code are relatively abstract, the details are, not unusual in German legislation, regulated by a decree of a Federal Minister.

[10] Federal Ministry of Health (2020). *Verordnung über die technischen und organisatorischen Vorgaben für die Durchführung einer Online-Wahl im Rahmen des Modellprojekts nach § 194a des Fünften Buches Sozialgesetzbuch*. Berlin. In German. Available from: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/GuV/O/Online-Wahl-VO_Bgbl.pdf [Accessed 20 June 2025]

[11] Bundesamt für Sicherheit in der Informationstechnik (2023). *Technische Richtlinie TR-03162, Version 1.3, 3.2.2023*. Bonn. In German. Available from: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03162/TR-03162_node.html#:~:text=Die\%20Technische\%20Richtlinie\%20TR\%20\%2D03162,Briefwahl\%20auch\%20Online\%2DWahlen\%20anzubieten [Accessed 20 June 2025]

– as § 194a already stated before. Hence, there is an increased interest in how this eVoting was implemented; it also implies that Council of Europe Recommendation CM/Rec(2017)5[12], which only applies to political elections, indirectly does apply and should hence be adhered to.

The Decree further stipulates that the participating social insurance institutions commission a service provider to run the online election system. The guidelines to follow are the

- BSI Basic IT Protection standard, "IT-Grundschutz"[13] and
- Technical Guideline TR-03162, which, at the time the Decree was passed, was still in its draft status.

In § 8, the Decree requires an independent security validation by an external expert, however only in view of the Basic IT Protection, not the protection of general voting principles.[14] Therefore, the external expert validation was to check for instance, whether backups were made and general IT security was maintained, but did not cover for instance protection of voting secrecy or any other specifics of eVoting. This is an interesting approach to eVoting security. § 194a (4) of the Social Code V stipulates that the voting principles listed in § 45 (2) of the Social Code IV shall be followed "with a view to the technical features also in the online elections"[15] The principles listed in this paragraph include only three, namely

- Free suffrage
- Secret suffrage
- Accountability in the terminology of the CoE, here in the German terminology (Public) Auditability of the whole election[16]

[12] Council of Europe 2017. *Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting*, Strasbourg. Available from: `https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680726f6f` [Accessed 28 March 2025]

[13] Federal Office for Information Security (2018). *Guide to Basic Protection based on IT-Grundschutz*. Bonn. In German. Available from: `https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/Basic_Security.html?nn=908032` [Accessed 20 June 2025]

[14] Cf. reference in § 8 to § 3 Paragraph 4 Sentence 1. This reference hence only covers the basic protection (IT-Grundschutz in the terminology used in Germany).

[15] Cf. Sozialgesetzbuch (SGB) Fünftes Buch (V) - Gesetzliche Krankenversicherung (Social Code V), *Op. cit.*, § 194a, our translation

[16] This term "Grundsatz der Öffentlichkeit der Wahl" means that the whole election process, except for casting the ballot, occurs in public and is fully auditable. In German practice this also includes each citizen's right to watch the emptying of the ballot boxes and the counting in person.

It has to be added that TR-03162 Section 2.1.1.3 requires a risk analysis for various specific attacks against the voting system, such as "ballot stuffing" or an "Italian attack" (meaning compromising voting secrecy[17]), however, this is not subject to the external security validation according to § 8 of the Decree and nowhere and in no shape or form does TR-03162 refer to CM/Rec(2017)5, which would actually have been a natural reference point for eVoting in a Member State of the Council of Europe. The Recommendation would have also provided an easy-to-use reference point with pre-defined requirements and attack vectors. Such reference would have also been perfectly in line with the "model character" of the project for political elections.

2. THE GENERAL VOTING PROTOCOL

The main eVoting protocol follows an Enveloping approach, with explicit reference to the system used in Estonia as depicted in Figure 1[18].

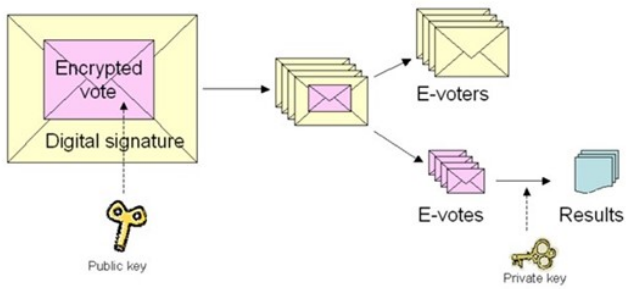


Figure 1: General envelope protocol

Here a brief description and analysis of the "pure" envelope protocol as used in Estonia.

[17] Whereby the literature mainly seems to focus on voter coercion (Italian coercion attack), see for instance Huber, N. et al. (2022). Kryvos: Publicly Tally-Hiding Verifiable E-Voting. In: Yin, H. and Stavrou, A. (eds.) *CCS 2022: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, Los Angeles, 7 Nov. USA: Association for Computing Machinery. Available from: https://doi.org/10.1145/3548606.3560701 [Accessed 20 June 2025], pp. 1443–1457 and Peng, K. and Bao, F. (2009). A Design of Secure Preferential E-Voting. In: Ryan, P.Y.A. and Schoenmakers, B. (eds.) *Vote-ID 2009: International Conference on E-Voting and Identity*, Luxembourg, 7-8 September. Germany: LNCS 5767. Available from: https://link.springer.com/chapter/10.1007/978-3-642-04135-8_9 [Accessed 20 June 2025], pp. 141-156

[18] Estonian National Electoral Committee (2010). *E-Voting System, General Overview*, Tallinn. Available from: https://www.valimised.ee/sites/default/files/uploads/eng/General_Description_E-Voting_2010.pdf [Accessed 20 June 2025], p. 10, Figure 1

The protocol assumes (i) an asymmetric, for instance RSA[19], key pair (external E, domestic D) of which E is delivered to the eVoter by the voting application and (ii) a digital signature available to the voter. The voter fills in the ballot (or casts a blank vote), whereupon it is encrypted with public key E giving E(ballot), the "inner envelope". Private key D is only known to the election committee and may also be distributed among the members of the committee.[20] The voter adds his or her signature to the now encrypted ballot ("outer envelope"). This combined envelope structure is sent to the electronic ballot box. The ballot box thereby contains the information who voted for whom only protected by the encryption of the inner envelope. In the tally, the signatures on the outer envelope are verified and the usual checks performed (eligible voter, only one vote cast, no vote cast by alternative channels, etc.). The outer envelope is then "removed", and the inner envelope forwarded to the election committee, who apply their private key D to open (decrypt) the ballot, which is then counted (cf. Figure 1 for the process).

This protocol at first glance corresponds to the standard postal voting procedure of two envelopes, their separation and the insertion of the inner ballot envelope in the ballot box. It therefore holds an intrinsic appeal to election officials who recognise their postal voting standard procedure. However, Enveloping has some serious and well-documented flaws:

a. The paper analogy does not hold. If a paper ballot envelope is taken out of the outer postal envelope, it is physically not there anymore as the paper envelope exists just once. Mixed with other ballot envelopes, voting secrecy can easily be achieved. In the electronic media, however, this analogy does not hold. The data records of (digital voter signature, E(ballot)) exist, whether in mirrored storage media, backups or illicit copies. Once the election committee private key D is known, it can easily be applied to give D(E(ballot)) = ballot, which in turn enables to reconstruct (digital voter signature, ballot) and hence the mass violation of voter secrecy. In that, Enveloping, as used for Estonian eVoting, violates the following standards of CM/Rec(2017)5:

[19] Rivest, R. L., Shamir, A., and Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM, 21(2)*, Available from: `https://dl.acm.org/doi/pdf/10.1145/359340.359342` [Accessed 20 June 2025], pp. 120-126

[20] Prosser, A. (2004) Implementation of Quorum-Based Decisions in an Election Committee. In: Traunmüller, R. (ed.) *DEXA/EGOV 2004: 15th International Workshop on Database and Expert Systems Applications*, Zaragossa, 30 August – 3 September. Germany: LNCS 3183, pp. 122-127

- E-voting shall be organised in such a way as to ensure that the secrecy of the vote is respected at all stages of the voting procedure. (Standard 19).
- The e-voting process, in particular the counting stage, shall be organised in such a way that it is not possible to reconstruct a link between the unsealed vote and the voter. Votes are, and remain, anonymous (Standard 26).
As seen above, it is possible to construct a link between the unsealed vote and the voter once the electronic ballot box and the private key of the election committee are brought together.
Where applicable, also Standard 25 is violated simply by analogy: *E-voting shall ensure that the secrecy of previous choices recorded and erased by the voter before issuing his or her final vote is respected*.

b. The ballot box data constitutes an inherent risk and hence should be destroyed as soon as possible. This however makes a judicial review of the eVoting virtually impossible as there are no artefacts left. An example may be the Austrian student elections in 2009, where the voting data was deleted prematurely and contrary to the applicable decree, which rendered the judicial review by the Austrian Constitutional Court rather difficult.[21]

c. This property also makes an independent recount virtually impossible (or meaningless). Either the mere ballots are handed over to the recount, which makes the recount completely dependent on the integrity of the election administration it is supposed to check; or ballot box and private key D are handed over giving the election committee at least the technical ability to verify how each voter voted. This, however, violates at least Standard 18: *The system shall provide sound evidence that only eligible voters' votes have been included in the respective final result. The evidence should be verifiable by means that are independent from the e-voting system*. Since there is no independent recount, the independent verification of the result is not possible.

For a detailed discussion of Enveloping in general and its deficiencies we refer to the literature.[22] More details on the process itself were published by

[21] Balthasar, A. and Prosser, A. (2012). E-Voting in der Sonstigen Selbstverwaltung - Anmerkungen zu VfGH vom 30. Juni 2011, B 1149, und vom 13. Dezember 2011, V 85-96. *Journal für Rechtspolitik (JRP)*, 2012(1), pp. 47-86.

[22] Springall, D. et al. (2014). Security Analysis of the Estonian Internet Voting System. In: *CCS'14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communication*

State Electoral Office of Estonia.[23] The system used at the social elections, however, had two substantial deviations from the Estonian algorithmic original discussed in the two following sections.

3. EXTENSION 1: HOMOMORPHIC ENCRYPTION

One may conclude that also TR-03162 does not fully believe that Enveloping is a sufficient safeguard against compromising as it enables ("can be used") a homomorphic encryption of the votes (Section 4.5.2 of Technical Guideline TR-03162). Generally, homomorphic encryption enables mathematical operations on encrypted data without access to the unencrypted data. The result of the operations is encrypted as well. A key field of application is the storage of sensitive (encrypted) data on a cloud server, where the result of a calculation is sent back to the owner of the data, also in encrypted form. The owner then has the private key to de-cypher the result and the cloud provider does neither know the data nor the result.[24] The crypto-systems are asymmetric, ie, public key cryptography.[25]

Let E() be the public ("external") part of an encryption function, D() the private or domestic part. Then, Figure 2 captures the concept of additive homomorphism. Homomorphically adding encrypted x and y (giving E(x) $\oplus$ E(y)) is identical to computing x+y and then encrypting the resulting sum. Operation $\oplus$ is the cryptographic equivalent of an addition.

Security, Scottsdale, Arizona, 3-7 November, USA: Association for Computing Machinery. Available from: http://dx.doi.org/10.1145/2660267.2660315 [Accessed 20 June 2025], pp. 703-715 and Bagnato, D. (2022). Recommendation CM/REC(2017)5 of the Council of Europe and an Analysis of eVoting Protocols. In: Kaiser, T. et al. (eds.) *CEEeGov 2022: Proceedings of the Central and Eastern European eDem and eGov Days*. Budapest, 22-23 September. USA: Association for Computing Machinery. Available from https://doi.org/10.1145/3551504.3551519 [Accessed 20 June 2025], pp. 169-178 and Karhumäki, J. and Meskanen, T. (2008). *Audit Report on Pilot Electronic Voting in Municipal Elections*, University of Turku, Turku

[23] State Electoral Office of Estonia (2016) *General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia*, Tallinn. Available from: https://www.venice.coe.int/files/13EMB/13EMB_Priit_Vinkel.pdf [Accessed 20 June 2025]

[24] Gentry, C. (2010). *Computing Arbitrary Functions of Encrypted Data*. Communications of the ACM, Vol. 53(3). Available from: https://doi.org/10.1145/1666420.1666444 [Accessed 20 June 2025], pp. 97-105 and Gentry, C., Sahai, A. and Waters, B. (2013). Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based. In: Canetti, R. and Garay, J.A. (eds.) CRYPTO 2013: Advances in Cryptology, *33rd Annual Cryptology Conference Proceedings*, Part I, Santa Barbara, 18-22 August. Germany: LNCS 8042. Available from: https://link.springer.com/chapter/10.1007/978-3-642-40041-4_5 [Accessed 20 June 2025], the authors also essentially contributed to the development of homomorphism in general.

[25] Salonaa A. (2013) *Public-Key Cryptography*. 2nd Ed., Berlin: Springer.

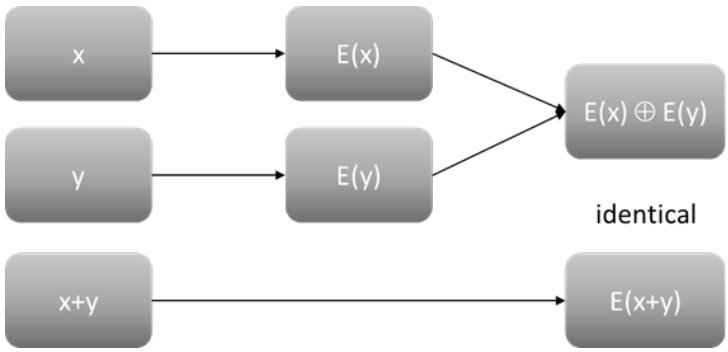


Figure 2: Additive homomorphism explained

Additive homomorphism readily lends itself to a homomorphic computation of an election result. Assume that the ballot consists of a single (yes/no or 1/0 question). Further assume three votes were cast and encrypted with E(), two of them "yes", one "no". Each vote is linked to the voter ID and the voter's digital signature ("outer envelope" in Figure 1). The homomorphic addition would then work as depicted in Figure 3.

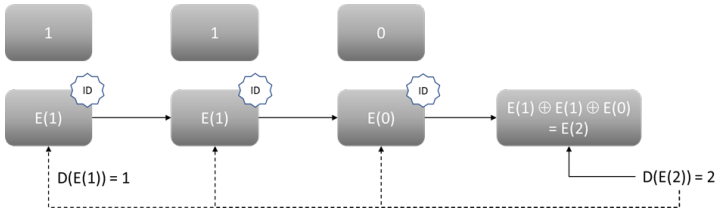


Figure 3: Casting and opening votes with homomorphic encryption

Homomorphic addition would yield E(2). Application of private key function D() yields the number of "yes" votes, i.e. the election result, by computing D(E(2)) = 2 without the necessity to decrypt ("open") the individual votes. But, and this is the main failure of this concept, you still need the private key to decipher the election results (here two "yes" votes). And once you have the domestic key D(), you may also decrypt each individual vote separately and thereby find out who voted for whom because the individual vote is linked to the voter ID. The unsolved problem here – and always when applying the envelope protocol - is that the individual votes which can be assigned to the voter still exist on the server of the election authority.

The addition of homomorphic encryption hence cannot solve the innate issues of envelope protocols. This result generally holds:

- Joint possession of the electronic ballot box and the private key of the election committee enables an attacker to break voting secrecy on a large scale;
- It also hinders to pass the ballot box on to a third party for an independent recount and keeping voter secrecy.

Hence, the violations of CM/Rec(2017)5 Standards 18, 19, 26 and, where applicable, Standard 25 mentioned in Section 2 a.-c. still apply. Therefore, by extension, also § 45 of the Social Code IV is not adhered to, as secrecy of the vote (Standards 19 and 26) and public reproducibility[26] (Standard 18) are not met.

4. EXTENSION 2: DIGITAL SIGNATURE KEY SURROGATE

Technical Guideline TR-03162, however, introduced another deviation from the Estonian system as it did not use digital signatures for the outer envelope. While digital signatures are extremely popular in Estonia, the digital signature is virtually non-existent in Germany and hence cannot be used for these purposes. TR-03162 therefore had to circumvent this issue. A recent press release of the Bundesdruckerei Group (100% state-owned former Federal Printing Office) stated that less than a fourth of the civil servants asked in a poll use digital signatures.[27] D-Trust, owned by Bundesdruckerei Group, recently published that only 16 % of the German companies use digital signatures,[28] hence the usage by private citizens cannot be significantly higher, rather the opposite. Unlike the Estonian ID[29], the German ID does not offer a digital signature, but it is only usable for identification purposes.[30]

[26] Cf. FN 21 concerning "Grundsatz der Öffentlichkeit der Wahl". If the election is not reproducible for an audit committee or court, it cannot possibly be reproducible for the general public.

[27] Cf. Bundesdruckerei GmbH (2023). *Volldigitale Prozesse in Behörden scheitern häufig an händischer Unterschrift*. [press release] 7 November. Available from: `https://www.presseportal.de/pm/14611/5643391` [Accessed 20 June 2025]

[28] Cf. Bundesdruckerei GmbH (2017). *Whitepaper: Durchgängig digital. mit Fernsignatur und elektronischem Siegel*. Available from: `https://www.d-trust.net/files/dokumente/pdf/whitepaper_fernsignatur_elektronisches_siegel.pdf` [Accessed 20 June 2025]

[29] e-Estonia. *E-Identity. ID-card* (n.d.). [online]. Available from: *https://e-estonia.com/solutions/e-identity/id-card/* [Accessed 20 June 2025]

[30] Bundesministerium des Inneren (2025) *Die elektronischen Funktionen des Personalausweises* [online] Available from: `https://www.personalausweisportal.de/Webs/PA/DE/`

It is the essence of the enveloping procedure to cast an authenticating digital signature on the encrypted ballot. In Sections 4.4f and particularly Figure 6, TR-03162 defines a surrogate for the usage of digital signatures.[31] Voters log into the election system using their Social Security Number, the last six digits of the backside of their eHealth Card[32] (both easily known to each medical service institution in Germany) plus the voter identification (Wahlkennzeichen, WKZ), which is an alphanumeric random character string issued for every voter in the roll and sent to voters by postal mail (2.2.1). Voters may also use their eID for login (4.4.2), but have to enter their WKZ anyway. Hence, the voter typically does not register by a strong means of identification (usage of the eID necessarily must be a minority programme), but by a character string sent by post. Hence, it is easy to intercept this letter and cast a vote on behalf of the voter if the above-mentioned six-digit social security number is known; it is also possible to collect WKZ. In our case, the demonstration and screenshots were produced using the data of the spouse of one of the authors – with her consent, but it would also have been technically possible to do that without her cooperation. According to Deutsches Ärzteblatt[33] the voter turnout at the elections was 11.5 million out of 55.3 million. This means that 43.8 million postal ballots were thrown into the wastebins and could have been used for electoral fraud.

A list of all generated WKZ is part of the election server system, however, has to be stored separately from the electronic ballot box (TR-03162, 2.2.2.4). After login, the usual voter checks are performed (eligible, has already cast a vote etc.). The following procedure to cast a vote is then performed (4.5.1 and 4.5.2 with Figures 6 and 7):

- The vote is encrypted with the public key of the election committee and sent to the election server without any authentication information (cf. Figure 4, Point 1).
- Upon receipt at the election server, the encrypted vote is signed by the election server and sent to the electronic ballot box. This is a

buergerinnen-und-buerger/der-personalausweis/funktionen/funktionen-node.html [Accessed 20 June 2025]

31 In the following, all section and figure references from TR-03162.

32 Note that the German Social Security Card is a chipcard, cf. Bundesministerium für Gesundheit (2024). *Elektronische Gesundheitskarte*. [press release] 5 December. Berlin. Available from: https://www.bundesgesundheitsministerium.de/themen/digitalisierung/elektronische-gesundheitskarte [Accessed 20 June 2025]. So a stronger identification could have been easily introduced.

33 Deutsches Ärzteblatt (2023). *Sozialwahl: Wahlbeteiligung trotz großer Kampagnen gesunken*. [online] Available from: https://www.aerzteblatt.de/news/sozialwahl-wahlbeteiligung-trotz-grosser-kampagnen-gesunken-07d62b7a-e6c0-401e-b4c8-107ed5835a90 [Accessed 20 June 2025]

clear surrogate to the vote-based signature in the "classical" Enveloping (Point 2). An advanced digital signature is permissible, a fully qualified digital signature is not required. An advanced signature does not require a qualified digital certificate nor a secure signature device.[34]

- This signed vote is then inserted in the electronic ballot box (Point 3).
- The WKZ is sent separately to another server to mark the WKZ as used; this entry must be stored without time stamp to avoid assignment to a vote according to the time the vote was signed and entered the ballot box. Interestingly, the voter login is not among the events to be protocolled either (2.4). Rather, TR-03162 explicitly rules out that insertion of a vote or insertion of a WKZ is logged (cf. Footnotes 9 and 10). It therefore must be noted that the election system cannot verify, when a voter (WKZ) voted.

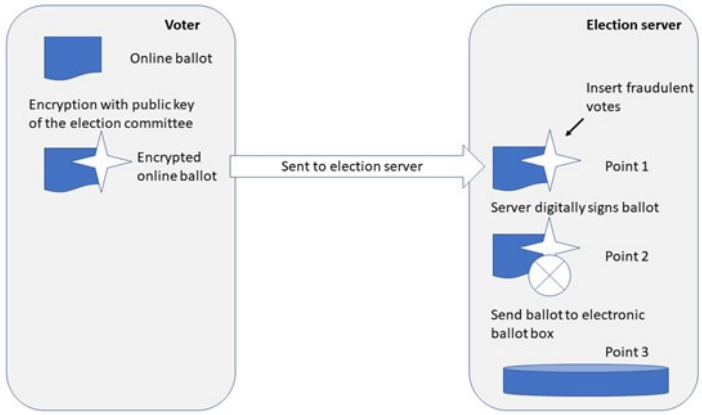


Figure 4: Voting procedure (derived from TR-03162, Figure 6, our translation and insertions)

Summarizing, the system design enables large-scale administrator fraud. The votes as received from the voters are encrypted with the public key of the election committee. The public key is, of course, known and a fraudulent election administration can insert votes and sign them.

[34] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. *Official Journal of the European Union* (L 257) 28 August. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0910` [Accessed 20 June 2025]

Submission of the WKZ and the vote are handled via two different "channels", ie, presumably two Web service addresses. There is no discernible mechanism to ensure that these two submissions are combined in a transaction (cf. ACID properties[35]). TR-03162 only states that if one fails, the event must be logged (4.5.2). What follows from that logging, is not specified.

In the counting stage, the signatures of the votes (by the election server) in the ballot box are verified and then either decrypted with the private key of the election committee or the result is homomorphically computed and the result is decrypted with that key. The ballots are then counted and the result established. In addition, the list of WKZ is checked and the sum of the WKZ and the sum of the votes are compared. TR-03162 also stipulates that the ballot box can be published. However, what would such a publication prove? It would merely show a list of ballots without any background information and the only validation would be the signature of the election server that could technically be faked by the server administration.

Let us now summarize the Sozialwahl eVoting in the light of Council of Europe Recommendation CM/Rec(2017)5 and mirror the technical properties of TR-03162 against selected standards in CM/Rec(2017)5. Standards quoted from the recommendation are depicted in italics.

5. SOZIALWAHL AND CM/REC(2017)5

The Social Election 2023 was in a Member State of the Council of Europe; hence the relevant recommendation of the Council of Ministers is fully applicable, despite its legally non-binding character, particularly in view of the stated "model character" of the eVoting.

The recommendation contains provisions for voting principles, any eVoting system used for political elections in a Member State must meet. The following chapter discusses, whether the system used in the German Social Election met these requirements, which were also required by the respective German law, § 45 (2) Social Code IV, or whether it violated them.

[35] As far as can be ascertained, the term goes back to: Haerder, T. and Reuter, A. (1983) Principles of transaction-oriented database recovery. *ACM Computing Surveys*, Vol. 15(4). Available from: `https://dl.acm.org/doi/10.1145/289.291` [Accessed 20 June 2025], pp. 287–317

5.1.SECRET SUFFRAGE

19. E-voting shall be organised in such a way as to ensure that the secrecy of the vote is respected at all stages of the voting procedure.

26. The e-voting process, in particular the counting stage, shall be organised in such a way that it is not possible to reconstruct a link between the unsealed vote and the voter. Votes are, and remain, anonymous.

As detailed in Section 2, the envelope procedure cannot fulfill these requirements[36].[37] Usage of a homomorphic encryption does not change this shortcoming as seen in Section 3. However, TR-03162 does not implement a classic envelope protocol. The vote is not signed by the voter, instead the WKZ is sent and stored separately from the vote (2.2.2.2); neither submission of the WKZ nor submission of the vote cast are logged. At first glance, voter secrecy appears to be ensured.

However, this is a web application, which must maintain its sessions, typically via cookies and the web application session referenced therein. Also, the vote must be included in a database representing the electronic ballot box. What does the ballot box table in that database look like? Does it have a primary key? If so, how is this key assigned? Typically, one would choose a random number or hexadecimal code and store the vote under that key. If that variant is chosen, there is a link Session – WKZ – ballot with assigned random key for database table TR-03162 appears to be aware of this issue, as it stipulates (our translation from the German original, Section 4.5.1):

"If the election platform maintains data during a processing, which enable a link between electronic vote, WKZ or identity of the voter, the election platform MUST

- Securely delete this data at the earliest possible stage, the latest however after conclusion of the transmission of the vote into the ballot box and
- Secure via technical/organisational measures that access to this data is only available via the election platform."

Therefore, the fundamental issues with envelope procedures may appear again in this scaled-down version of the protocol. Again, homomorphic encryption does not solve the issue. Note that the deletion of the data may fulfil the requirement for secret suffrage, but violates the auditability, both listed in § 45 (2) Social Code IV. Such a violation cannot be accepted "with a view to the technical features also at the online elections", as § 194a (4)

[36] Bagnato, D. (2022) Recommendation CM/REC(2017)5 of the Council of Europe and an Analysis of eVoting Protocols. *op. cit.*

[37] Prosser, A. (2014) Transparency in eVoting - Lessons learnt. *Transforming Government: People, Process and Policy*, 8(2), pp. 171-184

would suggest, at least not within the standards established by the Council of Europe[38].

5.2.FREE SUFFRAGE

15. The voter shall be able to verify that his or her intention is accurately represented in the vote and that the sealed vote has entered the electronic ballot box without being altered. Any undue influence that has modified the vote shall be detectable.

16. The voter shall receive confirmation by the system that the vote has been cast successfully and that the whole voting procedure has been completed.

17. The e-voting system shall provide sound evidence that each authentic vote is accurately included in the respective election results. The evidence should be verifiable by means that are independent from the e-voting system.

18. The system shall provide sound evidence that only eligible voters' votes have been included in the respective final result. The evidence should be verifiable by means that are independent from the e-voting system.

Apart from Standard 16, the system specified in TR-03162 does not fulfill any of these properties. The vote bears no authentication beyond the digital signature of the election server. Unlike in the Estonian system one cannot establish that the vote was cast by an eligible voter (the digital signature of the voter in the outer envelope). All this system can establish is the evidence that the vote was signed by the election system itself. There is no link to a WKZ or any other authentication information beyond that. Hence, the voter cannot verify that her vote was stored and counted as cast. Ex post publication of the ballots does not change this. All the system described in TR-03162 can verify is:

- There are as many WKZ as there are votes;
- All votes in the ballot box have been correctly signed by the election server;
- All votes have been cast in the election period.

[38] see Standard 39 below

5.3.ACCOUNTABILITY

39. The e-voting system shall be auditable. The audit system shall be open and comprehensive, and actively report on potential issues and threats.

The system described in TR-03162 can detect illicit access to election master data, such as the voter roll or the WKZ. However, there is no audit chain possible that establishes that:

- The vote was cast by an eligible voter;[39]
- The vote was inserted in the ballot box as cast by the eligible voter.[40]

The system described in TR-03162 is therefore not auditable. This view is also shared by the official audit report[41], which was published in late 2024, after the submission of this paper to MUJLT (p.42, our translation from German):

[The independent expert verifying the result] arrived at the conclusion that the auditability of the election technology employed for the Sozialwahl could not be ascertained, as the definition of the cryptographic protocol and the source code showed issues that prevented the auditability of the election result.

The "issues" leading to this assessment are not technically detailed in the audit report but will most likely be the ones listed above.

6. CONCLUSION

This paper analysed an eVoting system used for the German Social Elections in 2023, particularly the underlying Technical Guideline TR-03162. The system implements a classical envelope procedure with two major deviations: usage of homomorphic encryption and non-usage of digital signatures by the voter on the outer envelope of the vote with the WKZ mechanism as a substitute.

The paper established the following results in view of CM/REC(2017)5:

1. Use of homomorphic encryption does not solve the fundamental issues of Enveloping as the fact remains that voter identification data and (encrypted) vote are stored in the ballot box. Once the private key of the election committee has been provided, it can be used to decipher the connection voter – vote. This violated Standards 19 and 26.

[39] See argument in 5.2

[40] See argument in 5.2

[41] KPMG (2024) *Evaluierung des Modellprojekts zur Durchführung von Online-Wahlen bei den Krankenkassen nach § 194d SGB V*. Report from 30 October. Available from: `https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/5_Publikationen/Ministerium/Berichte/Abschlussbericht_Evaluation_Modellprojekt_Online-Wahlen.pdf` [Accessed 20 June 2025]

2. Addition of an artificial voter identifier (WKZ) instead of a digital signature of the voter (as in the Estonian "original" of the protocol) creates a whole host of auditability and verification issues. It enables large-scale administrator fraud. The protocol variant chosen for the Sozialwahl hence neither enables individual auditability by the voter nor general auditability in an independent recount. Also in this regard, the protocol addition does not solve the inherent auditability issue of the Envelope protocol violating Standards 15, 17, 18 and 39.
3. An artificial identifier like WKZ does not guarantee voter secrecy either, as the link voter – vote may be reconstructed by session data maintained by the servers involved violating Standards 19 and 26.
4. It was shown that the protocol chosen violated a number of major standards of Recommendation CM/REC(2017)5. Given that this eVoting was described as a "model project" in the relevant Decree, one can only strongly recommend that this system is never rolled out for real political elections.

The voter turnout showed that the eVoting pilot was no game changer: According to the Federal Election Commissioner for the Social Election 334,166 voters choose online voting, the portion of the total votes cast being between 2.42 % (DAK-Gesundheit) and 9.96 % (Techniker Krankenkasse). Techniker Krankenkasse, the one with the highest eVoting turnout, lost 380,590 voters in total despite 200,080 eVoters. eVoters totalled for 334,166 votes while the loss in total votes cast was 3,836,580.[42]

LIST OF REFERENCES

[1] Bagnato, D. (2022). Recommendation CM/REC(2017)5 of the Council of Europe and an Analysis of eVoting Protocols. In: Kaiser, T. et al. (eds.) *CEEeGov 2022: Proceedings of the Central and Eastern European eDem and eGov Days*. Budapest, 22-23 September. USA: Association for Computing Machinery. Available from `https://doi.org/10.1145/3551504.3551519` [Accessed 20 June 2025], pp. 169-178.

[2] Balthasar, A. and Prosser, A. (2012). E-Voting in der Sonstigen Selbstverwaltung - Anmerkungen zu VfGH vom 30. Juni 2011, B 1149, und vom 13. Dezember 2011, V 85-96. *Journal für Rechtspolitik (JRP)*, 2012(1), pp. 47-86.

[42] KPMG (2024) Evaluierung des Modellprojekts zur Durchführung von Online-Wahlen bei den Krankenkassen nach § 194d SGB V. *Op. cit.*

[3] Bundesamt für Sicherheit in der Informationstechnik (2023). *Technische Richtlinie TR-03162, Version 1.3, 3.2.2023.* Bonn. In German. Available from: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03162/TR-03162_node.html#:~:text=Die\%20Technische\%20Richtlinie\%20TR\%20\%2D03162,Briefwahl\%20auch\%20Online\%2DWahlen\%20anzubieten [Accessed 20 June 2025].

[4] Bundesdruckerei GmbH (2017). *Whitepaper: Durchgängig digital. mit Fernsignatur und elektronischem Siegel*. Available from: https://www.d-trust.net/files/dokumente/pdf/whitepaper_fernsignatur_elektronisches_siegel.pdf [Accessed 20 June 2025].

[5] Bundesdruckerei GmbH (2023). *Volldigitale Prozesse in Behörden scheitern häufig an händischer Unterschrift*. [press release] 7 November. Available from: https://www.presseportal.de/pm/14611/5643391 [Accessed 20 June 2025].

[6] Bundesministerium des Inneren (2025) *Die elektronischen Funktionen des Personalausweises* [online] Available from: https://www.personalausweisportal.de/Webs/PA/DE/buergerinnen-und-buerger/der-personalausweis/funktionen/funktionen-node.html [Accessed 20 June 2025].

[7] Bundesministerium für Arbeit und Sozialordnung (1997). *Wahlordnung für die Sozialversicherung* (Election Decree for the Social Elections). In German. Available from: https://www.gesetze-im-internet.de/svwo_1997/ [Accessed 20 June 2025].

[8] Bundesregierung (2023) *Wissenswertes zur Sozialwahl 2023*. [online] Berlin. Available: https://www.bundesregierung.de/breg-de/aktuelles/sozialwahl-2023-2188062 [Accessed 20 July 2025].

[9] Council of Europe (2017). *Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting*, Strasbourg. Available from: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680726f6f [Accessed 28 March 2025].

[10] Der Bundeswahlbeauftragte für die Sozialversicherungswahlen (2024). *Schlussbericht des Bundeswahlbeauftragten für die Sozialversicherungswahlen zu den Sozialwahlen 2023*. Final Report of the Federal Election Commissioner for the Social Election. Berlin: Bundesministerium für Arbeit und Soziales. Available from: https://www.bmas.de/SharedDocs/Downloads/DE/Meldungen/2024/bundessozialwahl-2023-schlussbericht.pdf?__blob=publicationFile&v=1 [Accessed 20 June 2025].

[11] Deutsches Ärzteblatt (2023). *Sozialwahl: Wahlbeteiligung trotz großer Kampagnen gesunken*. [online] Available from: https://www.aerzteblatt.de/news/sozialwahl-wahlbeteiligung-trotz-grosser-kampagnen-gesunken-07d62b7a-e6c0-401e-b4c8-107ed5835a90 [Accessed 20 June 2025].

[12] e-Estonia. *E-Identity. ID-card* (n.d.). [online]. Available from: *https://e-estonia.com/solutions/e-identity/id-card/* [Accessed 20 June 2025].

[13] Estonian National Electoral Committee (2010). *E-Voting System, General Overview*, Tallinn. Available from: https://www.valimised.ee/sites/default/files/uploads/eng/General_Description_E-Voting_2010.pdf [Accessed 20 June 2025].

[14] Federal Ministry of Health (2020). *Verordnung über die technischen und organisatorischen Vorgaben für die Durchführung einer Online-Wahl im Rahmen des Modellprojekts nach § 194a des Fünften Buches Sozialgesetzbuch*. Berlin. In German. Available from: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/GuV/O/Online-Wahl-VO_Bgbl.pdf [Accessed 20 June 2025].

[15] Federal Office for Information Security (2018). *Guide to Basic Protection based on IT-Grundschutz*. Bonn. In German. Available from: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/Basic_Security.html?nn=908032 [Accessed 20 June 2025].

[16] Gentry, C. (2010). *Computing Arbitrary Functions of Encrypted Data*. Communications of the ACM, Vol. 53(3). Available from: https://doi.org/10.1145/1666420.1666444 [Accessed 20 June 2025], pp. 97-105.

[17] Gentry, C., Sahai, A. and Waters, B. (2013). Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based. In: Canetti, R. and Garay, J.A. (eds.) CRYPTO 2013: Advances in Cryptology, *33rd Annual Cryptology Conference Proceedings*, Part I, Santa Barbara, 18-22 August. Germany: LNCS 8042. Available from: https://link.springer.com/chapter/10.1007/978-3-642-40041-4_5 [Accessed 20 June 2025].

[18] GKV Spitzenverband. *Die gesetzlichen Krankenkassen*. [online] Bonn. Available from: https://www.gkv-spitzenverband.de/krankenversicherung/kv_grundprinzipien/alle_gesetzlichen_krankenkassen/alle_gesetzlichen_krankenkassen.jsp [Accessed 19 June 2025].

[19] Haerder, T. and Reuter, A. (1983) Principles of transaction-oriented database recovery. *ACM Computing Surveys*, Vol. 15(4). Available from: https://dl.acm.org/doi/10.1145/289.291 [Accessed 20 June 2025], pp. 287–317.

[20] Huber, N. et al. (2022). Kryvos: Publicly Tally-Hiding Verifiable E-Voting. In: Yin, H. and Stavrou, A. (eds.) *CCS 2022: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, Los Angeles, 7 Nov. USA: Association for Computing Machinery. Available from: https://doi.org/10.1145/3548606.3560701 [Accessed 20 June 2025], pp. 1443–1457.

[21] Karhumäki, J. and Meskanen, T. (2008). *Audit Report on Pilot Electronic Voting in Municipal Elections*, University of Turku, Turku.

[22] KPMG (2024) *Evaluierung des Modellprojekts zur Durchführung von Online-Wahlen bei den Krankenkassen nach § 194d SGB V*. Report from 30 October. Available from: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/5_Publikationen/Ministerium/Berichte/Abschlussbericht_Evaluation_Modellprojekt_Online-Wahlen.pdf [Accessed 20 June 2025].

[23] Nakielski, H. (2022). *Gerichte und Richter:innen der Sozialgerichtsbarkeit*. [online]. Available from: https://netzwerk-sozialrecht.net/gerichte-und-richterinnen-der-sozialgerichtsbarkeit/ [Accessed 20 June 2025].

[24] Bundesministerium für Gesundheit (2024). *Elektronische Gesundheitskarte*. [press release] 5 December. Berlin. Available from: https://www.bundesgesundheitsministerium.de/themen/digitalisierung/elektronische-gesundheitskarte [Accessed 20 June 2025].

[25] Peng, K. and Bao, F. (2009). A Design of Secure Preferential E-Voting. In: Ryan, P.Y.A. and Schoenmakers, B. (eds.) *Vote-ID 2009: International Conference on E-Voting and Identity*, Luxembourg, 7-8 September. Germany: LNCS 5767. Available from: https://link.springer.com/chapter/10.1007/978-3-642-04135-8_9 [Accessed 20 June 2025], pp. 141-156.

[26] Prosser, A. (2004) Implementation of Quorum-Based Decisions in an Election Committee. In: Traunmüller, R. (ed.) *DEXA/EGOV 2004: 15th International Workshop on Database and Expert Systems Applications*, Zaragossa, 30 August – 3 September. Germany: LNCS 3183, pp. 122-127.

[27] Prosser, A. (2014) Transparency in eVoting - Lessons learnt. *Transforming Government: People, Process and Policy*, 8(2), pp. 171-184.

[28] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. *Official Journal of the European Union* (L 257) 28 August. Available from: https://eur-

lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0910 [Accessed 20 June 2025].

[29] Rivest, R. L., Shamir, A., and Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM, 21(2)*, Available from: https://dl.acm.org/doi/pdf/10.1145/359340.359342 [Accessed 20 June 2025], pp. 120-126.

[30] Salonaa A. (2013) *Public-Key Cryptography*. 2nd Ed., Berlin: Springer.

[31] *Sozialgesetzbuch (SGB) Fünftes Buch (V) - Gesetzliche Krankenversicherung* - (Artikel 1 des Gesetzes v. 20. Dezember 1988, BGBl. I S. 2477) (Social Code V). In German. Available from: https://www.gesetze-im-internet.de/sgb_5/ [Accessed 20 June 2025].

[32] *Sozialgesetzbuch (SGB) Viertes Buch (IV) - Gemeinsame Vorschriften für die Sozialversicherung* - (Artikel I des Gesetzes vom 23. Dezember 1976, BGBl. I S. 3845) (Social Code IV). In German. Available from: https://www.gesetze-im-internet.de/sgb_4/ [Accessed 20 June 2025].

[33] Springall, D. et al. (2014). Security Analysis of the Estonian Internet Voting System. In: *CCS'14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communication Security*, Scottsdale, Arizona, 3-7 November, USA: Association for Computing Machinery. Available from: http://dx.doi.org/10.1145/2660267.2660315 [Accessed 20 June 2025], pp. 703-715.

[34] State Electoral Office of Estonia (2016) *General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia*, Tallinn. Available from: https://www.venice.coe.int/files/13EMB/13EMB_Priit_Vinkel.pdf [Accessed 20 June 2025].

MUJLT Official Partner (Czech Republic)

ROWAN®
LEGAL

ROWAN LEGAL, advokátní kancelář s.r.o
https://rowan.legal

Cyberspace 2024 Partners

ROWAN®
LEGAL

Zákony pro lidi.cz

§ CODEXIS®

Wolters Kluwer

CATERING
FOR YOU

Notes for Contributors

Focus and Scope

Masaryk University Journal of Law and Technology (ISSN on-line 1802-5951, ISSN printed 1802-5943) is a peer-reviewed academic journal which publishes original articles in the field of information and communication technology law. All submissions should deal with phenomena related to law in modern technologies (e.g. privacy and data protection, intellectual property, biotechnologies, cyber security and cyber warfare, energy law). We prefer submissions dealing with contemporary issues.

Structure of research articles

Each research article should contain a title, a name of the author, an e-mail, keywords, an abstract (max. 1 500 characters including spaces), a text (max. 45 000 characters including spaces and footnotes) and list of references.

Structure of comments

All comments should contain a title, a name of the author, an e-mail, keywords, a text (max. 18 000 characters) and a list of references.

Structure of book reviews

Each book review should contain a title of the book, a name of the author, an e-mail, a full citation, a text (max. 18 000 characters) and a list of references.

Structure of citations

Citations in accordance with AGPS Style Guide 5th ed. (Harvard standard), examples:

Book, one author: Dahl, R. (2004) *Charlie and the Chocolate Factory*. 6th ed. New York: Knopf.
Book, multiple authors: Daniels, K., Patterson, G. and Dunston, Y. (2014) *The Ultimate Student Teaching Guide.* 2nd ed. Los Angeles: SAGE Publications, pp.145-151.
Article: Battilana, J. and Casciaro, T. (2013) The Network Secrets of Great Change Agents. *Harvard Business Review*, 91(7) pp. 62-68.
Case: *Evans v. Governor of H. M. Prison Brockhill* (1985) [unreported] Court of Appeal (Civil Division), 19 June.
Citation Guide is available from: https://journals.muni.cz/public/journals/36/download/Citationguide.pdf

Formatting recommendations

Use of automatic styles, automatic text and bold characters should be omitted.
Use of any special forms of formatting, pictures, graphs, etc. should be consulted.
Only automatic footnotes should be used for notes, citations, etc.
Blank lines should be used only to divide chapters (not paragraphs).
First words of paragraphs should not be indented.
Chapters should be numbered in ordinary way – example: "5.2 Partial Conclusions".

Submissions

Further information available at
https://journals.muni.cz/mujlt/about

© Masarykova univerzita, 2007 – 2025

LIST OF ARTICLES

Fatma Ceren Morbel: Network Effects and the Dynamics of Digital Markets in the Data Economy……..**3**

Mireille Martine Caruana, Roxanne Meilak Borg: Assessing Pandemic Measures: The Impact of Digital Technologies on Fundamental Rights…..……**27**

Joanna Wiszniewska: Influencer Marketing – Do We Need a New Law or a New Approach? Few Remarks From the European and Polish Perspective…..**57**

Domenica Bagnato, Robert Müller-Török, Alexander Prosser, Robert Stein: Evoting at the German Social Elections – Lessons Learnt……..**75**