Santander Art and Culture Law Review 2/2023 (9): 215-242
DOI: 10.4467/2450050XSNR.23.029.18649

VARIA

Gábor János Dudás*

gaborjanos.dudas@uni-corvinus.hu
orcid.org/0009-0002-1935-3765
Corvinus University of Budapest
Institute of Accounting and Economic Law
Fővám tér 8.
Budapest, Hungary

András György Kovács**

kovacsandras@birosag.hu
orcid.org/0000-0002-9768-7982
Eötvös Loránd University
Faculty of Law
Egyetem tér 1.
Budapest, Hungary

Márton Schultz***

schultzmarton@gmail.com
orcid.org/0009-0002-6659-5636
Hungarian Intellectual Property Office
Legal and International Department, Industrial Property Law Division
II. János Pál pápa tér 7.
Budapest, Hungary

Personal Data as Consideration

* **Gábor János Dudás** is Assistant Professor at the Institute of Accounting and Economic Law, Corvinus University of Budapest (Hungary). He holds a PhD (in law from public procurement and freedom of information). He also serves as Partner at DHZ Legal [Dudás Hargita Zavodnyik Ügyvédi Iroda]. He is also Attorney at Law, National Authority for Data Protection and Freedom of Information.

** **András György Kovács** is Habilitated Associate Professor at the Faculty of Law, Eötvös Loránd University (ELTE University) in Budapest (Hungary). He holds a PhD (in law from electronic communication). He also serves as Administrative Judge and Head of Panel dealing with data protection, competition, and consumer law, Curia of Hungary.

*** **Márton Schultz** is Legal Administrator, Hungarian Intellectual Property Office, Legal and International Department, Industrial Property Law Division, in Budapest (Hungary). He holds an LLM from Universität Potsdam and University of Szeged and a PhD from University of Szeged (in law from privacy).

Abstract: This article argues that personal data may have a commercial value in the European legal systems, and as such it can function as a consideration and has a *quid pro quo* character. It claims that the European Data Protection Board (EDPB) should not exclude that data concerning the data subject can be used as contractual consideration, especially in the world of the Internet. In particular, it cannot be excluded solely on the basis that the right to privacy is not transferable, a position taken thus far in the EDPB's practice. This proposed new approach is supported by the fact that in some EU Member States the property aspects of the general right of personality have been recognized, a stance which may also apply to personal data, without the need to recognize a kind of data ownership or *sui generis* intellectual property right in the data. Thus, the theory of commercial aspects of personality rights can be linked to the commercial value of personal data. The *quid pro quo* function of personal data may also be recognized in line with the provisions of the General Data Protection Regulation (GDPR). In fact, maintaining the interpretation of the EDPB – which denies the *quid pro quo* character of personal data from a fundamental rights perspective – means that the dangers of such data processing cannot be assessed. This affects cultural heritage in many aspects – from the sending of newsletters to selling merchandise products in museums. The EDPB's guidelines, as soft law, have no direct impact on the case-law of the national courts, thus this also significantly increases the risk of a collision between the simultaneously available remedy regimes established by the GDPR.

Keywords: commercial value of personal data, European Data Protection Board, commercialization of personality rights, personal data as an asset

Introduction

Today it has become clear that personal data has a huge potential in the digital single market of the European Union (EU), with data controllers, data processors, data miners, and data traders being the main winners.[1] As pointed out by the European Data Protection Board (EDPB), some online (social media or search) services are financed by users' payments, while some others are financed by the sale of online advertising services that reach the data subjects without any financial consideration from the consumer.[2] The economic role of personal data is particularly prevalent in connec-

[1] L. Trakman, R. Walters, B. Zeller, *Is Privacy and Personal Data Set to Become the New Intellectual Property?*, "International Review of Intellectual Property and Competition Law" 2019, Vol. 50(8), p. 948.

[2] EDPB, *Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects*, 8 October 2019, para. 4.

tion with the data management purposes of giant online platforms, such as the personalization of content, behavioural advertising, and data sharing.

As in all other cases, legislation and practice in this area try to keep pace with the changes in social conditions, including market conditions. It is now clear that personal data can be the subject of commercial transactions. This approach is also generally accepted in EU legislation, and is the regulatory logic behind the so-called "Digital Directive"[3] and the current drafts of the Data Act[4] and the Data Governance Act.[5] Personal data can therefore undeniably be the subject of a contract or a service to be provided under a contract.

However, the question of whether personal data is admissible as compensation for a contractual service remains open to the courts – including both the EU courts and the courts of the Member States. In other words, it is not a question of whether we can pay for the data, but whether we can pay for a service with our data, and if so, when the sharing of personal data constitutes consideration. Neither the Data Act nor the Data Governance Act are primarily intended to cover contractual arrangements between the consumer (data subject) and the data controller; and this is the subject of this paper. Insofar as regards the relationship between the data subject and the data controller, as it is currently regulated by the General Data Protection Regulation (GDPR),[6] it is neither implied that personal data can be consideration for a contract, nor that they have a monetary value, although it is not clear from the text of the norm that it adopts a contrary position. This is a significantly different position from, for example, the California Consumer Privacy Act (CCPA). In California, consumers have the right to object to the controller selling their personal data at any time (the so-called right to opt out).[7]

In our view, given the dominance of digital technologies this issue may become particularly relevant in all areas of social life, including the protection and enjoyment of digital heritage. For example, it is questionable whether a visitor can pay for a museum ticket by allowing the museum to resell, for advertising purposes, his or her personal data that were electronically provided by the visitor when purchasing the ticket. If the answer is no, the museum is obliged by the principles of data protection to clearly separate the legal transaction of admission to the museum and

[3] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, OJ L 136, 22.05.2019, p. 1.

[4] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)*, 23 February 2022, COM(2022) 68 final.

[5] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJ L 152, 3.06.2022, p. 1.

[6] 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, GDPR), OJ L 119, 4.05.2016, p. 1.

[7] California Consumer Privacy Act of 2018, Calfiornia Civil Code [1798.100-1798.199.100] (Title 1.81.5 added by Stats. 2018, Ch. 55, Sec. 3), Section 1798.120.

the processing of the data provided to it in this context from resale for advertising purposes as a separate transaction. If, however, the *quid pro quo* function of personal data is accepted, these two transactions can be merged into a single contractual agreement. But we can also turn this question around and ask whether access to a digital archive is free of charge if there is no charge for its access, but it is subject to registration with the obligation to provide personal data; and if not, whether the digital archive provider is obliged to allow the user requesting access to be exempted from the obligation to register, in whole or in part, by paying a certain amount. This is because the concept of consent as a legal basis for data processing includes the concept of voluntariness; the consent to data processing is only acceptable if it is given voluntarily. Thus, if the registration is mandatory for access, this in principle eliminates voluntariness, and in order to ensure free choice (as a precondition for voluntariness), the controller should and could offer an alternative means of access. If, on the other hand, the data provided during the registration can be used as a *quid pro quo*, then it is no longer necessary to provide voluntary access, and alternative access options are not necessary.

As we will see, the traditional approach to data protection has rejected the possible *quid pro quo* function of personal data, based on the fact that informational self-determination is deemed to be a protected fundamental right. A purely fundamental rights-based approach that neglects the commercial value of personal data could ultimately lead to individuals losing the right of disposal over their personal data,[8] as in the absence of adequate regulation large companies and online content providers could seek to exploit and commercialize their large data sets by using extra-legal means. Their actions may allow them to make significant amounts of profits on their data sets, while at the same time they may prevent data subjects from using their own data for commercial purposes.

Therefore, in the authors' view it is no longer possible to "hide" behind the argument according to which the right to privacy is a non-transferable fundamental right, but rather it is necessary to develop multi-disciplinary legal solutions which, while maintaining the dominance of the fundamental rights approach, ensure that the persons concerned can exercise their contractual freedom and informational self-determination in a way that allows them to commercially exploit their data, and which at the same time limits the same aspirations on the part of large companies, as in the case of consumer contracts. Economic operators can be compelled to engage in lawful conduct if the disadvantages of the unlawful conduct outweigh the benefits to be gained from an infringement.[9]

[8] O. Tene, J. Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, "Northwestern Journal of Technology and Intellectual Property" 2013, Vol. 11, p. 241.

[9] A. Menyhárd, *A magánélethez való jog a szólás- és médiaszabadság tükrében* [The Right to Privacy in the Context of Freedom of Expression and Media Freedom], in: Z. Csehi, A. Koltay, Z. Navratyil (eds.), *A személyiség és a média a polgári és a büntetőjogban*, Complex, Budapest 2014, p. 207.

The assessment of the *quid pro quo* function of personal data requires a holistic approach: in addition to data protection, it is primarily a matter of fundamental and personality rights, which also affect the fields of contract law, consumer protection law, and competition law. Thus when writing the present study, the authors have thus adopted a pragmatic research paradigm, following the logic of each of the above-mentioned areas of law while examining the central question of whether personal data can constitute consideration. Our research hypothesis was that if, according to the majority of the jurisdictions examined, it is possible (or at least not excluded) that personal data in a commercial transaction can be not only a service but also a consideration, then the traditional approach to data protection – which rejects this thesis – needs to be revised. The authors do not see the solution to this in amending or supplementing the GDPR, but in altering the related interpretation of the law. They also view the theoretical possibilities inherent in this approach, similar to the existence of the commercial aspects of personality rights,[10] as not being incompatible with the nature of the right to privacy.

Problems Related to the Right to Informational Self-Determination

Issues of principle

On the data protection side, the first issue to be examined is whether the provision of personal data for consideration is compatible with the principles of lawful and fair data processing. Indeed, it is questionable whether a fundamental right can be the subject of any commercial agreement. According to the legal literature, the commercial potential of personal data arises in three areas, namely direct marketing, profiling, and the transfer of personal data to third parties for use by the data controller and for adjusting them to its own marketing.[11]

The EDPB's guidelines explicitly oppose the possibility of selling fundamental rights, since the protection of personal data is a fundamental right guaranteed by Article 8 of the Charter of Fundamental Rights,[12] and while data subjects may consent to the processing of such data, it is possible to interpret the existing law such that they may not be allowed to sell them.[13] This interpretation was implicitly con-

[10] In civil law jurisdictions, personality rights protect the individual's personal interets against various types of infringements, such as bodily integrity, likeness, any action relating to defamation or libel. Most civil law systems provide a general protection of the personality, in which general subsections, various personality rights can be distinguished. It has long been thought that such rights only protect ideal, non-pecuniary interests. Nowadays monetary, commercial aspects of personality rights are also recognized in some countries like Germany, Austria or Hungary.

[11] F. Banterle, *The Interface Between Data Protection and IP Law: The Case of Trade Secrets and the Database Sui Generis Right in Marketing Operations, and the Ownership of Raw Data in Big Data Analysis*, in: M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?*, Springer, Berlin 2018, p. 413.

[12] Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391.

[13] EDPB, *Guidelines 2/2019…*, para. 54.

firmed by the EDPB,[14] but it may be argued that this approach is in contradiction with the Digital Directive.[15] The Directive does not reject the fundamental rights approach with respect to the protection of personal data, but does not perceive it as a conceptual barrier to the use of personal data for remuneration, and instead merely stresses the importance of introducing safeguards in this regard.

In the context of the legal basis for data processing, which is an important aspect of the data protection analysis, it should be pointed out that personal data can, in principle, be processed as contractual consideration on two legal bases: firstly, on the basis of the consent of the data subject; and secondly, based on a contract concluded with the data subject. These two legal bases are briefly described below.

Data processing based on the consent of the data subject

By its very nature, the right of informational self-determination should – pursuant to European legal doctrine[16] and the GDPR – always give the natural person concerned the right to determine who collects and uses his or her personal data and for what purposes. In our view, consent is also one of the most common legal bases for data processing in the field of cultural heritage protection, both for receiving museum newsletters and for registering for the purchase of tickets for exhibitions and performances online, although the provision of billing data and bank account numbers may also be provided on a contractual basis when purchasing tickets.

Article 7(4) GDPR seeks to ensure that consent is neither concealed in the provision of a contract for a service, nor linked to the provision of a contract for a service for which such personal data are not necessary. According to the Article 29 of the Working Party on Data Protection (hereinafter referred to as WP29), which is considered to be the predecessor of the EDPB, the GDPR thus ensures that the processing of personal data for which consent is sought does not directly or indirectly become consideration for the contract. The purpose of Article 7(4) GDPR is to guarantee that processing based on consent and processing based on a contract cannot be combined or merged.[17] The reason for this is that, as mentioned above, lawful consent is based on the condition of voluntariness, whereas in the case of the contractual legal basis, the processing is not essentially based on the free choice of the data subject, but on the necessity that without the data processing the contract would be impossible to perform.

Pursuant to the EDPB's guidelines, turning personal data into contractual consideration should generally be avoided, because the essential element of consent is

[14] EDPB, *Guidelines 05/2020 on Consent under Regulation 2016/679*, 4 May 2020, para. 26.

[15] Directive (EU) 2019/770, recital (24).

[16] Federal Constitutional Court (Germany), Judgment of 15 December 1983, 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83 = BVerfGE 65, 1.

[17] Article 29 Working Party, *Guidelines on Consent under Regulation 2016/679*, 10 April 2018, WP259 rev.01, section 3.1.2.

voluntariness.[18] In the absence of the latter, i.e. where the data subject does not have a real choice as to whether to provide the data, or where (s)he would suffer some disadvantage if (s)he does not provide the data, there is no valid consent. According to the EDPB, the compulsion to consent to the use of more personal data than strictly necessary limits the data subject's choices and prevents voluntary consent.[19]

However, the above may be disputed to the extent that a data subject who does not wish to provide his or her data as consideration does not necessarily have to fear a refusal to enter into a contract as a disadvantage, if the personal data are provided as an alternative consideration for entering into a contract. Thus, for example, the requirement of voluntary consent is not necessarily breached if the data controller gives the data subject the choice of providing the contractual consideration in cash, or by providing his or her personal data for a specific purpose. This possibility has been recognized by the EDPB itself, albeit with a slightly different logic: according to the EDPB, the data subject's consent is lawful where the data subject has the choice between services from the data controller that allow for the processing of personal data, and services that do not require consent – provided that these two services are equivalent.[20] For example, it may be acceptable for a data subject to be able to use all the features of a piece of software without consent, but with consent, for example, to have access to more and/or more detailed content in an environment with more sophisticated graphics.

A similar finding was made by the French Data Protection Authority (CNIL) in its decision against Google Inc. On 31 December 2021, the CNIL imposed a total fine of €150 million on Google for failing to make it easy for users of google.fr and youtube.com to refuse to accept cookies that were mandatory for the use of the sites. However, a more significant change for the digital services market is the fact that the CNIL, referring to a decision of the French Council of State, has also considered the use of cookie walls and paywalls by service providers to be acceptable in principle, provided that they offer adequate guarantees for the protection of users' personal data when applying these solutions.[21]

In the case of cookie walls, the service provider makes access to the services provided on its website subject to the mandatory acceptance by users of certain cookies that would otherwise only be used with consent. Notwithstanding the mandatory acceptance, the CNIL considers that the lawfulness of consent can be ensured if service providers offer data subjects an appropriate choice if they wish to refuse cookies. Such an option could be a paywall, whereby users could be entitled to use services for a fixed fee even if they do not accept the cookies on the cookie wall. However, this financial consideration should not be such as to deprive

18 EDPB, *Guidelines 05/2020…*, paras. 26-27.

19 Ibidem, para. 13.

20 Ibidem, para. 37.

21 Council of State (France), Decision no. 434684, 19 June 2020.

internet users of real choice. In other words, the price or compensation must be "fair", which is assessed on a casebycase basis.[22]

In the light of the CNIL decision, European data protection practice has therefore taken a small step away from the EDPB's position and towards the recognition of personal data as consideration.

The problem however is that the right to self-determination cannot be fully implemented in the current digital environment, because the regulation of consent and data subjects' rights gives only the appearance of self-determination.[23] For example, when the data subject notifies the data controller of the withdrawal of consent, the latter may not always reach the whole chain of data processors.[24] Noto La Diega points out that the data subject is often unaware of how many date processors process his or her personal data. In his empirical study, he found that in 2 hours of browsing he visited 32 websites and his computer communicated with 229 third-party websites.[25]

Hence, under a legal basis based on consent, data subjects may not be fully informed of the conditions of data processing, including the fact that they are entitled to receive compensation for the processing of their data by a data controller. This difficulty can, nevertheless, in our view be adequately addressed by making the legal instruments already provided by the GDPR – in particular the right to be informed under Article 14 and the right to be forgotten – more effective.

Data processing based on the performance of a contract

According to the WP29, the term "necessary for the performance of a contract" should be interpreted strictly. The processing must be necessary for the performance of the contract regarding each individual data subject.[26] This could include, for example, processing the address of the data subject for the delivery of goods purchased over the Internet, or processing credit card details to facilitate payment. In the context of employment, this legal ground may allow, for instance, the processing of information on wages and bank account details to enable wages to be paid. There must be a direct and objective link between the processing of data and

[22] Ibidem.

[23] H. Ursic, *The Failure of Control Rights in the Big Data Era: Does a Holistic Approach Offer a Solution?* in: M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?* Springer, Berlin 2018, p. 57.

[24] A. Sattler, *From Personality to Property?* in: M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?* Springer, Berlin 2018, p. 44.

[25] G. Noto La Diega, *Data as Digital Assets: The Case of Targeted Advertising*, in: M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?* Springer, Berlin 2018, p. 448.

[26] Article 29 Working Party, *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/ECWP217*, 9 April 2014, WP217, section III.2.2.i); Article 29 Working Party, *Guidelines…*, section 3.1.2.

the purpose of the performance of the contract. Consequently, personal data cannot be processed as consideration on a contractual basis either, since it can be replaced by a monetary consideration and is therefore not absolutely necessary for the performance of the contract.

At the same time the Digital Directive recognizes the right of Member States to freely determine their requirements for the formation, existence, and validity of a contract.[27] This approach is also in line with the fact that the rule according to which the regulation of the processing of personal data in the context of information society services offered directly to children is without prejudice to the general contract law of Member States,[28] which leads to the more general conclusion that the GDPR essentially does not intend to affect classic civil law issues.

Thus, contrary to the WP29's interpretation we can also get to the principle of freedom of contract through private law rules, which clearly does not prohibit the conclusion of a contract where the individual "pays" by providing his or her data. In fact, according to the legal literature, the data subject can explicitly regain his or her self-determination if the pecuniary value of personality rights is recognized, since by authorizing the use of his or her data the data subject can also obtain the consideration for the commercial exploitation thereof.[29]

In our view however, problems may arise from the fact that more and more personal data will be created in the future which will not be managed by the data subject, and of which (s)he will not be aware.[30] We are of the opinion that this would make it extremely difficult to deal with the issue on a purely private law, contractual basis. Indeed, in an online environment, it is difficult to envisage such contractual arrangements and licence fees between the data controller and each individual data subject, since most controllers do not obtain the data of the persons concerned directly from the data subjects, but rather from other controllers.

Conclusions on data protection

Overall therefore, there may be practical objections to the applicability of both of the two legal bases examined above in the context of data processing. However, the theoretical obstacle is whether the level of protection of personal data is equivalent to that of the protection of fundamental rights. As Sattler has pointed out, the introduction of public law rules into private law relationships may significantly prevent firms from developing innovative solutions.[31] Accordingly, in our view it is not necessary to emphasize the level of protection of fundamental rights for private data control-

27 Directive (EU) 2019/770, recital (24).

28 GDPR, Art. 8(4).

29 See A. Sattler, op. cit., p. 48.

30 See H. Ursic, op. cit., p. 67.

31 See A. Sattler, op. cit., pp. 47-48.

lers, given that the fundamental rights approach to the protection of personal data was originally and solely intended to protect the individual against the state, while such a level of protection is not necessary in the case of private data controllers.

Practical problems can be more easily addressed on the legal basis of consent, and this legal basis may also be more in line with the principle of informational self-determination since, unlike in the case of contracting, data processing on the basis of consent does not require that the data subject and the data controller enter into a direct legal relationship, and consent can be validly given without such a relationship. This is also confirmed by the already mentioned recital (24) of the Digital Directive, which repeatedly mentions consent as the legal basis for the provision of personal data as contractual consideration.

Developments and Realities in Competition and Consumer Protection Law

In recent years, more and more European businesses have turned (fully or partially) to online contracting solutions.

A business that knows its consumers and their consumer behaviour and consumption patterns can use this knowledge to manipulate them effectively, and thus can gain a competitive advantage.[32] Consequently, data has become a commodity in the digital marketplace.[33] As Andrew Keen rightly points out, we all work for Facebook and Google, completely free of charge, producing the personal data that makes these companies so valuable, and in return we get free use of their services.[34] In the digital economy, the data controllers of personal data are primarily the giant companies that attract and capture the attention of consumers with their services and sell that attention to other companies, in particular advertisers.

In 2017, the European Commission underlined in its inquiry into the e-commerce sector that the collection, processing, and use of big data is becoming increasingly important in e-commerce, and the analysis of big data may result in better products and services, which can bring significant benefits and make businesses more efficient. On the other hand, the increased importance of data may give rise to competition concerns as well.[35]

In the EU, online platforms are the main instruments to support digital commerce. Today, more than a million EU businesses trade on online platforms, the key enablers of digital commerce, to reach their customers. It is estimated that around

[32] S. Baker, *Numerátorok*, transl. by R. Komáromy, Geopen, Budapest 2009, p. 57 (original title: *The Numerati*).

[33] G. Schneider, *European Intellectual Property and Data Protection in the Digital-Algorithmic Economy: A Role Reversal(?)*, "Journal of Intellectual Property Law & Practice" 2018, Vol. 13(3), p. 231.

[34] A. Tari, *#yz Generációk online* [#yz Generations Online], Tericum, Budapest 2015, p. 30.

[35] European Commission, *Report from the Commission to the Council and the European Parliament: Final report on the E-commerce Sector Inquiry*, 10 May 2017, COM(2017) 229 final, sections (54)-(56).

60% of the total digital economy-related purchases of goods and services for residential consumption, and 30% for public consumption, are made through online intermediaries.[36] Online platforms have become unavoidable for a large number of businesses.[37] In addition, the increased use of online platforms for transaction intermediation, coupled with the strong indirect network effects that feed on the data-driven advantages of online platforms, is leading to a growing dependence of businesses on online platforms as their "gateway" to the market and consumers.[38] This problem is exacerbated by the growing importance of online platforms in mediating transactions between consumers and businesses: businesses are increasingly dependent on online platforms; and strong data-driven network effects, combined with a significant fear factor, are upsetting the balance between the bargaining power of traders and platforms.[39]

The 2015 draft of the Digital Directive also stressed that in the digital economy, market players increasingly see information about individuals as having a value comparable to money. According to the draft, it is common for digital content to be provided not for a price, but for a consideration other than money, such as access to personal data or other data.[40] Unfortunately, the relevant recitals are not included in the final version of the Digital Directive. In the pre-draft consultation, the vast majority of consumers, Member States, and the legal professions argued that not only digital content supplied for a price, but also digital content supplied in exchange for consumers' data (personal and other) should be addressed, while businesses were more divided on this issue.[41]

In 2018, the European Parliament proposed an amendment to the Directive that would allow the contractual relationship between online intermediary service providers and consumers to be deemed to exist even in cases where services are provided to consumers in exchange for the provision of personal or other data.[42]

---

36 European Commission, *Proposal for a Regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services*, 26 April 2018, COM(2018) 238 final, p. 1.

37 European Commission, *Questions and Answers – EU Negotiators Agree to Set Up New European Rules to Improve Fairness of Online Platforms' Trading Practices*, 14 February 2019, https://ec.europa.eu/commission/presscorner/detail/en/MEMO_19_1169 [accessed: 14.07.2023].

38 European Commission, *Proposal for a Regulation…*, COM(2018) 238 final, p. 1.

39 European Commission, *Commission Staff Working Document, Executive Summary of the Impact Assessment accompanying the document: Proposal for a Regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services*, 26 April 2018, SWD(2018) 139 final, p. 1.

40 European Commission, *Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content*, 9 December 2015, COM(2015) 634 final, recital (13).

41 Ibidem, recital (13)-(14), Art. 3(1).

42 European Parliament, *Opinion of the Committee on Industry, Research and Energy for the Committee on the Internal Market and Consumer Protection on the proposal for a regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services (COM(2018)0238 - C8-0165/2018 - 2018/0112(COD))*, 23 November 2018, ITRE_AD(2018)627047, recital (8).

This proposal has not been included in the regulation.[43] In our view, the manifestation of the proposal is in line with the trend in the digital economy whereby businesses often offer "free" services for which consumers "pay" with their data, or in some cases the essence of the whole business model is that the business processes data through the use of its services by consumers and exploits them with algorithms for different purposes, i.e. "makes them marketable". Consumers therefore often use the services of businesses in exchange for valuable consideration (their data), in return for what appear to be free services.

The value and the *quid pro quo* character of personal data require a rethinking of several civil law institutions. According to Ursic, an amendment to the GDPR from a consumer protection perspective may be necessary in the light of data subjects' rights and the economic interests associated with big data.[44]

At the same time, even within the framework of the current consumer protection legislation,[45] the acceptance of personal data as a value has already appeared in the judicial practices of the Member States,[46] and although the European Court of Justice has not yet interpreted[47] the price concept of the Unfair Commercial Practices Directive (UCP Directive),[48] the Curia of Hungary held that even if the UCP Directive's price concept included an authorization to use personal data, it was not able to influence the transactional decision, and in particular could be misleading on the basis of the evidence in the specific case at hand.[49] Thus, although the Curia of Hungary did not thereby recognize the *quid pro quo* nature of personal data in the specific case, in our view it left open the possibility for the administrative bodies responsible for consumer protection to assess the disadvantages resulting from the use of personal data as a *quid pro quo*, provided that there is sufficient evidence to do so.[50]

43 Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, OJ L 186, 11.07.2019, p. 57.

44 See H. Ursic, op. cit., p. 78.

45 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'), OJ L 149, 11.06.2005, p. 22, Art. 6(1)(d); *2008. évi XLVII. törvény a fogyasztókkal szembeni tisztességtelen kereskedelmi gyakorlat tilalmáról* [Act XLVII of 2008 on the Prohibition of Unfair Business-to-Consumer Commercial Practices], Magyar Közlöny 2008/95, section 6(1)(c).

46 Curia of Hungary, Judgment of 6 October 2021, Kfv.II.37.243/2021/11.

47 Ibidem, para. 73.

48 Directive 2005/29/EC, Art. 6(1)(d).

49 The Curia of Hungary interpreted the rules that were in force prior to the transposition of the Omnibus Directive (Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, OJ L 328, 18.12.2019, p. 7).

50 Curia of Hungary, Judgment of 6 October 2021, Kfv.II.37.243/2021/11, para. 71.

Private Law Options for the Recognition of Pecuniary Interests in Personal Data

Data as an intellectual property right

By its very nature, data can constitute a right similar to intellectual property rights, as it is also characterized by ubiquity: unlike physical objects and things, data is independent of time and space; the same data can be in several places at the same time and can be legally handled by several persons. This is particularly true for digital and online data, as opposed to analogue personal data,[51] as digital technologies allow for the large-scale collection and analysis of data, with the associated economic potential to be exploited. For this reason, some argue that digital data should, under the law, be the subject of exclusive rights.[52]

To examine this issue, we first look at how data is protected by intellectual property rights, and then we present the views that seek to ensure an increased protection for data in general, and for personal and non-personal data, in the form of a separate (*sui generis*) intellectual property right.

The current system of protection

Data *per se* is not protected by intellectual property (IP) law, as only IP rights that are explicitly mentioned by law are protected (*numerus clausus*).[53]

The TRIPS Agreement protects undisclosed information from being acquired, used, or disclosed without the rightholder's consent if it is secret, has commercial value, and reasonable steps have been taken to keep it secret.[54] Accordingly, trade secrets are protected by an EU directive,[55] which requires Member States to protect the confidentiality of the data, rather than the data itself. Personal data can also be the subject of a trade secret, such as the contact details of customers or information about their behaviour.[56]

Under the TRIPS Agreement, compilations of data that constitute an intellectual creation by virtue of the selection or arrangement of their contents are protect-

[51] L. Chrobak, *Proprietary Rights in Digital Data? Normative Perspectives and Principles of Civil Law*, in: M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?*, Springer, Berlin 2018, pp. 255-256.

[52] A. Wiebe, *Protection of Industrial Data: A New Property Right for the Digital Economy?* "Journal of Intellectual Property Law & Practice" 2017, Vol. 12(1), p. 67.

[53] See L. Chrobak, op. cit., pp. 266-267.

[54] Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), 15 April 1994, 1869 UNTS 299, Art. 39(2).

[55] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, OJ L 157, 15.06.2016, p. 1.

[56] See F. Banterle, op. cit., p. 418.

ed, but this protection does not extend to the data itself.[57] Individual databases of an original nature are considered to be works of authorship and their authors are entitled to copyright. However, databases rarely satisfy the requirement of originality.[58] Moreover, in the EU, the producer of the database enjoys *sui generis* protection.[59]

Sui generis intellectual property right

Both the legal literature and economic actors, such as German car manufacturers, have raised the possibility that the law should provide for exclusive rights over data, especially over non-personal data.[60] According to Sattler, there are already several indications that the right to personal data is not exclusively a personality right, inasmuch as the significant pecuniary value,[61] the possibility of compensation, and the portability of the data all point to an emerging property right, but at the same time he also recognizes that the personality right nature of personal data is further strengthened by the right to be forgotten.[62] Richter also raises the possibility of creating a new copyright-related right.[63] Another part of the legal literature disagrees with the treatment of data as IP rights.[64]

Lessig also raises the possibility of protecting the ownership of data.[65] However, only an IP protection can be relevant, since data is ubiquitous, independent of time and space, can be present in multiple places at the same time, in analogue or digital form, and therefore its protection is more akin to that of a patent or copyright. While property rights provide for the indefinite allocation of the physical world in the context of the most complete disposal of things, rights related to things and other analogue objects of rights (e.g. electricity), IP is for a limited period of time, and the protection of the interests of the individual and the community is primarily based on temporality.[66] After a fixed period of time, the right ceases to ex-

[57] TRIPS Agreement, Art. 10(2).

[58] C. Sappa, *How Data Protection Fits with the Algorithmic Society via Two Intellectual Property Rights – A Comparative Analysis*, "Journal of Intellectual Property Law & Practice" 2019, Vol. 14(5), pp. 407-418.

[59] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77, 27.03.1996, p. 20.

[60] W. Kerber, *A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis*, "GRUR International" 2016, Vol. 11, pp. 989-998.

[61] G. Malgieri, *"User-Provided Personal Content" in the EU: Digital Currency Between Data Protection and Intellectual Property*, "International Review of Law, Computers & Technology" 2018, Vol. 32(1), pp. 118-140.

[62] See A. Sattler, op. cit., pp. 42-43.

[63] H. Richter, *The Power Paradigm in Private Law*, in: M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?*, Springer, Berlin 2018, p. 554.

[64] T. Fia, *Resisting IP Overexpansion: The Case of Trade Secret Protection of Non-Personal Data*, "International Review of Intellectual Property and Competition Law" 2022, Vol. 53, p. 943.

[65] L. Lessig, *Code and Other Laws of Cyberspace*, Basic Books, New York 1999.

[66] A. Acquisti, C.R. Taylor, L. Wagman, *The Economics of Privacy*, "Journal of Economic Literature" 2016, Vol. 54(2), p. 447.

ist, the intellectual creation becomes a part of the public domain, and the monopoly granted by the right is terminated. As Kohler points out, the right to dispose of IP can only be justified for as long as it is in the interest of the individual, after which it must be in the public interest; the determination of this period varies from country to country and from one form of protection to another, and is a matter of legal policy.[67] A period of protection for data is also conceivable, but it should be relatively short, because the value of data lies in its timeliness, which changes quickly over time. However, the problem is that pecuniary value is linked only to specific data processing purposes, whereas the same data can be lawfully used for various purposes. It cannot be excluded that several data controllers use similar data sets or personality profiles for the same purpose.

In the case of a patent, the registered rightholder can exploit the invention, the author can sell the work after its creation, and in the case of a trade name, the right can be proved by use. While in the case of IP rights the moment of creation is easy to establish and prove, personal data are created and change continuously with the behaviour and conduct of the person(s) concerned, and in this respect they are similar to personality rights, which is not a coincidence because they are part of private life. The fact that their value is linked to the purpose of the data processing does not change this, since the data subject's right to self-determination would be violated if another data controller could not use his or her data for the same purpose. According to Chrobak, an exclusive right over personal data also threatens the free flow of information and the freedom of the Internet.[68] For this reason, in our view the IP-based protection is alien to the nature of personal data.

Some argue that protecting data as a separate IP right can contribute to transparency in the contractual terms set by data controllers[69] and can ultimately strengthen the protection of privacy rights.[70] Others argue that overprotection not only reduces the public domain, but also distorts competition.[71] When granting exclusive rights, it should always be taken into account that this will prevent the data from being used by others. According to Sappa, the current system of protection, based on trade secrets and a *sui generis* database protection, leads to a situation where large companies control the flow of information, preventing its further use and social progress.[72] The legal literature on IP protection does not provide sufficient insight into the content of an exclusive IP right protecting personal data, how such a right fits into the IP regime, and what regulatory anomalies it hides.

67 J. Kohler, *Das Autorrecht*, Fischer, Jena 1880, pp. 47-50.

68 See L. Chrobak, op. cit., p. 269.

69 See A. Sattler, op. cit., p. 42.

70 See H. Ursic, op. cit., p. 77.

71 H. Ullrich, *Expansionist Intellectual Property Protection and Reductionist Competition Rules: A TRIPS Perspective*, "Journal of International Economic Law" 2004, Vol. 7, p. 410.

72 See C. Sappa, op. cit., p. 414.

Therefore we believe that there are other ways to justify the *quid pro quo* nature of personal data. Such an exclusive right would shift the focus away from self-determination towards data ownership, and would also leave open the relationship between the protection of personal data and privacy.

The EU has not moved towards the exclusive right approach, but is rather pushing for data sharing. This position should be supported, since granting an exclusive right would not solve, in and of itself, the problems that arise in the provision of online services and in other sectors, and data subjects would remain vulnerable insofar as regards the use of their personal data.

The European trends with respect to the pecuniary value of personality rights

Personality rights as property rights

In addition to data protection rules, the protection of personal data in private law is ensured by personality rights. Personality rights are not transferable or alienable. According to Kohler, this is the fundamental difference between personality rights and IP rights,[73] which is why in *civil law* jurisdictions personality rights, including personal data, cannot be the subject of a contract or its consideration. In US law, the right to the commercial use of personality rights is considered a property right, known as the *right to publicity*.

However, recognition of the property value of certain aspects of personality has also started in Europe. In 1999, the German Federal Court of Justice (BGH) recognized that certain personality rights, such as the right to a name or the right to one's own image, have a property value, the commercial use of which is at the discretion of the rightholder.[74] According to the BGH, these property aspects of a general right of personality are heritable[75] and are protected for a period of 10 years after death, after which they become part of the public domain.[76] Following this pattern, the Austrian Supreme Court also recognized the property value of certain personality rights in the year 2010, indicating that names and images have a pecuniary value that can be measured in money.[77]

In the field of cultural heritage, the question is, to what extent can personality aspects of well-known personalities, such as Johann Sebastian Bach[78] or

[73] See J. Kohler, op. cit., p. 74.

[74] NJW 2000, 2195.

[75] Federal Court of Justice (Germany), Judgment of 1 December 1999, NJW 2000, 2195; NJW 2000, 2201; H.-P. Götting, *Die Vererblichkeit der vermögenswerten Bestandteile des Persönlichkeitsrechts – ein Meilenstein in der Rechtsprechung des BGH*, "Neue Juristische Wochenschrift" 2001, p. 585.

[76] Federal Court of Justice (Germany), Judgment of 5 October 2006, BGHZ 169, 193.

[77] Supreme Court (Austria), Judgment of 21 June 2010, SZ 2010/70.

[78] Higher Regional Court of Dresden (Germany), Judgment of 4 April 2000, NJW 2001, 615.

Mona Lisa,[79] be monetized by private persons other than museums and cultural institutes. This question also affects trademark law, starting from simple merchandise products to goods and services not related to the work and life of the famous person in question.

In both German and Austrian law, personality rights are characterized by the unity of personal and property relations, similar to copyright law, which is a significant difference compared to other European legal systems. According to Sattler, the protection of personal data must also be characterized by the inseparable unity of personal and property relations, similarly to copyright law, and as such it is regulated by the German system of the protection of personality.[80] The analogy with copyright would also provide an answer to the prohibition of the transfer of personality rights, since the only relevant form of exploitation would be a licence for their use, although European countries have no uniform regulation in this regard.

Property law consequences

In addition to German and Austrian law, the jurisprudence of several European countries (e.g. France,[81] Poland,[82] Spain[83]) recognize a set of legal consequences based on damages and/or unjust enrichment – typically originating from an analogy with licensing – for the use of personality rights for advertising purposes. The Hungarian legislator, influenced by German case law,[84] has made it possible for the person concerned to request the court to grant him/her the pecuniary advantage obtained by the infringement of his/her personality right in the case of the commercial use thereof,[85] which the heirs are entitled to claim after the death of the person concerned.[86] On this basis, the infringer must pay the remuneration that the rightholder would have received if the infringer had requested authorization to exploit the personality right.

The problem of the unjust enrichment of data controllers is also raised in the data protection literature.[87] Nonetheless, the GDPR currently only allows for compensation which presupposes the fault of the infringer. Judicial practice tends to

79 Federal Patent Court (Germany), Judgment of 25 November 1997, GRUR 1998, 1021.

80 See A. Sattler, op. cit., p. 46.

81 A. Trebes, § 59 Frankreich, in: H.-P. Götting, C. Schertz, W. Seitz (eds.), *Handbuch des Persönlichkeitsrechts*, C.H. Beck, Munich 2019, Rn. 77.

82 Court of Appeal in Kraków (Poland), Judgment of 7 February 1995, I ACr 697/94.

83 Constitutional Court (Spain), Judgment of 26 March 2001, STC 81/2001.

84 L. Vékás, *Über die Expertenvorlage eines neuen Zivilgesetzbuches für Ungarn*, "Zeitschrift für Europäisches Privatrecht" 2009, p. 551.

85 *2013. évi V. törvény a Polgári Törvénykönyvről* [Act No. V of 2013 on the Civil Code], Magyar Közlöny 2013/185, section 2:51(1)(e).

86 Ibidem, section 2:50(2).

87 See L. Trakman et al., op. cit., p. 949.

interpret the conditions for compensation narrowly, as the mere feeling of frustration from the infringement does not justify compensation.[88] In addition, proving the damage is no simple task, which is why the German courts' jurisprudence on personality rights has moved towards the concept of enrichment without an objective legal basis.[89] Enrichment can also be equal to a proportion of the infringer's income, as in patent or trademark law.[90]

The fundamental rights background of the pecuniary value of personality rights

According to the Spanish Constitutional Court, the property right to one's own image is not part of the fundamental rights protection based on the protection of human dignity, which protects moral interests.[91] However, according to the German Federal Constitutional Court (BVerfG), the private law recognition of the pecuniary value of personality rights is not contrary to the provisions of constitutional law, although it is not part of the fundamental law-based general right to personality.[92] In a decision of the European Court of Human Rights,[93] which referred to the above position of the BVerfG, it was argued that an infringement of the property aspects of personality rights may result in a violation of the right to property. The applicant argued that the infringement had only concerned pecuniary components of their personality rights and thus, the court should have analysed the relation of the alleged infringer's right to freedom of speech and the right to property of the rightholder. The Court, however, left the question unanswered.

Based on the above approaches, the commercialization of personality rights in private law is not prohibited from a fundamental rights perspective, which in our view could also be extended to personal data using the same logic. In this framework, the private law could protect pecuniary aspects of the personality that are not subject to the protection of human rights of traditional personality aspects, such as private life or human dignity. In the field of cultural heritage, an additional human right – the right to artistic expression – may be involved, which must be examined separately from the above problem, just as aspects of freedom of expression would be.

88 Case C-300/21, *UI v Österreichische Post AG*, Opinion of Advocate General Campos Sánchez-Bordona, 6 October 2022, ECLI:EU:C:2022:756, para. 114.

89 Federal Court of Justice (Germany), Judgment of 14 February 1958, BGHZ 26, 349; Federal Court of Justice (Germany), Judgment of 26 October 2006, NJW 2007, 689.

90 High Court of Kecskemét (Hungary), Decision no. 8.P.20.334/2017/17.

91 Constitutional Court (Spain), Judgment of 26 March 2001, STC 81/2001.

92 Federal Constitutional Court (Germany), Judgment of 22 August 2006, NJW 2006, 3409; Federal Court of Justice (Germany), Judgment of 26 October 2006, NJW 2007, 689.

93 ECHR, *Ernst August von Hannover v Germany*, Application no. 53649/09, Judgment of 19 February 2015.

The specificities of the pecuniary value of personal data

In our view, certain personality rights may have pecuniary value because they are capable of materialization, i.e. they may become physically perceptible to third parties, which allows them to acquire a new function other than their original one (e.g. a function of indication for goods, enhancement of their attractiveness, etc.), and thus to become separated, to a certain extent, from the person concerned, i.e. to become materialized. Some personality rights, such as honour and personal liberty, cannot be materialized, while the protection of the physical integrity of the human body relates to a physical body already in existence, which is, by its very nature, perceptible to third parties.[94] Accordingly, in our view the concept of pecuniary value does not permeate the entirety of the data protection regime, but rather it can be linked only to specific data processing purposes, since the use of personal data continues to fall exclusively within the personality rights of the person concerned.

The pecuniary value of personal data differs in several respects from the commercial use of other personality rights. The pecuniary value of personality rights may be linked to specific behaviours (e.g. use on street posters), whereas in the case of personal data it may be linked to specific data processing purposes.

Personal data, like other personality rights, may be materialized and become perceptible to third parties, but their function – unlike in the case of a name or a voice recording – does not change if they are used for commercial purposes, since the function of personal data is always to identify or to be able to identify the data subject. Consequently, personal data cannot be fully materialized and separated from the data subject. Nor can the commercial traffic link the personal data to another person, which is a prerequisite of the right of disposal in the case of the public use of names and images, because only authorized persons can access them, not third parties. While in the case of a street poster with a person's face on it, third parties may think that the rightholder has sold the rights to use his/her image to the advertising company, the use of personal data is typically on a large scale and not in a public place, so that a similar association of images does not seem relevant.

In the case of a breach of personal data of pecuniary value, the transfer of the pecuniary advantage obtained by the breach may also be interpreted as a private law sanction, which may be calculated on the basis of an analogy with licensing, since the breach may result from the lack of a contract between the data controller and the data subject in that case as well. However, the fictitious licence fee has to be typically determined under a different methodology than in the case of the use of names and images for advertising and marketing purposes. In the case of other personality rights, the amount of the fee to be paid can be determined more easily from the factual background (e.g. the publication of a wedding photo on the

[94] M. Schultz, *A személyiségi jogok vagyoni értéke és tárgyiasulása* [Commercial Value and Manifestation of Personality Rights], ORAC, Budapest 2022, p. 156.

front page of a national daily newspaper[95] or the use of a facial image for a certain period of time, in a certain territory and in a certain number of copies for advertising a service).[96]

The Dangers of the Denial of the Concept of Personal Data as Consideration for a Uniform Application of European Data Protection Law

As we have shown in the previous sections, the arguments in favour of the processing of personal data for remuneration are so strong and numerous – both in terms of the actual facts and the legislative changes – that it is difficult to justify upholding the conclusions of the EDPB's guidelines to the contrary, which could also deal a serious blow to the uniform application of the European data protection legislation as a whole.

For many decades, the guidelines of the EDPB and of its predecessor, the WP29, have been the main legal instruments in the European regulatory space that have essentially determined the uniform application of data protection rules. The legal practitioners' reference to them as binding rules is generally accepted by the national courts of the Member States, which is due to the EDPB's high professional reputation, which stems from the fact that the Board is predominantly composed of the representatives of the national authorities, and thus it represents not only the opinion of an institution of the Union *per se*, but the consensus of the Member States as well. This can be clearly seen from the fact that the acceptance of the guidelines is irrespective of whether they are issued by an advisory body (WP29) or by a collegial body (Board, juridical body) established by the GDPR. In practice, there is no difference between the binding force of the positions they adopt, although their legal status is different.

Their binding force is not of a legal origin, but based on authority. This lack of a legal origin is the case for at least two reasons: the EDPB is an EU agency created not by primary law, but by the EU institutions, so it is not entitled either to create binding law or to exercise wide discretionary powers. On the other hand, the guidelines issued by the EDPB – the content of which is disputed in the present study – are not even non-binding acts of EU law under Article 288 TFEU,[97] but fall within the scope of the subordinate category of soft law, which does not constitute a legal act and which may be set aside by a national court as a result of, or even without, a preliminary ruling procedure, as is described below.

[95] *Douglas v Hello! Ltd.* [2005] EWCA Civ 595.

[96] Federal Court of Justice (Germany), Judgment of 18 March 1959, NJW 1959, 1269.

[97] Consolidated version of the Treaty on the Functioning of the European Union, OJ C 115, 9.05.2008, p. 47.

The EDPB is also part of the process of the mushrooming of agencies or "agencifiction",[98] whereby a "second-tier" EU institutional system is created by secondary law outside the EU's primary law,[99] a process that is as haphazard[100] as the designation of documents of a legal nature not falling within the scope of Article 288 TFEU. The fundamental question is under what conditions and to what extent the European Commission or other EU institutions can delegate their own tasks to one type of them, namely to the so-called "regulatory agencies". In the context of a preliminary ruling procedure, national courts – if they wish to establish the *quid pro quo* nature of personal data – may question the extent of the delegation of powers under the *Meroni* doctrine,[101] while they may question the basis on which the EDPB adopts normative acts (opinions, guidelines) under the *Romano* judgment.[102] The foregoing may be questioned even in circumstances where the possibility of discretionary powers in the case of an agency has been recognized by the European Court of First Instance (currently named the General Court),[103] and in the *ESMA* case[104] the European Court of Justice (ECJ) has eased the conditions for delegations of powers to public entities in comparison to the *Meroni* doctrine, and in addition it did not rule out this possibility in the specific case by referring to the institutional framework established by Articles 263 and 277 TFEU, essentially by invoking the possibility of ordinary judicial review by the ECJ.

In the context of the judicial review of the EDPB's "guidelines", we refer to Advocate General Bobek's opinion, according to which the correct approach would be that if something is called a "guideline", it should be considered as not having any binding legal effect and that anyone has the right to completely ignore it.[105] However, the ECJ has maintained its previous approach – that in each individual case

[98] K. Verhoest, S. van Thiel, S.F. De Vadder, *Agencification in Public Administration*, in: *Oxford Research Encyclopedia of Politics*, Oxford University Press, Oxford 2021, doi.org/10.1093/acrefore/9780190228637.013.1466.

[99] Commission of the European Communities, *Communication from the Commission to the European Parliament and the Council: European agencies – The way forward*, 11 March 2008, COM(2008) 135 final, p. 2.

[100] H.C.H. Hofmann, *Agency Design in the European Union*, "Windsor Yearbook of Access to Justice" 2010, p. 309.

[101] Case C-9/56, *Meroni & Co., Industrie Metallurgiche, SpA v High Authority of the European Coal and Steel Community*, Judgment of 13 June 1958, ECLI:EU:C:1958:7.

[102] Case C-98/80, *Giuseppe Romano v Institut national d'assurance maladie-invalidité*, Judgment of 14 May 1981, ECR-01241.

[103] Case T-187/06, *Ralf Schräder v Community Plant Variety Office (CPVO)*, Judgment of 19 November 2008, ECR II-03151.

[104] Case C-270/12, *United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union*, Judgment of 22 January 2014, ECLI:EU:C:2014:18.

[105] Case C-911/19, *Fédération bancaire française (FBF) v Autorité de contrôle prudentiel et de résolution (ACPR)*, Opinion of Advocate General Bobek, 15 April 2021, ECLI:EU:C:2021:294, paras. 90-95; Case C16/16 P, *Kingdom of Belgium v European Commission*, Opinion of Advocate General Bobek, 12 December 2017, ECLI:EU:C:2017:959, paras. 144-171.

and irrespective of the formal label of the act concerned, it must first be decided whether it is a "genuine" or "false" soft law measure – which can be decided by analysing its content. If something is formulated in mandatory terms, it may be subject to annulment, and it follows from the foregoing that as long as such a "guideline" is not annulled, it is "binding",[106] although it is also clear that such a guideline must be annulled, as being an invalid act by the ECJ if a preliminary ruling procedure is initiated by a national court.

Even if a guideline produces non-binding legal effects, its invalidity – for example, on the grounds of the issuer having exceeded its power – may be examined by the ECJ if a national court so requests in a reference for a preliminary ruling, even in a case not directly involving the parties concerned, provided that the reference is made in the context of a genuine legal dispute in which the issue concerning the validity of an EU act is raised at least in an ancillary manner.[107] Even in the case of non-invalid and non-binding guidelines, national courts have the possibility to derogate from them, provided that they offer sufficient justification.[108] We consider that sufficient arguments have been put forward in the present study for a national court's decision to depart from the guidelines.

An important point regarding the EDPB's guidelines is that the GDPR does not use the "utmost account" requirement at all in the application of the guidelines, which often makes the legal effect explicit, even if not automatically binding, for other regulatory agencies.[109] And neither the preamble (134) nor Article 94(2) GDPR explicitly establishes that the WP29 guidelines can be automatically maintained and can be referred to as the Board's position, i.e. qualifying as the Board's guideline.

Point [54] of the EDPB's guideline no. 2/2019, which is the main point of criticism in the present study, does not seem to be a substantive statement that would indicate that it is not a binding rule, even in the light of the overview of the guideline as a whole, and therefore it cannot be excluded that it might be annulled by the ECJ on the initiative of a national court. Even if it were perceived as non-binding by the national court and yet its validity was not called into question, a derogation could be sought on the basis of the arguments we have presented. Either scenario, if it were to occur in the legal practice, would constitute a major blow to the reputation of the EDPB and its guidelines, with potential spill-over effects for the whole of the uniform application of the European data protection rules.

106 A.Gy. Kovács, T. Tóth, A. Forgács, *The Legal Effects of European Soft Law and Their Recognition at National Administrative Courts*, "ELTE Law Journal" 2016, Vol. 2, p. 66.

107 C-911/19, paras. 36-37, 53-56 and 64; Case C322/88, *Salvatore Grimaldi v Fonds des maladies professionnelles*, Judgment of 13 December 1989, ECR-04407, para. 8; C16/16 P, para. 44.

108 C-911/19, para. 44; A.Gy. Kovács, T. Tóth, A. Forgács, *Effects of European Soft Law at National Administrative Courts*, "Loyola University Chicago International Law Review" 2016, Vol. 14(1), p. 120.

109 Kovács, T. Tóth, A. Forgács, *Effects*..., pp. 107-109.

Conclusions

Personal data are currently used as consideration for online content services and therefore they have a *de facto* pecuniary value. Insofar as regards cultural heritage, this can especially affect ticket sales, newsletters, marketing activities, and the commercial exploitation of paintings and likenesses.

Developments in competition law and consumer protection law have highlighted the economic potential and competitive advantage of collecting and commercializing consumer data. The recognition of personal data as contractual consideration could, thus, lead to online content providers or products related to the Internet of things (e.g. kitchen or other household appliances) raising the price of goods or services, as they would lose the personal data that they have so far obtained for free, and they would "cut back" on the price only in case of a consent given for the commercial use of personal data. Such market developments should be prevented at all costs, as in many cases data subjects would only seemingly receive value for the use of their personal data, or there is a risk that market actors would overprice the value of their non-controlling activities in order to obtain the necessary consent for data processing.

A further problem is that the economic potential of personal data covers so many areas and so many data controllers and processors that it seems almost impossible to monitor it at the level of the data subject, even if a specific role were included in the regulation to help the data subject. Nevertheless, the EDPB's position denying the pecuniary value of personal data cannot be upheld. In our view, such value cannot be excluded solely on the ground that the right to privacy is not transferable, as this position does not allow for an assessment of the risks of such data processing. In our view, the case law mentioned in the introduction should therefore permit a visitor to pay for a museum ticket by allowing the museum to resell the personal data electronically provided when purchasing the ticket for advertising purposes, subject to appropriate data protection and consumer protection safeguards, as such an agreement could be beneficial for both parties. At present however, such resales for advertising purposes are to a large extent made in the "grey zone", precisely because of the EDPB's refusal to accept them.

Only with sufficient transparency and preventive instruments can the legislator protect the privacy of individuals, which also applies to the situation where the use of personal data as consideration is established. This requires private law to consider personal data as a legal object that can be monetized and sold. The foregoing is also supported by the recognition in some Member States of the property aspects of a general personality right, which can therefore also apply to personal data without the need to recognize a sort of data ownership. This would make it clear that the sale of the likeness of persons in paintings and photographs, whether on merchandise or in any other form, is either the right of a person or it belongs to the public domain. It would also provide an answer to the question of the extent

to which, especially after the death of the person concerned, any person or even a cultural institution may be entitled to exploit such personality aspects.

The commercial use of personal data can fit dogmatically into the European models of the pecuniary value of personality rights, both in terms of the relationship between personal and property relations, as well as in terms of both unjust enrichment and contractual exploitation. Nonetheless, the problem is that the regulation of personality rights is not an EU policy area, but a matter falling within the competence of the Member States. The EU data protection regulation of the pecuniary value of personal data may give rise to the Member States' resistance, as such regulation would ultimately have an impact on the national regulation of personality rights, and the recognition of the pecuniary value of personality rights is far from being the prevailing position in most Member States, neither from a fundamental rights nor from a private law perspective. However, it could be useful, in the future, for EU policy makers to keep an eye on the directions in which the national legislation and enforcement related to the pecuniary value of personality rights are evolving, and to assess them in the context of the *quid pro quo* of personal data. Indeed, the protection of human dignity and privacy is undergoing changes which are likely to have an impact on the right to informational self-determination. It seems unlikely that this will take the form of a *sui generis* IP right, as the concept of the property aspects of personality rights is much more suited to the nature of personal data.

In our view, the EDPB should therefore also recognize the monetary value of personal data in some form, as the lack of such recognition will not only lead to consumers and data subjects not being able to properly exercise their right to informational self-determination and ultimately to a decrease of their privacy, but may also undermine the uniform application of European data protection law in the long run.

Hence, the EDPB should also consider developing a new policy in this area, heeding the words attributed to James E. Watson, according to which "if you can't beat them, join them".[110]

References

2008. évi XLVII. törvény a fogyasztókkal szembeni tisztességtelen kereskedelmi gyakorlat tilalmáról [Act XLVII of 2008 on the Prohibition of Unfair Business-to-Consumer Commercial Practices], Magyar Közlöny 2008/95.

2013. évi V. törvény a Polgári Törvénykönyvről [Act No. V of 2013 on the Civil Code], Magyar Közlöny 2013/185.

Acquisti A., Taylor C.R., Wagman L., *The Economics of Privacy*, "Journal of Economic Literature" 2016, Vol. 54(2).

[110] After G.Y. Titelman, *Random House Dictionary of Popular Proverbs and Sayings*, Random House, New York 1996, p. 159.

Agreement on Trade-Related Aspects of Intellectual Property Rights, 15 April 1994, 1869 UNTS 299.

Article 29 Working Party, *Guidelines on Consent under Regulation 2016/679*, 10 April 2018, WP259 rev.01.

Article 29 Working Party, *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/ECWP217*, 9 April 2014, WP217.

Baker S., *Numerátorok*, transl. by R. Komáromy, Geopen, Budapest 2009.

Banterle F., *The Interface Between Data Protection and IP Law: The Case of Trade Secrets and the Database Sui Generis Right in Marketing Operations, and the Ownership of Raw Data in Big Data Analysis*, in: M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?*, Springer, Berlin 2018.

California Consumer Privacy Act of 2018, Calfiornia Civil Code [1798.100-1798.199.100].

Case C16/16 P, *Kingdom of Belgium v European Commission*, Opinion of Advocate General Bobek, 12 December 2017, ECLI:EU:C:2017:959.

Case C-98/80, *Giuseppe Romano v Institut national d'assurance maladie-invalidité*, Judgment of 14 May 1981, ECR-01241.

Case C-270/12, *United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union*, Judgment of 22 January 2014, ECLI:EU:C:2014:18.

Case C-300/21, *UI v Österreichische Post AG*, Opinion of Advocate General Campos Sánchez-Bordona, 6 October 2022, ECLI:EU:C:2022:756.

Case C322/88, *Salvatore Grimaldi v Fonds des maladies professionnelles*, Judgment of 13 December 1989, ECR-04407.

Case C-9/56, *Meroni & Co., Industrie Metallurgiche, SpA v High Authority of the European Coal and Steel Community*, Judgment of 13 June 1958, ECLI:EU:C:1958:7.

Case C-911/19, *Fédération bancaire française (FBF) v Autorité de contrôle prudentiel et de résolution (ACPR)*, Opinion of Advocate General Bobek, 15 April 2021, ECLI:EU:C:2021:294.

Case T-187/06, *Ralf Schräder v Community Plant Variety Office (CPVO)*, Judgment of 19 November 2008, ECR II-03151.

Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391.

Chrobak L., *Proprietary Rights in Digital Data? Normative Perspectives and Principles of Civil Law*, in: M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?*, Springer, Berlin 2018.

Commission of the European Communities, *Communication from the Commission to the European Parliament and the Council: European agencies – The way forward*, 11 March 2008, COM(2008) 135 final.

Consolidated version of the Treaty on the Functioning of the European Union, OJ C 115, 9.05.2008, p. 47.

Constitutional Court (Spain), Judgment of 26 March 2001, STC 81/2001.

Council of State (France), Decision no. 434684, 19 June 2020.

Court of Appeal in Kraków (Poland), Judgment of 7 February 1995, I ACr 697/94.

Curia of Hungary, Judgment of 6 October 2021, Kfv.II.37.243/2021/11.

Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, OJ L 157, 15.06.2016.

Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, OJ L 328, 18.12.2019, p. 7./

Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, OJ L 136, 22.05.2019, p. 1.

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77, 27.03.1996, p. 20.

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'), OJ L 149, 11.06.2005, p. 22.

Douglas v Hello! Ltd. [2005] EWCA Civ 595.

ECHR, *Ernst August von Hannover v Germany*, Application no. 53649/09, Judgment of 19 February 2015.

EDPB, *Guidelines 05/2020 on Consent under Regulation 2016/679*, 4 May 2020.

EDPB, *Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects*, 8 October 2019.

European Commission, *Commission Staff Working Document, Executive Summary of the Impact Assessment accompanying the document: Proposal for a Regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services*, 26 April 2018, SWD(2018) 139 final, p. 1.

European Commission, *Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content*, 9 December 2015, COM(2015) 634 final.

European Commission, *Proposal for a Regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services*, 26 April 2018, COM(2018) 238 final.

European Commission, *Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)*, 23 February 2022, COM(2022) 68 final.

European Commission, *Questions and Answers – EU Negotiators Agree to Set Up New European Rules to Improve Fairness of Online Platforms' Trading Practices*, 14 February 2019, https://ec.europa.eu/commission/presscorner/detail/en/MEMO_19_1169 [accessed: 14.07.2023].

European Commission, *Report from the Commission to the Council and the European Parliament: Final report on the E-commerce Sector Inquiry*, 10 May 2017, COM(2017) 229 final.

European Parliament, *Opinion of the Committee on Industry, Research and Energy for the Committee on the Internal Market and Consumer Protection on the proposal for a regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services (COM(2018)0238 - C8-0165/2018 - 2018/0112(COD))*, 23 November 2018, ITRE_AD(2018)627047.

Federal Constitutional Court (Germany), Judgment of 15 December 1983, 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83 = BVerfGE 65, 1.

Federal Constitutional Court (Germany), Judgment of 22 August 2006, NJW 2006, 3409.

Federal Court of Justice (Germany), Judgment of 5 October 2006, BGHZ 169, 193.

Federal Court of Justice (Germany), Judgment of 1 December 1999, NJW 2000, 2195.

Federal Court of Justice (Germany), Judgment of 1 December 1999, NJW 2000, 2201.

Federal Court of Justice (Germany), Judgment of 14 February 1958, BGHZ 26, 349.

Federal Court of Justice (Germany), Judgment of 18 March 1959, NJW 1959, 1269.

Federal Court of Justice (Germany), Judgment of 26 October 2006, NJW 2007, 689.

Federal Patent Court (Germany), Judgment of 25 November 1997, GRUR 1998, 1021.

Fia T., *Resisting IP Overexpansion: The Case of Trade Secret Protection of Non-Personal Data*, "International Review of Intellectual Property and Competition Law" 2022, Vol. 53.

Götting H.-P., *Die Vererblichkeit der vermögenswerten Bestandteile des Persönlichkeitsrechts – ein Meilenstein in der Rechtsprechung des BGH*, "Neue Juristische Wochenschrift" 2001.

High Court of Kecskemét (Hungary), Decision no. 8.P.20.334/2017/17.

Higher Regional Court of Dresden (Germany), Judgment of 4 April 2000, NJW 2001, 615.

Hofmann H.C.H., *Agency Design in the European Union*, "Windsor Yearbook of Access to Justice" 2010.

Kerber W., *A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis*, "GRUR International" 2016, Vol. 11.

Kohler J., *Das Autorrecht*, Fischer, Jena 1880.

Kovács A.Gy., Tóth T., Forgács A., *Effects of European Soft Law at National Administrative Courts*, "Loyola University Chicago International Law Review" 2016, Vol. 14(1).

Kovács A.Gy., Tóth T., Forgács A., *The Legal Effects of European Soft Law and Their Recognition at National Administrative Courts*, "ELTE Law Journal" 2016, Vol. 2.

Lessig L., *Code and Other Laws of Cyberspace*, Basic Books, New York 1999.

Malgieri G., *"User-Provided Personal Content" in the EU: Digital Currency Between Data Protection and Intellectual Property*, "International Review of Law, Computers & Technology" 2018, Vol. 32(1).

Menyhárd A., *A magánélethez való jog a szólás- és médiaszabadság tükrében* [The Right to Privacy in the Context of Freedom of Expression and Media Freedom], in: Z. Csehi, A. Koltay, Z. Navratyil (eds.), *A személyiség és a média a polgári és a büntetőjogban*, Complex, Budapest 2014.

Noto La Diega G., *Data as Digital Assets: The Case of Targeted Advertising*, in: M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?* Springer, Berlin 2018.

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, GDPR), OJ L 119, 4.05.2016, p. 1.

Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, OJ L 186, 11.07.2019, p. 57.

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJ L 152, 3.06.2022, p. 1.

Richter H., *The Power Paradigm in Private Law*, in: M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?*, Springer, Berlin 2018.

Sappa C., *How Data Protection Fits with the Algorithmic Society via Two Intellectual Property Rights – A Comparative Analysis*, "Journal of Intellectual Property Law & Practice" 2019, Vol. 14(5).

Sattler A., *From Personality to Property?* in: M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?* Springer, Berlin 2018.

Schneider G., *European Intellectual Property and Data Protection in the Digital-Algorithmic Economy: A Role Reversal(?)*, "Journal of Intellectual Property Law & Practice" 2018, Vol. 13(3).

Schultz M., *A személyiségi jogok vagyoni értéke és tárgyiasulása* [Commercial Value and Manifestation of Personality Rights], ORAC, Budapest 2022.

Supreme Court (Austria), Judgment of 21 June 2010, SZ 2010/70.

Tari A., *#yz Generációk online* [#yz Generations Online], Tericum, Budapest 2015.

Tene O., Polonetsky J., *Big Data for All: Privacy and User Control in the Age of Analytics*, "Northwestern Journal of Technology and Intellectual Property" 2013, Vol. 11.

Titelman G.Y., *Random House Dictionary of Popular Proverbs and Sayings*, Random House, New York 1996.

Trakman L., Walters R., Zeller B., *Is Privacy and Personal Data Set to Become the New Intellectual Property?*, "International Review of Intellectual Property and Competition Law" 2019, Vol. 50(8).

Trebes A., *§ 59 Frankreich*, in: H.-P. Götting, C. Schertz, W. Seitz (eds.), *Handbuch des Persönlichkeitsrechts*, C.H. Beck, Munich 2019.

Ullrich H., *Expansionist Intellectual Property Protection and Reductionist Competition Rules: A TRIPS Perspective*, "Journal of International Economic Law" 2004, Vol. 7.

Ursic H., *The Failure of Control Rights in the Big Data Era: Does a Holistic Approach Offer a Solution?* in: M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?* Springer, Berlin 2018.

Vékás L., *Über die Expertenvorlage eines neuen Zivilgesetzbuches für Ungarn*, "Zeitschrift für Europäisches Privatrecht" 2009.

Verhoest K., van Thiel S., De Vadder S.F., *Agencification in Public Administration*, in: *Oxford Research Encyclopedia of Politics*, Oxford University Press, Oxford 2021, doi.org/10.1093/acrefore/9780190228637.013.1466.

Wiebe A., *Protection of Industrial Data: A New Property Right for the Digital Economy?* "Journal of Intellectual Property Law & Practice" 2017, Vol. 12(1).