PRO PUBLICO BONO – Public Administration, 2024/1, 237–261. • DOI: 10.32575/ppb.2024.1.11

Imre Borisz Páll

FROM VISION TO PRACTICE – OBSERVATIONS ON BUTTARELLI'S PRIVACY 2030 IN THE CONTEXT OF DATA PROTECTION IN HUNGARY[1]

Imre Borisz Páll, LL. M. PhD student, Ludovika University of Public Service, Faculty of Public Governance and International Studies, Doctoral School of Public Administration Sciences; Head of Department, National Authority for Data Protection and Freedom of Information, pall.imre@naih.hu

European Data Protection Supervisor (EDPS) Giovanni Buttarelli's posthumous manifesto, Privacy 2030: A New Vision for Europe, places data protection in a global context. Competition and data protection authorities within the EU cooperate and share information about their official inquiries. If properly enforced, the GDPR may be an effective tool of transparent data processing in the EU, and can serve as a model for the rest of the world. Enforcement is the duty of Member States' DPAs, therefore, it may be worth analysing Buttarelli's views in relation to the issues currently facing Hungarian data protection regulation. The paper critically presents Buttarelli's main views, while discussing them in relation to Hungarian public administration through a specific legal case. As a result of the comparative analysis, it can be concluded that by enhancing the data protection culture and its administrative enforcement, our personal data can be better protected.

Keywords:
data protection, democracy, European Union, GDPR, new technologies, public administration

[1] The manuscript was closed on the 14th of February, 2023.

INTRODUCTION

In this article, I examine which findings of Giovanni Buttarelli's posthumous manifesto, *Privacy 2030: A New Vision for Europe*[2] are relevant to the data protection provided by the Hungarian public administration, and to what extent.

On the one hand, this analysis can be justified by the fact that Hungary is also affected by the global megatrends discussed by the late EDPS's paper, or at least their consequences, so not even this country's public administration can avoid being part of the global discourses on issues related to digitisation, global climate change, or mass migration. On the other hand, no analysis of the ideas presented by *Privacy 2030* has been written in the context of Member States' data protection authorities, including the Hungarian DPA, therefore raising the topic can be considered timely even in 2023, when GDPR has already been applied for five years.

It should be emphasised that this study does not summarise Buttarelli's oeuvre, and is not specifically concerned with privacy protection as such, but instead with various aspects of data protection related to it. Specifically, this analysis focuses on certain currently topical questions closely related to the data protection provided by the public administration.

THE GLOBAL CONTEXT OF THE ISSUES RAISED BY PRIVACY 2030

While reading *Privacy 2030,* it seemed to me as if Buttarelli was attempting to answer the question articulated by Giovanni Sartori long before: "In particular, is democracy an adequate instrument in view of the ambitions of a technological age, an age that ultimately looks forward to the 'planning of history'?"[3]

Marc Rotenberg, in the afterword to *Privacy 2030,* emphasises that the paper reaches beyond the domain of data protection, while focusing on broader questions related to climate change and sustainability, or ethics and human rights.[4] He argues that Buttarelli envisaged two contrasting visions of the futures shaped by new technologies and AI, one that serves to preserve democratic institutions, the rule of law and safeguards for the individuals, and another that would "combine the power of automation and logic of efficiency with a growing scarcity of resources", leaving humans "as little more than data points, subject to systems we do not understand and cannot control".[5]

Malavika Jayaram identifies the key words of the manifesto as: power, inequality, digital underclass, algorithmic bias and colonisation.[6] The uneven allocation of the digital dividend and the disproportionate impact of privacy harms on the poor and marginalised,

[2] Buttarelli 2019.
[3] Sartori 1987: 429.
[4] Rotenberg 2019: 29.
[5] Rotenberg 2019: 30.
[6] Jayaram 2019: 31.

in combination with the results of the climate crisis leads to a scenario where "those who contributed the least to environmental damage" and "those who didn't design technologies that are ubiquitous and insatiable" will suffer the most.[7]

In Jules Polonetsky's evaluation, the main issues addressed in *Privacy 2030* are the excesses of surveillance, the power of tech platforms, the impact of automation and the exacerbation of inequality in the data-driven economy.[8] Polonetsky disagrees with Buttarelli's EU-centric view on the basis that the internet allows the evasion of the application of GDPR, therefore he suggests instead "a global alliance of free societies who can work in international coalitions to counter these threats" with "a vision of global leadership and cooperation".[9] In Polonetsky's opinion, Buttarelli's greatest contribution in the paper and as EDPS, "*is his insistence that we see the impact of data on social welfare*" in the interest of being able "*to ensure technology and data are forces for good in society*".[10]

Maria Farrell agrees that *Privacy 2030* goes far beyond data protection. The radical concentration of power "is not a technocratic concern for specialists but an existential issue for our species", because "data maximisation exploits power asymmetries to drive global inequality".[11] Farrell emphasises that the manifesto presents an EU-version of the internet "that starts with the society we as citizens want to live in", instead of "the oppressive brittleness of China's state sovereignty model" or "the colonialist extraction of Silicon Valley".[12] She points out that *Privacy 2030* is optimistic about the future of technology, because modern technology, when not at the service of a harmful business model, can "banish inequality, repair our environment and support us all in living our best lives".[13]

Rocco Panetta agrees that "[T]his is a European story spreading all around the world."[14] Agreeing with his view on the merits of *Privacy 2030,*[15] he also highlights the importance of the paper's main observations in the context of the upcoming ePrivacy Regulation that is complementary to GDPR.[16] He argues that in Buttarelli's vision "all

7 Jayaram 2019: 31.
8 Polonetsky 2019: 33.
9 Polonetsky 2019: 34.
10 Polonetsky 2019.
11 Farrell 2019: 35.
12 Farrell 2019: 36.
13 Farrell 2019.
14 Panetta 2019: 38.
15 Panetta 2019: 38: "The strength of this posthumous work lies in its slipping in the wounds that most threaten contemporary society: digital inequality and discrimination capable of exponentially increasing the information asymmetry between rich and poor, increasingly marked disparities between the north and south of the world, dramatic environmental crisis, also caused by an uncontrolled production of high-tech devices and an unprecedented energy consumption that these devices require, the will to shape the young and the very young, to the point of affecting the cognitive and relational processes to which the XXI century had accustomed us to it. The accent is further placed on the effects that uncontrolled profiling through algorithms generates money produce on reality as a consequence of a sort of digital colonization."
16 Panetta 2019.

contemporary problems are linked together and led to the threatening of freedom and democracy", in particular "environmental issues, climate change, migration flows, poverty and inequality, sovereignism and white supremacism" that are exacerbated by "a technological fever and data processing bulimia".[17] Therefore, *Privacy 2030* urges that algorithms and AI, whether they are used in the private or the public sector, should undergo an "ethical due process".[18]

As Shoshana Zuboff articulates in her afterword: "Lawmakers have been silent for too long or they have allowed the details of rule making to obscure the emergency that cries out for democratic control over surveillance capitalism."[19]

Regardless of how the various editors interpret Buttarelli's vision, the issues discussed in his posthumous paper seem to have already attracted the attention of other authors. In this sense of the word, the manifesto cannot be considered original, but rather a call for attention to already known global problems, which shares the optimistic view that mankind and its living environment still can have a future as long as certain crucial decisions are made. This view seems to be close to the opinion that "we are deciding, […] which evolutionary pathways will remain open and which will forever be closed".[20]

On the other hand, there are those who argue that: "It is doubtful whether Homo sapiens will still be around a thousand years from now […]."[21] But then again, optimists declare that: "Thanks to its capacity for reinvention, capitalism has overcome its periodic crises and outlived its critics, from Karl Marx on."[22]

THE MAIN ISSUES DISCUSSED IN PRIVACY 2030

The paper argues that data is power (see Figure 1), but relatively few wield this power.[23] Instead of digitisation empowering people, in practice it erodes their freedom. Starting with a discussion of the phenomenon of data maximisation and the uneven distribution of power, the first chapter presents the consequences of these developments. Among other challenges, Balkin highlights the existing issue of "asymmetries of knowledge, power, and control".[24]

17 Panetta 2019: 38.
18 Panetta 2019: 40.
19 Zuboff 2019: 42.
20 Kolbert 2015: 268.
21 Harari 2014: 7.
22 Rodrik 2012: 233.
23 Buttarelli 2019: 6.
24 Balkin 2020: 12.

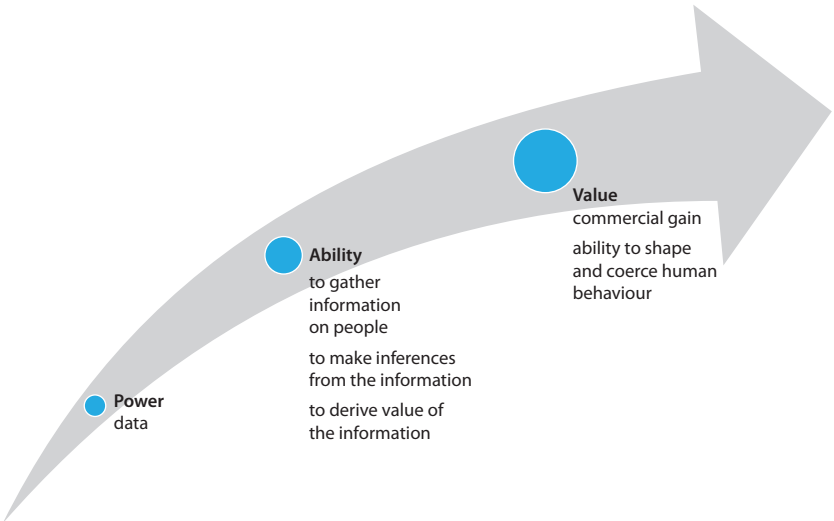


Figure 1: "Data is power"
Source: compiled by the author.

Privacy 2030's key argument contends that the 20th century direction of technological development had changed by the 21st century. While in the 20th century technological innovations were primarily developed for military purposes and became available to civilians later on, in the 21st century, state actors tend to purchase new technologies from the private sector.[25]

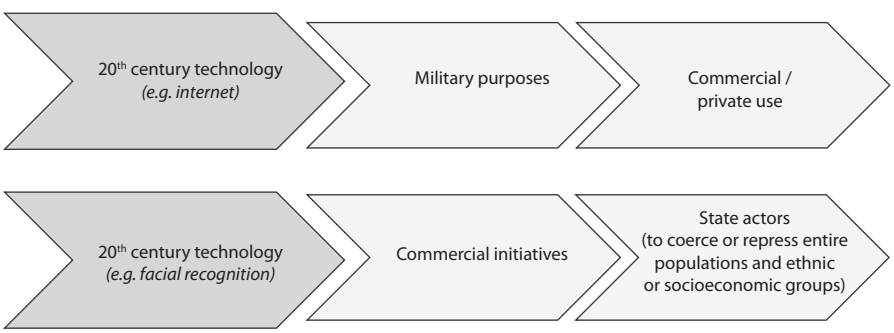


Figure 2: Development of the direction of 20th and 21st century technology
Source: compiled by the author.

[25] Buttarelli 2019: 7.

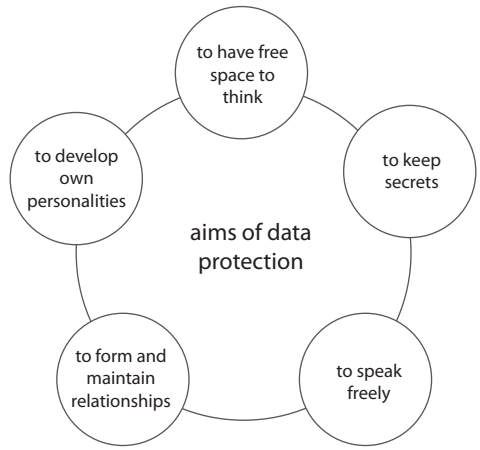


Figure 3: The aims of data protection
Source: compiled by the author.

Meanwhile, the essential principle of data protection (see Figure 3), in the context of privacy conflicts involving the abuse of modern technologies, is that personal data should serve the personal purposes of individuals. However, today "relationships are mediated by revenue-maximising algorithms and providers are not accountable for the risks inherent in their services".[26]

While the consequences might appear to be data protection related issues only, the problems which emerge affect the present and future destiny of our social organisations as a whole.[27] Sartori's attitude appears to be in line with the above, though it is seemingly far more pessimistic: "Technology truly is our deus ex machina; it is the god that keeps us alive, and yet it enslaves us to its machina. For in the end, the deus is no other than ourselves; it is we who have to pay for the miracles we receive."[28]

The first chapter of *Privacy 2030* warns that the lack of data sharing – since data is power – linked to the lack of accountability "has contributed to polarisation and the weakening of the social fabric".[29]

However, the manifesto points out that the "EU's core values are solidarity, democracy and freedom" and the conception of EU data protection "has always been the promotion of responsible technological development for the common good".[30]

[26] Buttarelli 2019.
[27] Rodotá 2004.
[28] Sartori 1987: 432.
[29] Buttarelli 2019: 7.
[30] Buttarelli 2019.

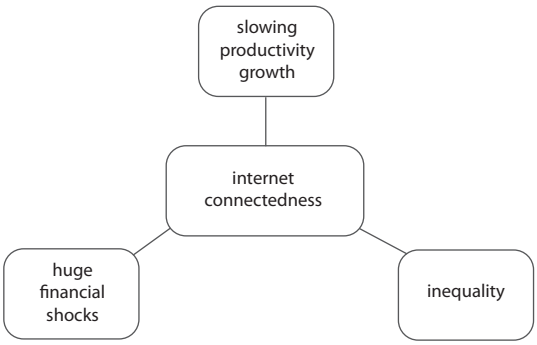


Figure 4: Consequences of internet connectedness
Source: compiled by the author.

The second chapter of *Privacy 2030* argues for a fairer redistribution of digital goods. This part of the manifesto contends that, while the key global controllers of personal data are China and the US, internet connectedness has not resulted in a more proportionate distribution of goods, but instead inequality, declining productivity growth, and a large financial shock (see Figure 4).[31]

Buttarelli believes that this also stems from the ownership structure of the digital markets and AI industry, which is illustrated below (see Figure 5).

The chapter identifies a gap between the power elite and the rest of society, which has led to the creation of a "*digital underclass*", which is not in a position to exercise its fundamental rights (see Figure 6).[32]

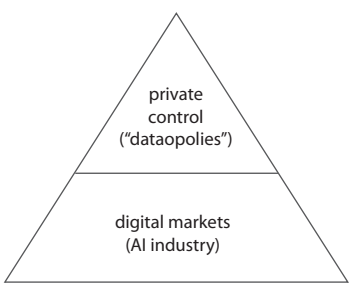


Figure 5: Structure of the digital markets and AI industry
Source: compiled by the author.

[31] Buttarelli 2019: 8.
[32] Buttarelli 2019: 9.

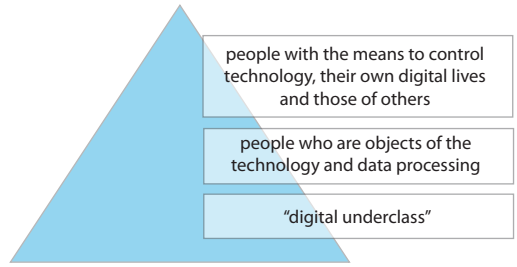


Figure 6: Structure of societies in the digital age
Source: compiled by the author.

The main consequence of this transformed structure is that the business interests of multinational tech giants often enjoy priority over the rights of individuals with less influence. This can also happen because privately-owned platforms act as intermediaries between the state and its citizens (see Figure 7), while those platforms have grown so large that they are not transparent and accountable.[33]

All of this also results in the most vulnerable workers in the private sector being monitored with the latest technologies, while dual-use technologies in the hands of authoritarian regimes are used to repress the human rights of minority groups.[34] Moreover, Balkin convincingly argues that due to the capabilities of the new technologies, the entire society is under surveillance, regardless of the social status of individuals.[35]

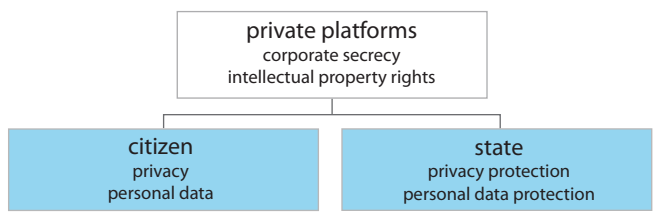


Figure 7: Interests of tech giants against the rights of the individual and role of the state
Source: compiled by the author.

[33] Buttarelli 2019: 11.

[34] Buttarelli 2019: 10.

[35] Balkin 2020: 16–17: "Fifth, the data that companies gather from end users can have significant external effects on third parties who may not even be users of the site. As digital companies know more about a given person, they can also know more about other people who are similar to that person or are connected to that person. In the digital age, everyone is always informing on everyone else. Thus, an individual's response to a notice-and-choice regime may affect the privacy of many other people who have no say in the matter. And when companies manipulate end users' moods and decisions – including their decisions to vote – they affect not only particular end users but many other people as well.
Notice-and-choice models are most inadequate when end users are most vulnerable, and when asymmetries of knowledge, power, and control are greatest. Put another way, notice-and-choice models of privacy are the most inadequate under precisely the conditions that define surveillance capitalism. That is why we need the fiduciary model."

Privacy 2030 warns of the dangers to democracy and the rule of law resulting from the operation of tech giants without democratic accountability, while also drawing attention to the fact that in case of infringement of the GDPR, anyone seeking redress can only achieve this by being represented at the court by expensive lawyers, which is unavailable to the average individual. Meanwhile, DPAs, "along with other enforcers, face enormous challenges in uncovering opaque business practices to uphold the rights of individuals".[36] According to the manifesto, either data protection rights can be enforced in court in a costly way, or the EU Member States' data protection authorities can try to enforce the data protection rules, which may not be in the financial interests of multinational companies.

Meanwhile, instead of solving social problems, tech giants are exacerbating the digital divide. *Privacy 2030* criticises the effects of their business strategies, arguing that societies "become dysfunctional when many people see others having more or better. This is the urgent ethical question of our day."[37]

Thus, the core message of this chapter is that the "EU should address not only digital disenfranchisement and lack of access to digital infrastructure and services but also digital inequality".[38]

The third chapter of *Privacy 2030* argues for a digital green new deal to achieve environmental sustainability.

The core message of this section is that digital technology and privacy regulation should not pose problems for each other, but can be part of the solution to the existing problems. In its current form, data maximisation works against EU law and environmental sustainability (Figure 8) since the "religion of data maximisation" appears unsustainable from an environmental perspective.[39]

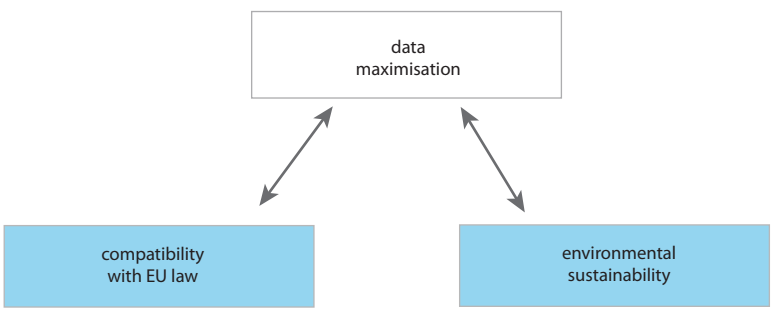


Figure 8: Data maximisation, EU law and environmental sustainability in Privacy 2030
Source: compiled by the author.

[36] Buttarelli 2019: 11.
[37] Buttarelli 2019: 12.
[38] Buttarelli 2019.
[39] Buttarelli 2019: 14.

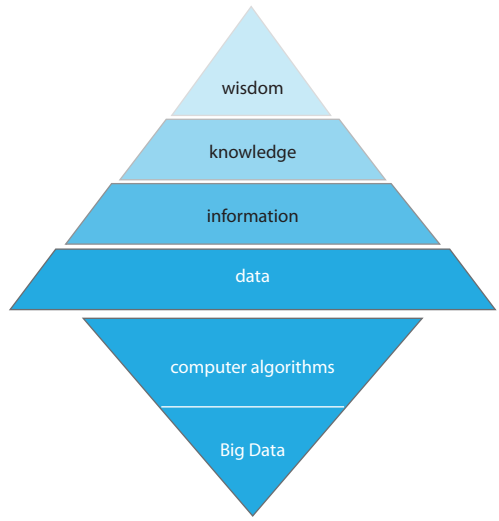


Figure 9: The traditional pyramid of learning – human
Source: compiled by the author.
Figure 10: The modern pyramid of learning – computer
Source: compiled by the author.

Other authors have expressed similar views. Harari, for example, also deals with the phenomenon of data maximisation, calling it "Dataism", or "Data Religion".[40] He points out how "Dataism" inverted the traditional pyramid of learning (see Figures 9 and 10). In his view, "[h]itherto, data was seen as only the first step in a long chain of intellectual activity",[41] but today "Dataists are sceptical about human knowledge and wisdom, and prefer to put their trust in Big Data and computer algorithms".[42]

From a global perspective, Buttarelli's paper presents a possible interpretation and sequence of events, which sheds light on the environmental, social, and human rights effects of the cooperation between tech giants and oil-producing multinationals (see Figure 11).[43]

40 Harari 2017: 428–462.
41 Harari 2017: 429.
42 Harari 2017.
43 Buttarelli 2019: 15.

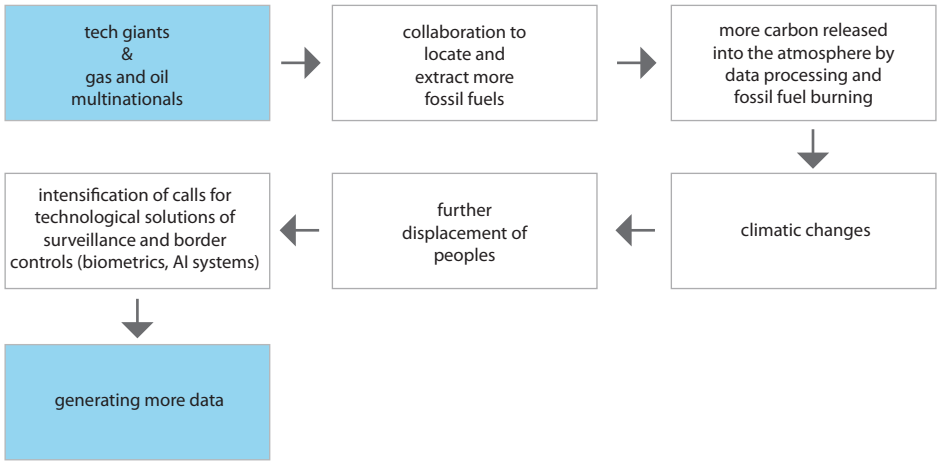


Figure 11: The data generating model of cooperation between tech giants and gas and oil multinationals
Source: compiled by the author.

At the same time, in *Privacy 2030,* Buttarelli notes that technological achievements do not necessarily only have negative effects. From an optimistic perspective, the chapter highlights how big data, AI and IoT can advance environmental sustainability[44] (see Figure 12).

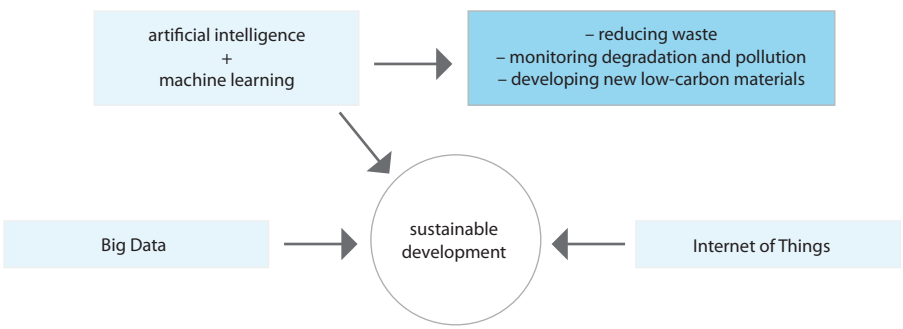


Figure 12: AI's role in advancing environmental sustainability according to Buttarelli
Source: compiled by the author.

[44] Buttarelli 2019: 16.

Privacy 2030 observes that a huge amount of data that has been collected, which is being controlled by 5-10 companies, mostly based in China and the United States. The main concern expressed in this chapter of the paper is how and whether that data is being used for the benefit of the public. The manifesto states that independent researchers and academics have difficulties while attempting to access these data that would be essential "to understanding the full extent of the harm wrought by their business models".[45]

The conclusion of this chapter is that upholding the core principles of the EU's approach to data protection, such as data minimisation and quality on the one hand, and access to large companies' datasets on the other, would also help to fight the expanding carbon footprint of digital technology and environmental degradation.[46]

The fourth chapter of *Privacy 2030* deals with the harmful effects of modern digital technologies as a new business model, which represents the greatest danger from the point of view of the most vulnerable individuals.

The paper convincingly argues that after 2000 the business model changed, in contrast to traditional media and advertising practices, from then on becoming based on the monitoring of users and the collection of their personal data for business purposes. With the development of technology, more and more sensitive personal data is collected by the devices around us, until finally the tech firms and governments are not only monitoring our environment, but also extending their surveillance to people's biometric data, DNA and even brain waves (see Figure 16).[47]

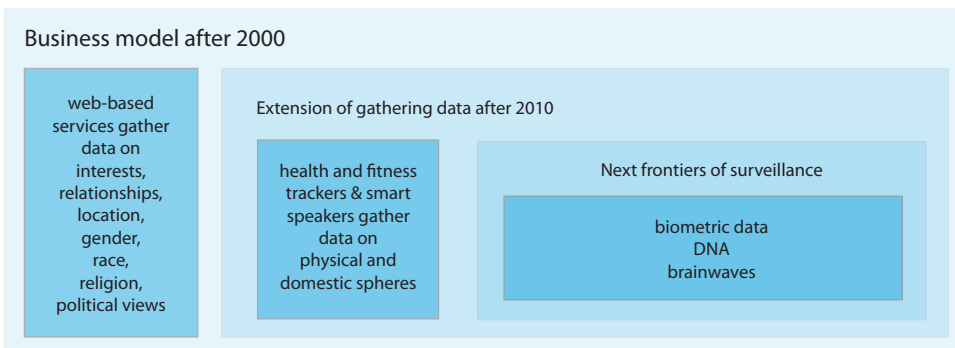


Figure 13: The new business model of web-based services
Source: compiled by the author.

[45] Buttarelli 2019.
[46] Buttarelli 2019.
[47] Buttarelli 2019: 19.

A very fair warning was delivered in *Privacy 2030* by highlighting how easily the "manipulation machine" works since, due to the concentration of the market for mass internet communications, "the big platforms provide an easy target for exploits [sic]".[48]

The paper repeatedly argues that the large tech companies should be held accountable for their actions. The vision, published in 2019, stated that the "EU still has the chance to entrench the right to confidentiality of communications in the ePrivacy Regulation under negotiation, but more action will be necessary to prevent further concentration of control of the infrastructure of manipulation".[49] If this statement was clearly true in 2019, then four years later, in 2023, when the ePrivacy Regulation is still "under negotiation", is no exaggeration to state that the "manipulation machine" has won the first battle against transparency, accountability and sustainable data processing.

The ethically well-grounded main argument in *Privacy 2030* against data maximisation and the misuse of individuals' personal data derives from the right to human dignity that "demands limits to the degree to which an individual can be scanned, monitored and monetised".[50]

The fifth chapter of Buttarelli's manifesto explores the role of the EU in the regulation of new technologies. This categorically refers to the context of democracy and human rights and clearly distinguishes autocracies from democracies, even raising the possibility of a "splinternet", in the event that "certain regions of the world cannot safeguard the values of human dignity and democracy".[51]

The final chapter of Buttarelli's *Privacy 2030* argues that besides the modernised Convention 108, the GDPR is only one possible tool for the protection of personal data and thereby privacy,[52] although the joint application of several other regulations is necessary for effective legal protection[53] (see Figure 14).

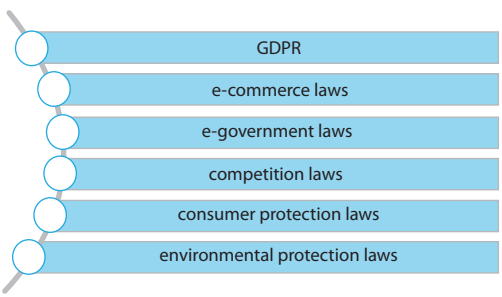


Figure 14: Tools of privacy and data protection in the European Union
Source: compiled by the author.

[48] Buttarelli 2019: 17.
[49] Buttarelli 2019: 18.
[50] Buttarelli 2019: 19.
[51] Buttarelli 2019: 21.
[52] Buttarelli 2019.
[53] Buttarelli 2019: 23–24.

Figure 15: Results of cooperation between competition and data protection authorities
Source: compiled by the author.

This part of the paper urges DPAs and the competition authorities of the Member States to cooperate in order to take effective action against multinational tech giants, where this is justified by the public interest.[54]

According to Buttarelli's vision, such cooperation could have a number of results (see Figure 15).[55] Among those possible effects, participation, or at least its transatlantic interpretation, is treated by Balkin in the context of freedom of expression that is essential for a democratic society: "the right of freedom of expression is not only the right to participate in democracy, but also the right to participate in a democratic culture."[56]

This final part of the manifesto states that these outcomes serve the social and environmental good through the appropriate handling and processing of personal data using new technologies, which can lead to the sovereignty of (European) values and technologies (see Figure 16).[57]

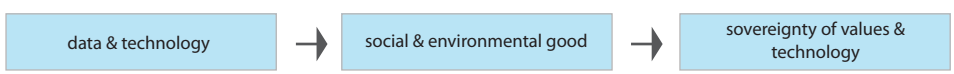


Figure 16: Personal data and digital sovereignty
Source: compiled by the author.

[54] Buttarelli 2019: 24.
[55] Buttarelli 2019: 27.
[56] Balkin 2016: 1212.
[57] Balkin 2016.

This concept of sovereignty of values and technology is expressed in a radical assertion made in this chapter: "Personal data generation that does not serve democratically mandated public interests or empower people should be treated like data pollution that has a real life impact on society and the environment."[58] This conclusion is in line with the previously elaborated issues related to human rights, environmental sustainability, data minimisation and maximisation or corporate accountability.

Therefore, one may conclude that this chapter argues convincingly for the necessity of building a European digital commons, especially if we take into consideration some apparent hostility toward the ePrivacy Regulation that "indicates a backlash of the EU's ambition to modernise its privacy norms".[59]

ON BUTTARELLI'S TRAILS – ACTUAL QUESTIONS OF THE DATA PROTECTION PROVIDED BY HUNGARIAN PUBLIC ADMINISTRATION

Although *Privacy 2030* outlines a mostly EU-level vision, the enforcement of relevant data protection rules, such as the GDPR, remains the task of the Member States, including their data protection authorities, and Buttarelli encouraged these bodies to better cooperate with each other and the competition authorities.

The issue of artificial intelligence (AI), mentioned several times in the manifesto, clearly appeared in the decision NAIH-85-3/2022 of the Hungarian National Authority for Data Protection and Freedom of Information (NAIH).[60] Based on Article 58(2) (d) of the GDPR, the Hungarian DPA ordered the controller, a local commercial bank, to bring its data processing operations into compliance with the provisions of the GDPR, that is, to abstain from analysing emotions during AI-based audio analysis of the clients' conversations with its call centre, and to properly ensure the rights of the data subjects. Since the decision also imposed a 250 million HUF administrative fine, the data controller filed a motion to the Budapest Capital Regional Court, seeking for legal remedy. As of now, the legal process is still ongoing, therefore it is necessary to wait until this is concluded for a further analysis of how effectively the Hungarian DPA protects data subjects' rights when the GDPR is infringed by AI-based data processing.

Privacy 2030 also deals with the issue of the unfair use of personal data as an inherent feature of the new web-based business model. The NAIH, which is the Hungarian DPA, often receives complaints regarding the data processing activities of multinational tech giants established in Ireland. Since the Irish DPA's activity in the field of the protection of personal data did not meet the data subjects', the DPAs' or the EDPB's expectations, Article 65(1) (a) of the GDPR has been applied regarding several cases pending before the

[58] Balkin 2016: 25.
[59] Balkin 2016: 26.
[60] NAIH decision NAIH-85-3/2022. See: www.naih.hu/hatarozatok-vegzesek/file/517-mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei

Irish DPA, resulting in the EDPB's binding decisions in 2022. This recent turn of events[61] highlights the importance of effective cooperation between the EDPB and the DPAs.

Privacy 2030 states: "The ethnic profile of the typical European data protection authority, perhaps even more than the Silicon Valley coding community, is overwhelming white. Agencies in the EU should diversify their own workforce better to reflect the societies they represent by recruiting more people of colour and ensuring gender balance."[62] If we are to take Buttarelli and the editors of his posthumous paper seriously, it is worth examining the demographics of the Hungarian DPA's personnel more closely.

Since there is no acceptable reason to process personal data about the ethnic profile of the employees [see Art. 9(1) GDPR], it is impossible to provide reliable statistics on the number of members of staff from ethnic minority backgrounds. In addition, it should be pointed out that unlike many European countries, Hungary statistically has no significant proportion of "people of colour" among its inhabitants, therefore only the number of Hungarian Roma population can be examined as such (see Figure 17), while bearing in mind that being Roma means an identity and not necessarily the colour of one's skin.

Based on the official 2011 statistics (KSH), 3% of the Hungarian population declared themselves to be Roma.[63] There is no legal ground for processing a list of the ethnic background of employees, but it seems to be reasonable to conclude that not even 3% of the personnel of NAIH was recruited from among the Roma. According to NAIH statistics from 15 June 2022, of it had 113 employees at that time,[64] meaning the lack of at least 3-4 Roma employees, in terms of the requirements of *Privacy 2030,* would represent room for HR improvement in this area for the DPA.

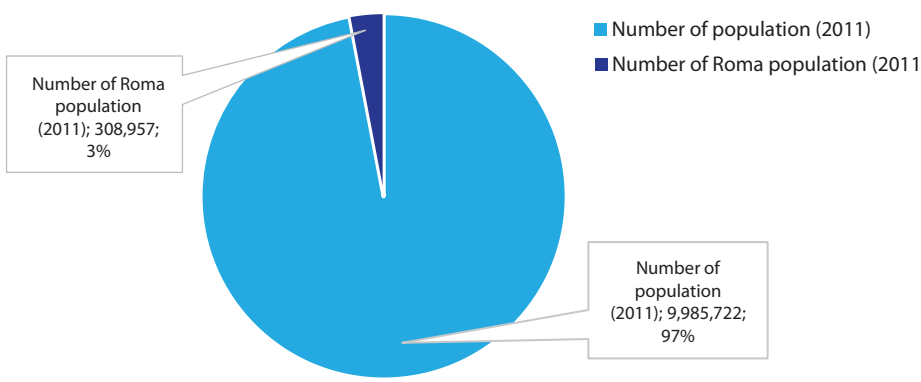


Figure 17: Number of Roma population in Hungary (2011)
Source: compiled by the author.

[61] DPC 2023.
[62] Buttarelli 2019: 24.
[63] See: www.ksh.hu/nepszamlalas/docs/tablak/nemzetiseg/09_01_02.xls
[64] NAIH equal opportunities policy (June 15 2022), 1–2.

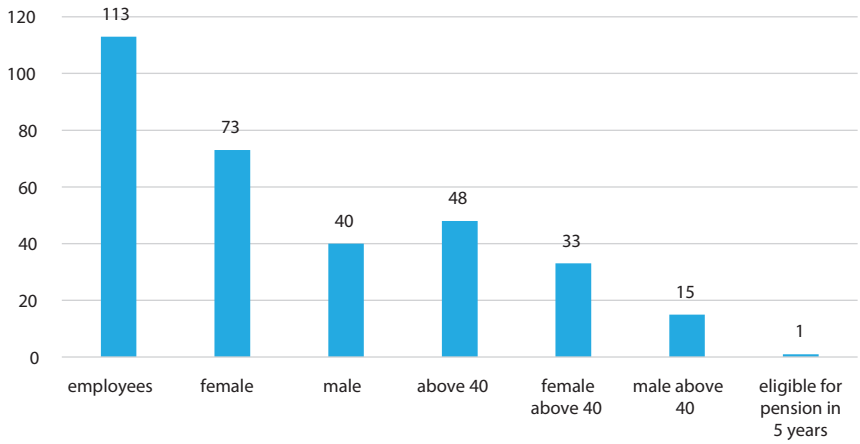


Figure 18: Gender and age balance of employees of NAIH, the Hungarian DPA (June 15, 2022)
Source: compiled by the author.

The gender balance, and the age balance not mentioned in the manifesto, can be better analysed based on the same NAIH statistics, which indicate that 65% of the employees are female and 35% are male.

Further analysing the available NAIH statistics, it can be stated that the gender balance and also the age balance clearly shows that males, and especially those above the age of 40, regardless of whether they are "people of colour" or not, are underrepresented (see Figure 18).

Privacy 2030 with its complex vision requires not only the EU to act, but also expects each Member State's DPA to exercise its enforcement powers. The question of the possible influence of public administration is well-known in the theory of Hungarian public administration. Focusing on the non-hierarchical administration, András Patyi describes Tibor Madarász's model, pointing out that there is necessarily a sphere that falls out of the scope of the influence of the authorities (see Figure 19).[65]

	influence of public administration public authority				activities out of the scope of the influence of public administration	
activity / (legal) situation	acts	prohibits	prescribes	restricts	informs	raises awareness / culture of data protection
all						
most						
many						
certain						

Figure 19: The Madarász model of the scope of influence of public administration
Source: compiled by the author.

[65] Patyi 2017: 56–58.

The theoretical question of the influence of public administration became quite practical, when the NAIH decided in 2020 that, based on Article 58(2) (g) of the GDPR, it has the corrective power to order ex officio the erasure of personal data in a situation where such request was not submitted by any data subject. The legal debate about the corrective powers of the Hungarian DPA finally resulted in the very important 3110/2022 (III. 23.) AB decision.[66]

One of the most significant decisions of the Constitutional Court of Hungary in recent years related to the administrative protection of personal data is the 3110/2022 (III. 23.) AB decision. In 2021, after it lost an administrative lawsuit, NAIH submitted a constitutional complaint to the Constitutional Court to annul judgments 105.K.706.125/2020/12 of the Budapest-Capital Regional Court and Kfv.II.37.001/2021/6 of the Kúria (i.e. supreme court), as it considered the two court decisions to be contrary to the Fundamental Law of Hungary.[67]

Initiated by an individual's notification, NAIH conducted a data protection inquiry, and after the data controller partly disputed the findings, an ex officio authority procedure for data protection was initiated against the data controller who had collected signatures (and other personal data, including e-mail addresses) for his campaign called "Let's join the European Public Prosecutor's Office".

In its final decision NAIH/2020/974/4,[68] the authority found that the data controller had collected the personal data of the data subjects without legal basis for the purpose of maintaining further contact, and did not provide adequate information on all the essential circumstances of the data processing, thereby infringing several articles of the GDPR. The DPA also found that since the data controller had not provided adequate information to the data subjects about the purpose of the data processing, this violated the basic requirement of fair data processing [Article 5(1) (a) GDPR, "lawfulness, fairness and transparency"]. The authority ordered the data controller to erase the unlawfully collected personal data and obliged him to pay a 1 million HUF data protection fine {3110/2022 (III. 23.) AB decision [2]}.

The data controller (plaintiff) filed a suit for legal remedy to the Budapest-Capital Regional Court, reasoning that the authority, in accordance with Act CXII of 2011 on the right to informational self-determination and on the freedom of information (Infotv.), could only have applied the legal consequences (expressly) defined in the GDPR, so the authority would not have been entitled to order the ex officio erasure of the collected personal data. The court of first instance came to the conclusion that "data erasure can only take place upon the request of the data subject, the petitioner [i.e. NAIH] is not entitled to order it ex officio, its provision to this effect is null and void due to the violation of its powers" {3110/2022 (III. 23.) AB decision [2]}.

66 3110/2022 (III. 23.) AB decision.

67 This section is based on the translation of the author. The English texts below are not official translations of the quoted Court judgements and decisions of the Constitutional Court of Hungary.

68 NAIH/2020/974/4, see: www.naih.hu/files/NAIH-2020-974-hatarozat.pdf

For different reasons, both the plaintiff and the defendant appealed the decision to the Kúria. The Kúria rejected the data controller's appeal for procedural reasons, but regarding the authority's appeal against the decision of the court of first instance, confirmed the decision in its effect. Kúria found that

- the disputed part of the authority's final decision was not suitable for review, as the petitioner did not comply with its obligation to provide reasoning; furthermore,
- neither the appeal nor the counter-appeal contested that the court of first instance made the legal basis of an incompletely justified decision [of NAIH] the subject of a legal review, partly ex officio and partly based on the authority's new argument {3110/2022 (III. 23.) AB decision [4]}.

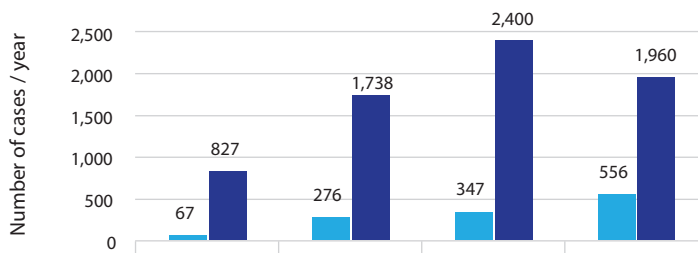
Therefore, the Kúria carried out a substantive inquiry related to the findings of the judgement's further references on its legal bases, and on the grounds of joint interpretation of Articles 58(2) (g) and 17 of the GDPR, it came to the conclusion that "erasure of data can only take place at the request of the data subject, so it was justified for the Regional Court to find that the petitioner [i.e. NAIH] lacks the powers to order the erasure ex officio" {3110/2022 (III. 23.) AB decision [4]}.

Following the judgment of the Kúria, Hungarian DPA submitted a constitutional complaint to the Constitutional Court because, according to its position, the court decisions of first and last instance violated several provisions of the Fundamental Law of Hungary, and the contested judgments limited the powers of the authority laid down in the Fundamental Law that resulted in a "serious disruption" of its operation, and therefore those decisions were contrary to the Fundamental Law. The authority therefore requested that the Constitutional Court declare the two judgements to be contrary to the Fundamental Law and to annul them, as well as submitting a request to suspend the execution of the judgments. {3110/2022 (III. 23.) AB decision [5]}. Regarding the danger of disruption of its operation caused by the two judgments, NAIH alleged that:

- ex officio ordering the erasure of data processed unlawfully has long been within its power
- it would mean emptying the DPA's power of control provided in the Fundamental Law, if the authority only has the option of formal control, without actual means of intervention
- according to the logic of the two contested court decisions, the data subjects must first request the erasure of their personal data from the data controller, and then they can apply to the authority based on Article 77 GDPR, which "in case of unlawful data processing involving hundreds of thousands or millions of data subjects, it can also represent an unmanageable amount of official cases in the operation of the petitioner, the same time it also has a negative effect on the enforcement of data subject rights, while until the end of which the personal data will remain in the – unlawful – processing of the data controller, without effective supervisory control"

– it is contrary to the powers of the public authorities guaranteed in the Fundamental Law, if the DPA "is barred from ex officio erasure of unlawfully processed data, because this deprives the data protection authority of the possibility of substantive, effective and efficient reparation of the infringement of rights, consequently the level of the protection of fundamental rights previously achieved is lowered, and in practice serious dysfunctions occur" {3110/2022 (III. 23.) AB decision [6]}

The NAIH also objected that the two Courts had reached their conclusions by applying a merely semantic interpretation of the GDPR, which is contrary to Article 28 of the Fundamental Law. Moreover, the authority took the firm position that the Courts "came to a conclusion clearly contrary to the Fundamental Law within the scope of the interpretation of the legal norms, and the regulations were not actually interpreted, but overwritten, and they carried out legislative activity contra legem, even contra constitutionem, in a way that violates legal certainty", which on the other hand also raises the issue of the violation of the right to a fair trial, since the two Courts that acted "absolved themselves from the principle of subjection to the law" {3110/2022 (III. 23.) AB decision [7]}.



	2018	2019	2020	2021
authority procedure	67	276	347	556
authority inquiry	827	1,738	2,400	1,960

Figure 20: Data protection procedures 2018–2021
Source: compiled by the author based on NAIH 2021.

In terms of legal certainty, the authority referred to the fact that Recital (129) GDPR also expresses the requirement for consistent and uniform enforcement, within the framework of which other supervisory authorities also recognise the power to order erasure of personal data ex officio.

According to the DPA's argument, both the Regional Court and the Kúria failed to initiate the preliminary ruling procedure in connection with the provisions of the GDPR. In the authority's view, this violated the authority's right to due process and legal remedy, as well as limiting its powers of control, especially given that all the relevant aspects of EU law remained unexplored and the relevant provisions were interpreted differently from

the purpose of the legal norm. "Therefore, this violation of fundamental rights occurred due to the absence of sufficient legal reflection on EU law." The NAIH also found it to be a violation of its fundamental rights that the Courts "did not comply with their obligation to provide reasons, did not examine its arguments regarding the essential part of the case with sufficient thoroughness, and in violation of the obligation to remain within the limits of the request for legal review, the Kúria examined issues that were not the subject of the judicial review" {3110/2022 (III. 23.) AB decision [8]}.

In order to explain her legal position, the Constitutional Court contacted the Minister of Justice, who explained in her reply that

- the constitutional complaint concerns the content of the disputed judicial decisions and not the applied law, therefore she cannot evaluate those
- the Court of Justice of the European Union is authorised to interpret the GDPR authentically
- the corrective powers provided by GDPR also extend to data protection supervisory authorities ordering the data controllers to bring their data processing operations into compliance with the provisions of GDPR, which may even mean an order to erase unlawfully processed personal data, "the Government is not aware of any legal interpretation contrary to this in connection with the enforcement of the GDPR in the Member States"
- a legal interpretation, which prohibited the ordering of ex officio data erasure "would lead to a seriously disadvantageous, constitutionally unjustifiable situation for the data subjects, as a situation would arise in which a multitude of the data subjects would not have access to legal protection in the absence of an expressed will during the application of the GDPR, […] thus this would result in constitutionally unjustified distinct (discriminatory) and different regimes in nature"
- the legislator tried to clarify the legal interpretation giving priority to EU law with the amendment of Infotv. that would come into force on 1 January 2022 {3110/2022 (III. 23.) AB decision [11]}

The Constitutional Court considered the constitutional complaint of the Hungarian DPA well-grounded {3110/2022 (III. 23.) AB decision [25]}.

In its 3110/2022 (III. 23.) AB decision, it explained, among other things, that all the provisions of the GDPR fundamentally serve the purpose of limiting personal data processing within legal boundaries, which can be based on the application of the basic principles {3110/2022 (III. 23.) AB decision [35]}.

The Constitutional Court essentially accepted the authority's argument, but also found that, as its 2/2019 (III. 5.) AB decision had already explained, "the binding force of European Union's law does not originate from itself, but is based on Article E) of the Fundamental Law, and does not override Article R) (1) of the Fundamental Law, according to which the Fundamental Law is the foundation of the legal system of Hungary" {3110/2022 (III. 23.) AB decision [42]}. The decision also explained that following the submission of the motion

by the NAIH to the Constitutional Court, the authority turned to the European Data Protection Board regarding the interpretation of the powers laid out in Article 58(2) (g) of the GDPR.

In its opinion 39/2021[69] adopted on 14 December, 2021, the EDPB explained that Article 58(2) (g) and Article 17 of the GDPR regulate two different cases, so the former one "provides an appropriate legal basis for the supervisory authority to order ex officio the erasure of unlawfully processed personal data in cases where the data subject (érintett) has not submitted such a request" {3110/2022 (III. 23.) AB decision [51]}. The Constitutional Court came to the conclusion that the two disputed judgements are not in accordance with the function and content of the GDPR in terms of the right to protection of personal data as a fundamental right {3110/2022 (III. 23.) AB decision [54]}.

It also noted ironically that the Courts involved in the case "did not perceive that the broad data protection supervisory authority control was ensured based on the obligations arising from the Fundamental Law, EU law and international law, even before the GDPR". Furthermore, it determined that "based on paragraphs (2) and (3) of Article E) and Article VI(4) of the Fundamental Law, and GDPR as a source of EU law ensuring the uniform application of data protection and freedom of information, the Authority is entitled to order ex officio the erasure of unlawfully processed personal data even in the lack of a request to this effect" {3110/2022 (III. 23.) AB decision [56]}.

Consequently, the Constitutional Court established that the "Kúria's judgement No. Kfv.II.37.001/2021/6. and the Budapest-Capital Regional Court's judgement No. 105.K.706.125/2020/12. are contrary to the Fundamental Law", and therefore cancelled them {3110/2022 (III. 23.) AB decision [57]}.

Since the Constitutional Court reached a decision based on the above points, it did not find it justified to examine the NAIH's further arguments.

In this case, Buttarelli's warning came true, as the authority's decision was contested,[70] but the NAIH was also confident about the meaning and role of its corrective powers.

CONCLUSIONS

Although Hungarian law and its theory approaches data protection from different directions than Buttarelli, finally we may conclude, agreeing with him, that public administration is currently facing enormous challenges at a time when our societies are under metamorphosis due to the increasing use of AI, algorithms and many other ICT-related data processing activities.

[69] EDPB opinion 39/2021 (December 14, 2021). Source: https://edpb.europa.eu/system/files/2022-01/edpb_opinion_202139_article_582g_gdpr_en.pdf

[70] Buttarelli 2019: 23.

Hopefully, these changes will not end in a dystopian and authoritarian future, but will instead contribute to a more transparent and democratic world.

While the effective enforcement of the GDPR is expected from DPAs, it is equally important to raise data subjects' awareness of their rights in data protection and to encourage data controllers to implement additional data protection measures. Only public administration, data controllers and data subjects together can build what we may call a "*data protection culture*".[71]

REFERENCES

Balkin, Jack M. (2016): Information Fiduciaries and the First Amendment. *University of California Davis Law Review,* 49(4), 1185–1234.

Balkin, Jack M. (2020): The Fiduciary Model of Privacy. *Harvard Law Review Forum,* 134(11), 11–33. Online: https://harvardlawreview.org/wp-content/uploads/2020/10/134-Harv.-L.-Rev.-F.-11.pdf

Buttarelli, Giovanni (2019): *Privacy 2030: A New Vision for Europe.* Online: https://iapp.org/media/pdf/resource_center/giovanni_manifesto.pdf

DPC (2023): *Data Protection Commission Announces Conclusion of Two Inquiries into Meta Ireland.* 4 January 2023. Online: www.dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland

EDPB opinion 39/2021 (December 14, 2021). Online: https://edpb.europa.eu/system/files/2022-01/edpb_opinion_202139_article_582g_gdpr_en.pdf

Farrell, Maria (2019): Afterword: A Cage Went in Search of A Bird. In Buttarelli, Giovanni: *Privacy 2030: A New Vision for Europe.* [s. l.]: IAPP, 35–36. Online: https://iapp.org/media/pdf/resource_center/giovanni_manifesto.pdf

Harari, Yuval Noah (2014): *Sapiens.* London: Vintage Books.

Harari, Yuval Noah (2017): *Homo Deus.* London: Vintage Books.

Jayaram, Malavika (2019): Afterword: The Future is Already Distributed – It's Not Evenly Just. In Buttarelli, Giovanni: *Privacy 2030: A New Vision for Europe.* [s. l.]: IAPP, 31–32. Online: https://iapp.org/media/pdf/resource_center/giovanni_manifesto.pdf

Kolbert, Elizabeth (2015): *The Sixth Extinction.* London – New Delhi – New York – Sydney: Bloomsbury.

NAIH (2021): *A Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2021. évi tevékenységéről.* Budapest: Nemzeti Adatvédelmi és Információszabadság Hatóság. Online: https://naih.hu/eves-beszamolok?download=507:naih-beszamolo-a-2021-evi-tevekenysegrol

NAIH equal opportunities policy (June 15, 2022).

[71] Szabó 2022: 67.

Panetta, Rocco (2019): Afterword: Privacy 2030: To Give Humans a Chance. In Buttarelli, Giovanni: *Privacy 2030: A New Vision for Europe.* [s. l.]: IAPP, 37–40. Online: https://iapp.org/media/pdf/resource_center/giovanni_manifesto.pdf
Patyi, András (2017): *A közigazgatási működés jogi alapjai.* Budapest: Dialóg Campus.
Polonetsky, Jules (2019): Afterword: A Mission Greater Than Compliance. In Buttarelli, Giovanni: *Privacy 2030: A New Vision for Europe.* [s. l.]: IAPP, 33–34. Online: https://iapp.org/media/pdf/resource_center/giovanni_manifesto.pdf
Rodotá, Stefano (2004): *Privacy, libertà, dignità.* Discorso conclusivo della Conferenza internazionale sulla protezione dei dati. Online: www.privacy.it/archivio/rodo20040916.html
Rodrik, Dani (2012): *The Globalization Paradox.* Oxford: Oxford University Press.
Rotenberg, Marc (2019): Afterword: The Future of Privacy and a Vibrant Democracy. In Buttarelli, Giovanni: *Privacy 2030: A New Vision for Europe.* [s. l.]: IAPP, 29–30. Online: https://iapp.org/media/pdf/resource_center/giovanni_manifesto.pdf
Sartori, Giovanni (1987): *Theory of Democracy Revisited I–II* Chatham, NJ: Chatham House.
Szabó, Endre Győző (2022): *A védelmi lépcső elmélete.* Budapest: Ludovika.
Zuboff, Shoshana (2019): Afterword: Many Facets of the Same Diamond. In Buttarelli, Giovanni: *Privacy 2030: A New Vision for Europe.* [s. l.]: IAPP, 41–42. Online: https://iapp.org/media/pdf/resource_center/giovanni_manifesto.pdf

Constitutional Court of Hungary's decisions

2/2019 (III. 5.) AB decision
3110/2022 (III. 23.) AB decision

Court decisions

Kúria's judgement No. Kfv.II.37.001/2021/6.
Budapest-Capital Regional Court's judgement No. 105.K.706.125/2020/12.

NAIH decisions

NAIH/2020/974/4. Online: www.naih.hu/files/NAIH-2020-974-hatarozat.pdf
NAIH-85-3/2022. Online: www.naih.hu/hatarozatok-vegzesek/file/517-mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei

Imre Borisz Páll is a lawyer, specialised in Data Security and Data Protection (LL. M.). He is currently Head of Department at the National Authority for Data Protection and Freedom of Information. He is a PhD student at Ludovika University of Public Service Doctoral School of Public Administration. His area of expertise is the administrative law issues of data protection subject to the EU General Data Protection Regulation. His research area in the doctoral school is "Public Administration and Governance", his research topic is "The impact of new technologies on the social public sphere and and democracy". Within this framework, "The role of data protection law in the context of protecting human dignity and ensuring social publicity".