Doctoral (PhD) dissertation theses

PROCESSING OF PERSONAL DATA AT THE INTERSECTION OF EUROPEAN DATA PROTECTION, COMPETITION LAW AND CONSUMER PROTECTION

Dr. Tóth Fanni

Supervisor:
Dr. habil. Zsolt Hajnal PhD
associate professor

UNIVERSITY OF DEBRECEN
Géza Marton Doctoral School of Law and Political Sciences

Debrecen, 2026

I. ANTECEDENTS AND OBJECTIVES OF THE DOCTORAL DISSERTATION

My choice of topic was motivated by the discussion about the disclosure of criminal personal data in connection with a given archival research; on the other hand, it coincided with the beginning of the application of the GDPR. These two facts together aroused my interest and helped me to define the topic I would like to deal with in my thesis: the role of personal data and the regulation of their processing in the EU.

In the digital economy, personal data play a key role, and they have given rise to the business model that has led to the dominance of online platforms and ecosystems. On the other hand, there are the data subjects who theoretically have their personal data, who mostly become data subjects on the basis of a legal relationship: employees, library members, purchasers of products or users of services. As the latter are also consumers, the role of data protection and consumer protection has been particularly emphasized by the rapid pace of technological development, the new challenges constantly emerging through platforms, which have shown that although the protection of consumers' data is an integral part of consumer protection, the relationship between the two is complex and complicated. The data processing of online platforms has an impact not only on individual data subjects and users, but also on other actors of the digital economy, such as business users and third parties, which raised the need to analyse the role of data collection and management in processes affecting market competition, as well as in the decisions of the Commission and authorities, and then the need to regulate it in competition law.

The aim of the thesis is to map the processing of personal data, thereby exploring the intersections of data protection, competition law and consumer protection in a digital environment, and to interpret the impact on market competition and consumers. I have unified the EU legal sources that safeguard the protection of data subjects in connection with the processing of their personal data. To this end, I have analysed the GDPR and the ePrivacy Directive in detail, and in relation to the latter, I have examined the draft e-Privacy Regulation and the provisions of the proposal of the digital omnibus package on cookies. The package proposal affects the provisions of the GDPR and competition law in several respects, and I have briefly referred to the proposed amendments. I have also analysed the legislative acts containing competition law and consumer protection measures in connection with the processing of personal data.

I sought answers to four questions and formulated the following hypotheses:

1.) Are users aware of the value of their personal data, the process of becoming an economic value, and does the right to transparent information provided by the GDPR help them make an informed decision about the processing of their personal data, and is it able to counteract information asymmetry? According to my hypothesis , *data subjects are not aware of the value of their personal data, and the transparency requirements of the GDPR and the Privacy Policy do not help them to resolve the information asymmetry in practice.*

2.) To what extent is the GDPR's regulatory nature and territorial scope able to ensure uniform protection of data subjects in the EU, with special regard to the applicability of the conceptual system, the enforcement of data processing principles, the rights of data subjects and enforcement issues; and does the ePrivacy Directive provide an adequate level of protection? I assume that *the regulational nature and territorial scope of the GDPR are fundamentally suitable for ensuring uniform protection of data subjects, but its enforcement system, especially in cross-border cases, is not effective, as well as the uncertainties in the interpretation of its conceptual system and the difficulties in the practical enforcement of data subjects' rights. However, the cookie regulation of the ePrivacy Directive does not adequately ensure the protection of users.*

3.) Based on the relationship between the processing of personal data and market competition, which provisions of the GDPR have become motivating factors for further tightening, and in what direction are the stricter provisions embodied in platform legislation capable of influencing market competition? According to my hypothesis, *since a close correlation can be demonstrated between the processing of personal data by platforms and the development of market competition, platform legislation on the one hand tightens the applicability of the GDPR provisions on legal bases, and on the other hand, strengthens those of the data subjects' rights that allow personal data to be effectively integrated into the digital economy, but at the same time limit the data processing of large platforms and give room for market competition.*

4.) Is the EU consumer protection toolkit capable of dealing with the asymmetric situation of consumers – related to personal data? I assume that *the EU consumer protection toolkit contributes to the reduction of the asymmetric situation of consumers in relation to personal data, but it is not able to completely eliminate it; which may also indicate that a specific regulatory area, the consumer protection data law, is emerging.*

I primarily used the method of legal analysis and comparison, for which I considered the normative text of the legal sources to be of fundamental importance. I considered the related

EU documents and the results of the relevant large number of literature to be valuable sources. I examined the formation of the EU legislator's intention with the comparative method of legislation, which provided an opportunity for both forward and backward view. I used both the legislative analysis and the comparative method to examine the elements of data protection, competition law and consumer protection instruments. This provided an opportunity to understand the context of the legislative acts and to determine how coordinated and coherent the EU measures are. I relied to a lesser extent on the historical method in order to determine the drivers of the development of data protection. In order to approach the legislation from a practical point of view, I examined a large number of legal cases, both from the case law of the CJEU and from domestic court and authority procedures. In addition to the classic examples, I have also tried to focus on the newer ones and draw conclusions from them. Presenting the application of the law through concrete examples, I made findings in the field of data protection, competition law and consumer protection regarding control and enforcement issues, as well as the factors motivating the EU's legislative processes.

Regarding the structural structure of the thesis, logic required me to deal with the value and significance of personal data after clarifying the basic concepts. On the one hand, the economic significance of personal data is related to the methods of data collection, and on the other hand, it provides a basis for the presentation of the rights of the data subjects, as well as the presentation of the role and regulation of electronic communications data. After that, I focused on the role of personal data in market competition, and then on the consumer protection aspects. Since data are decisive in both areas of law, competition law and consumer protection are intertwined, I still considered it justified to present them in a separate chapter, because the same market behaviour is evaluated and regulated from a different point of view by their provisions.

II. NEW SCIENTIFIC RESULTS OF THE DISSERTATION

1.) Are users aware of the value of their personal data, the process of becoming an economic value, and whether the right to transparent information provided by the GDPR helps them make informed decisions about the processing of their personal data, and is it able to counteract information asymmetry?

Understanding the value of personal data is closer to knowing how service providers get hold of big data, what they do and how they use it. Users often provide their data themselves, in other cases it is acquired by platforms. The data set is not valuable in itself, it must be

managed, the purpose of which is to observe the behavior of users, evaluate their personal characteristics through profiling, and predict their expected behavior. Based on the values obtained, they personalize advertisements and target users, thus monetizing personal data. Although profiling can carry advantages, it typically carries more dangers because they influence user decisions. These processes mostly remain hidden from users.

With regard to the processing and use of personal data for marketing purposes, the knowledge of the two parties is not the same. In a technological and legal sense, the platform has significantly more information than the user, which leads to information asymmetry and imbalance. In order to balance this, the legislator expects transparent data management and information from the data controller, and provides the data subject with the right to do so, which is embodied in the data protection notice. Based on this, the data subject, the user, can make an informed decision about whether and to what extent they consent to the processing of their personal data. It must be stated – agreeing with the opinion of Edwards-Veale and Waerdt – that consent has become a devalued currency in terms of online platforms; the GDPR is unable to manage information asymmetry, it cannot eliminate the gap between platforms and users, thus the asymmetry is fixed rather than eliminated. It is unable to manage it because it does not take into account the business model of the platforms based on data collection and data monetization, as well as the technologies used in the processing of personal data, while the GDPR places the responsibility on the affected users, who in practice are forced to make a decision. This is the origin of the paradox of the right to informational self-determination: the regulation emphasizes individual freedom of decision, while the right of self-determination itself causes a decision-making dilemma for users. The situation is further aggravated by the unmanageable amount of data protection notices, the scope of the information, the time required to read, and the incomprehensible legal language, which can also be related to the fact that the goal of data controllers is not to help the data subjects, but to ensure their own legal protection, which is understandable based on the requirement of accountability. All of this leads users to the behavior of clicking the accept button almost automatically. In my view, this attitude is a behavioral problem only in name, in fact it is an adequate behavior and a "response" to the situation arising from information asymmetry, and since the behavior has become permanent into consent fatigue, decision and consent are now more of a burden than a right.

As a solution, the following could be considered: linguistic simplification; visual articulation of information; offering built-in simple choices; the use of data protection icons. In my opinion, if data protection icons had been available at the same time as or shortly after the introduction of the GDPR, which is already adequate for the digital environment – for which,

however, there is still a lack of widespread research support, standards and a delegated act from the Commission – they could have provided significant help to those affected. However, in the case of data-driven companies, I think the solutions listed above are limited in their effectiveness, because consent fatigue is already fixed. To eliminate information asymmetry, a more radical approach is needed that allows for easier communication, for example, the user could pre-set on their device on which interfaces they consent to the monitoring of user behavior and which they do not.

In the three-party chain outlined above, users cannot solve the asymmetric situation, the platforms do not want to, and the legislators did not take into account the information and behaviour expected from the average user during the creation of the GDPR. On the other hand, it can be stated that the legislator imposes a lot of requirements and rules on the data controller, but if it fully meets the expectations of the GDPR and can prove it, then the protection of the data controller's position is realized, but the protection of the user's position is only in principle. This means that in the GDPR, the legislator's intention treats the protection of the data controller and the data subject symmetrically, but it also does not mean that both parties can meet the expectations of the GDPR to the same extent due to the information asymmetry.

Based on the analysis of the economic value of personal data, it can be stated that – due to data collection, profiling, cookies, the scope of data processing information, and information asymmetry – the gap between the platform and the user is getting deeper and deeper, the latter are less and less able to make informed decisions, and thus become the subjects of intrusive personalized ads. The provisions of the DMA do not help this situation either, because it leaves the way open for gatekeepers to process and cross-use data if they obtain the user's consent, thus restarting the vicious circle. There are several protection mechanisms available against personalized advertising. The institutions of the GDPR would provide an adequate level of protection for users, but this is undermined by information asymmetry. It is also a counterweight that the legislator provides guarantees in relation to profiling and targeted advertising (the right to object and to information), and that the protection must also extend to data transfers to third countries. As a further solution, the use of a model requiring consent or payment of a fee has emerged, which, however, is not a realistic alternative based on the EDPB opinion and the Commission's investigation. It is also important whether the user can protect himself against it. There are sectors where the negative effects of profiling and targeted advertising can be prevented by prudent and conscious behaviour. However, there are areas where it can protect itself against the impact of advertising, but cannot protect itself against the consequences of profiling (financial services).

My conclusion is in line with my preliminary expectations: *Users are not aware of the value of their personal data because they do not fully understand the business model of large platforms. Although the right to transparent information provided by the GDPR and the Privacy Policy provide an opportunity to make an informed decision regarding the processing of their data and to resolve information asymmetry; in practice, however, they only play a formal role, so they are not able to eliminate the imbalance.*

2.) To what extent is the regulation and territorial scope of the GDPR able to ensure uniform protection of data subjects in the EU, with special regard to the applicability of the conceptual system, the enforcement of data processing principles, the rights of data subjects and enforcement issues; and does the ePrivacy Directive provide an adequate level of protection for users?

The type of law of the GDPR is a guarantee to provide uniform protection for data subjects, and only leaves room for national regulation in a few areas. The interests of the data subjects required the extension of the territorial scope, i.e. it must be applied to data controllers with and without a place of business, in the latter case data operations may be related not only to the provision of goods and/or services, but also to the observation of behaviour. Its value lies in the fact that it provides protection for data subjects in terms of overseas data controllers and marketing advertising.

In principle, technology-neutral definitions of data protection concepts provide solid foundations. Among the elements of the conceptual system, the value of the definition of personal data is that it includes a wide range of data; however, it should also be seen that it also provides an opportunity for an expansive, broad interpretation, which means that in a digital environment – taking into account scientific-technical developments – sooner or later any information will result in the identifiability of a natural person. Nevertheless, I do not agree with the point of the proposal of the digital omnibus package that ties the criterion of identifiability to a subjective standard, thus trying to narrow down the scope of personal data. It is to be feared that the concept of mobile interpretation will mean different levels of protection for the data subject. I also consider it a problem that the interpretation of information is made difficult by elements that cause uncertainty. From the point of view of the protection of the data subject, the issue of personal data or anonymised data is of paramount importance. Practice shows that anonymization is not an effective method, and there is a real risk of re-identification. The reason can be methodological, or even a systemic problem. Regardless of the cause, it can definitely undermine the protection of those affected.

With regard to the protection of the personal data of the data subject, the type of legislation, the territorial scope and the conceptual apparatus are of fundamental importance, but they are not sufficient in themselves, it is necessary to provide rights for the data subjects themselves. I can highlight two of the rights of the data subject that provide control over the process of data processing, which provide intensive protection not only in theory but also in practice. One is the right to object, which is a so-called absolute right and is also an effective tool against direct marketing advertising. The other is not formulated as a right, yet it provides the strongest protection with a general prohibition on data processing against the effect of a decision based solely on automated data processing and profiling, which has a legal effect on the data subject or significantly affects him/her. This very valuable protection function is intended to be destroyed by the proposal of the digital omnibus package by enabling algorithmic decision-making for the conclusion and performance of contracts, even if the decision cannot be made exclusively by automated means. Furthermore, there are data subject rights that theoretically provide strong protection for data subjects, but are less functional in practice (theright to privacy, the right to data portability, the right to be forgotten).

The data processing principles built on the responsibility of the data controller serve the protection of data subjects. Purpose limitation, data minimisation, limited storage, fairness are all effective principles, as well as built-in and default data protection and data protection impact assessment. If the data controller considers the data protection impact assessment not only as a formal obligation, it provides a guiding principle for bringing the individual characteristics and the GDPR provisions into harmony and minimising risks. I believe that impact assessment is not only a valuable tool supporting the protection of data subjects' data – which is also able to prepare the possibility of default settings that ensure a fair decision-making environment – but can also become a self-regulatory tool for service providers.

Member State supervisory authorities have the right to carry out inspections, but the GDPR requires a one-stop-shop procedure for cross-border cases. This is beneficial for the companies under investigation, but it causes serious enforcement problems, as only a few LSAs concentrate large cases and can only be dealt with under the consistency mechanism once the cooperation tools have been exhausted. In the case of large cases, enforcement is disproportionate, slow and inefficient. A further problem is that the main supervisory authority role is given to the authority of the Member State where the platform is headquartered and where, as a consequence, the Member State's economic interests in relation to the platforms are also significant. In my opinion, the GDPR procedural regulation will not address the underlying problem; the real solution would be centralisation of enforcement in the case of large cases, as

in the case of the DMA or the DSA. As enforcement is centralised in the event of a breach of the provisions of the DMA, this may indirectly contribute to a reduction in the burden on data protection authorities, but companies that are about to become gatekeepers may cause new surprises related to data processing, thus reproducing enforcement issues as well. A systemic enforcement problem has been brought to the surface in the Facebook v Bundeskartellamt case. According to the CJEU ruling, if it is necessary to examine data protection aspects, the competition authority of the Member State can do so and establish the infringement with regard to the GDPR. The TEU does not contain the specific framework and rules of the principle of sincere cooperation contained therein, which has been replaced by EU case law (and confirmed by the EDPB), which may also govern cooperation between other authorities.

Users must also be protected with regard to communications transmitted on communication networks and data stored on their devices, which is currently regulated by the ePrivacy Directive. However, the GDPR must be applied in all cases that are not subject to the specific obligations set out in the Directive, typically cookies placed on the end-user's device. Some of them are necessary for the operation of websites, while others are closer to determining the personal characteristics of users. The current Directive does not adequately protect users from messages for direct marketing purposes, its provisions do not address technological challenges, and the implementation in the Member States hinders uniform application. The legislator intends to solve these problems first through the legislative procedure for the e-Privacy Regulation and currently for the Digital Omnibus Package. The package proposes that the rules on cookies be brought under the scope of the GDPR, thus linking access to the end device and data processing, and proposes a built-in solution for the management of consent fatigue. However, it does not regulate cookie walls and envisages a subjective decision regarding personal data. Overall, therefore, the adoption of this version may reduce the level of data protection.

The above confirms my hypothesis. *The GDPR's regulational nature, territorial scope, risk management and system of principles provide a stable framework for the uniform protection of today's stakeholders. Its technology-neutral conceptual system is flexible, but the digital environment and the technological context are increasingly challenging its adequacy. Its implementation is made more difficult by the decentralized structure, and the procedural regulation of the GDPR will only be able to help to a limited extent. The content of the data subjects' rights provides strong control, but in practice it raises applicability problems. The ePrivacy Directive, in the field of cookie regulation, does not provide uniform protection for users, mainly due to the different implementation in the Member States.*

3.) Based on the relationship between the processing of personal data and market competition , which provisions of the GDPR have become motivating factors for further tightening, and in what direction can the stricter measures embodied in platform legislation influence market competition?

The experience of abuse of dominant position and merger cases has shown the close relationship between the handling of personal data in the digital economy and the development of competition in the market. Huge data assets are a raw material for platforms that enable them to analyse user behaviour, target users with advertisements, build relationships with business users, etc. Unfair acquisition of personal data and linking between their services can lead not only to a dominant position in the market, but also to its abuse, creating a barrier to entry for other market participants. The size of data assets and the impact on the market can be further increased by mergers. Nevertheless, until 2017, the Commission firmly insisted that the protection of privacy and personal data were not among the criteria of competition law assessment, and a turnaround only occurred when Facebook merged its own and the acquired WhatsApp database.

In order to encourage the fair processing of data and market behaviour by large online platforms, and at the same time to help smaller businesses and move markets, the legislator had to steel the provisions of the GDPR. The most appropriate way to achieve these goals was to strengthen and supplement the provisions in the DMA related to legal bases and data access and portability, which at the same time respect the expectation of Article 102 TFEU: it does not take action against a dominant position, but regulates market behaviour that abuses it.

While the GDPR left a wide range of legal bases for data controllers, the DMA opted for a regulation that leaves no discretion, in such a way that it regulates only gatekeepers in a differentiated and targeted manner. According to the DMA, gatekeepers can only process and combine personal data on the basis of consent, but they cannot use non-publicly available data that is generated in connection with the activities of business users or that has been provided or generated by the latter's customers. The DMA has also extended the right of data access and portability under the GDPR – providing continuous and real-time access to data for end-users, business users and authorised third parties – thereby enabling the switching of service providers and the integration of data into the economy. Another provision for the latter purpose is that the gatekeeper must provide third parties providing online search software with access to the data generated during end-user searches carried out by its search engine, but before that, personal data must be anonymised.

Further rethinking the GDPR's right to data access and portability resulted in a complete regulation, the Data Act, which, in the case of IoT products to be marketed from September 2026, obliges the manufacturer to provide the user with direct access to the data recovered or generated during the provision of the service by default; before this time, the data owner must ensure that the data is made available. Users of IoT products can access, use and share generated data (personal and non-personal), and these rights must also be provided to third parties upon user request. Although the GDPR provides data portability rights for data subjects, I believe, a greater shift is expected from the obligation of manufacturers, which may trigger user activity.

By evaluating platform legislation, the Data Act supports data sharing with an outdated approach, thereby facilitating the circulation of data in the economy, and thus the strengthening and competitiveness of the European data economy. Because of these capabilities, the Data Act will be one of the central regulations of the EU data economy, as proposed by the Digital Omnibus Package. Its real value will be shown by the extent to which users will be able to take advantage of the opportunities and the extent to which beneficiaries will be able to exploit the potential of the regulation. Compared to the Data Act, the DMA is, in my opinion, a belated regulation, but it has the advantage of acting ex ante and allowing for a change in the circle of recipients. This will create a more level playing field and a fairer business environment in the market, and will amplify the innovative resources of platforms. I consider the DMA to be overdue because, due to the consent fatigue that characterizes users, it can no longer make a significant contribution to solving data protection problems. In addition, the DMA wants to support market competition while allowing data protection problems to be reproduced, which leads to the conclusion that the EU is not protecting users against their will, but is creating an opportunity for them to protect their data.

My hypothesis was confirmed. *The examined competition cases pointed out that there is a close connection between the processing of personal data by platforms and the development of market competition, and big data assets play a decisive role in market competition and abuse of dominant positions. Therefore, the provisions of the GDPR that contributed to the creation and use of big data assets through the unfair data processing of platforms, and thus to the anti-competitive behaviour of platforms, had to be strengthened in the platform legislation. Consent was given a much more characteristic role in the DMA from the GDPR, and the right to data access and data portability were also included in the DMA and the Data Act. Restrictions on platforms' data processing and the mobilisation of personal data can foster competition in the market.*

4.) Is the EU's consumer protection toolkit capable of addressing the asymmetric situation of consumers in relation to personal data?

EU consumer protection law seeks to strengthen the protection of consumers with regard to the processing of their data by supplementing the provisions of the classic regulatory areas. The majority of legislation, where relevant, aims to counteract information asymmetry by informing the consumer and prescribing transparency. The CR Directive requires consumers to be provided with additional information before the conclusion of the contract, including whether the price is personalised. The DSA sets out a number of transparency measures to ensure the identifiability of advertisements, which serve to control unsolicited advertisements, and service providers operating the online giant platform and the very popular online search engine must also make their advertising databases publicly available.

Another element of the consumer protection system is the regulation of contracts. The DCS Directive provides rights for contractual performance, remedies, etc. It recognises the provision of digital content or services without monetary compensation, although it does not define this type of contract and does not protect against the devaluation of the service. The UCT Directive protects consumers from unfair terms in the case of contracts that have not been individually negotiated, but its annex does not contain unfair terms in relation to digital markets or platforms, even though legal cases show that online platforms collect personal data fraudulently by hiding behind standard contract terms.

The assessment and mitigation of risks is suitable for protecting the interests of the data subjects and users. Both the GDPR and the DSA focus on risk management and reduction, but while the former requires a data protection impact assessment with a criterion determined by the data controller in respect of high-risk data processing operations, the latter imposes a risk assessment obligation for a specific category of systemic risks, but only for online giant platforms and providers operating very popular online search engines. The latter are expected to provide stronger protection for consumers, especially as they will also have to be accompanied by an annual independent audit.

Children as a vulnerable consumer group are strongly protected by the legislator. The UCP Directive classifies the invitation of children to make purchases as an aggressive commercial practice. Based on the provisions of the GDPR, profiling cannot be carried out (at most for their well-being, based on legal exceptions), and consequently targeted advertising is not allowed. The DSA establishes a clear prohibition for profiling advertising using the personal data of minors, which, however, only applies to online platforms. This differentiated prohibition – for me – is an imprint of the fact that the legislator had a stronger motivation for regulating

platforms than the interests of children. In my opinion, it would be necessary to extend the ban uniformly to all service providers that disseminate information, as well as targeted advertising based on profiling using special categories of personal data.

The provisions and annex of the UCP Directive do not explicitly identify prohibited commercial practices related to personal data, in particular those related to dark solutions, and although the Commission has instructed that these can be addressed on the basis of the provisions and the existing blacklist, their absence significantly complicates the procedures initiated in such cases. The fact that the increasing number of types of dark solutions has provoked a regulatory response in several pieces of legislation leads to a further fragmentation of the consumer protection toolkit. The UCP Directive plays the most important role in dealing with them, as if a conduct does not fall within the scope of the DMA or the DSA, the solution may be to include it in the UTP. This fact further aggravates the lack of a blacklist of prohibited practices related to personal data in the UCP Directive. This not only creates further fragmentation, but also coherence problems, which is a factor against uniform consumer protection. Fragmentation and coherence problems arise not only in the area of dark solutions, but also in the regulation of profiling and personalised advertising.

Due to profiling, algorithms and opaque technologies, asymmetry in the digital space is constantly increasing, and as a result, the average consumer can also become vulnerable; however, the concept of the average consumer does not contain any relevant element. As a solution, the amendment of the UCP Directive could be considered, but also the systemic technical embedding of legal norms, which would burden the regulatory administration on service providers, while also recognizing their regulatory capacity. The EU intends to address digital vulnerability with the Digital Equity Act, the DFA, and the legislative process is currently being prepared.

Due to the large and increasingly frequent appearance of data protection provisions layered on the elements of the consumer protection toolkit, the possibility has arisen that a specific regulatory area is emerging, which I have called consumer protection data law. However, on the basis of the difference in the nature of legal protection, the lack of an independent institutional and conceptual system, but most of all the lack of a separate legal entity, it must be concluded that we cannot speak of an independent consumer protection data law; moreover, this is also reinforced by the above-mentioned cases of lack of coherence. Consequently, this part of my hypothesis must be refuted. However, in the chapter focusing on the GDPR, consumer protection outlooks and the findings of the chapter examining the tools of consumer protection in relation to personal data have led to the fact that there is a

demonstrable parallel between the GDPR and the DSA and classic consumer protection law on several points (territorial scope, ex ante regulation, etc.), which focuses on the protection of the consumer, emphasizing the values that have guided the protection of consumers in the EU for decades.

My findings are in line with my expectations: *In a digital environment, consumer protection and data protection often intersect, so the legislator reinforces the protection of the weaker party with data protection provisions layered on classic consumer protection tools. This contributes to the reduction of the asymmetric situation of consumers, but it is not able to completely eliminate it. One of the reasons for this is that in the digital space, the average consumer may also become vulnerable, but the threads of legislation on how to deal with digital vulnerability are still outlined. Therefore, it would be essential for consumer protection law to react faster and more consistently to the digital environment. Another reason is that since consumer protection law is horizontally linked to other areas of law, the approach and the logic of regulation are also different, which increases the problems of coherence, especially in consumer protection legislation related to data protection. The tips of the iceberg are dark solutions, profiling and personalized advertising.* I have to refute the second part of my hypothesis*: the provisions of consumer protection law related to the processing of personal data do not lay the foundations for the development of consumer protection data law; the nature of protection, the examination of legal entities and the institutional and conceptual system do not support this. At the same time, consumer protection has an increasingly strong data protection segment.*

I examined the role of the processing of personal data in the relationship between service providers and data subjects and users, which also revealed the regulatory processes and intersections of data protection, competition law and consumer protection. We cannot talk about consumer protection data rights, but it can be stated that the appearance of data protection provisions in consumer protection legislation is gaining strength in the digital environment, consolidating the rights of consumers. This process is currently at a point where they are mutually reinforcing: the perspective of consumer protection prevails in data protection, and the approach of data protection is integrated into consumer protection. With regard to the ongoing legislative processes, I am of the opinion that it would be desirable if the DFA regulation that is being drafted would address digital vulnerability on a horizontal level, and would also fit into the system of the EU's digital rulebook. I do not agree with all the points of the proposal in the digital omnibus package, so I believe that clear boundaries should be set

with regard to data protection objectives and the objectives of the economic exploitation of data.

III. LIST OF PUBLICATIONS ON THE TOPIC OF THE DISSERTATION

DEBRECENI EGYETEM
EGYETEMI ÉS NEMZETI KÖNYVTÁR
H-4002 Debrecen, Egyetem tér 1, Pf.: 400
Tel.: 52/410-443, e-mail: publikaciok@lib.unideb.hu

Nyilvántartási szám: DEENK/228/2026.PL
Tárgy: PhD Publikációs Lista

Jelölt: Tóth Fanni
Doktori Iskola: Marton Géza Állam- és Jogtudományi Doktori Iskola
MTMT azonosító: 10066479

A PhD értekezés alapjául szolgáló közlemények

Folyóiratcikkek, tanulmányok (8)

1. **Tóth, F.**: The Role of Personal Data and Data Protection in Platform Regulations Affecting Market Competition.
   Acta Universitatis Sapientiae Legal Studies. "Accepted by Publisher", 1-15, 2026. ISSN: 2285-6293.

   MTA Állam- és Jogtudományi Bizottsága: B

2. **Tóth, F.**: A személyes adatok és az adatvédelem szerepe a piaci versenyt érintő európai uniós platformjogszabályokban.
   Debreceni jogi műhely. 22 (1-2), 205-227, 2025. ISSN: 1787-775X.
   DOI: http://dx.doi.org/10.24169/DJM/2025/3-4/9

   MTA Állam- és Jogtudományi Bizottsága: B

3. **Tóth, F.**: Az intelligens játékok személyesadat-védelmi vonatkozásai.
   Gazdaság és Jog. 31 (11-12.), 48-56, 2023. ISSN: 1217-2464.

   MTA Állam- és Jogtudományi Bizottsága: B

4. Hajnal, Z., **Tóth, F.**: Protection of Children's Personal Data and Risks Posed by Smart Toys.
   Acta Universitatis Sapientiae Legal Studies. 12 (1), 43-59, 2023. ISSN: 2285-6293.
   DOI: http://dx.doi.org/10.47745/AUSLEG.2023.12.1.04

   MTA Állam- és Jogtudományi Bizottsága: B

5. **Tóth, F.**: A fogyasztó személyes adatai értékének jelentősége.
   In: Újratervezés : fogyasztói szabályozási modellek, digitalizáció, adatvédelem. Szerk.: Szikora Veronika, Árva Zsuzsanna, Főnix Média, Debrecen, 157-176, 2019. ISBN: 9789634900795

DEBRECENI EGYETEM Egyetemi és Nemzeti Könyvtár

DEBRECENI EGYETEM
EGYETEMI ÉS NEMZETI KÖNYVTÁR
H-4002 Debrecen, Egyetem tér 1, Pf.: 400
Tel.: 52/410-443, e-mail: publikaciok@lib.unideb.hu

6. **Tóth, F.**: A GDPR újdonságai: a rendeletjelleg és az érintettek jogai = Novelties of the GDPR ?- the regulation form and the rights of the data subjects.
In: A jog tudománya, a mindennapok joga II. / (szerk.) Siska Katalin, Bodnár Beáta, Győri Ágoston, Ivánka-Tóth Barbara Stella, Joó László Ádám, Kőhalmi Máté, Monok Tamás, Salvador Neto Luis, Szabó Mercédesz Ibolya, Tóth Fanni, Wágner Tamás Zoltán, Debreceni Egyetem, Állam- és Jogtudományi Kar, Debrecen, 126-145, 2019. ISBN: 9789634901242

7. **Tóth, F.**: A GDPR-ról - különös tekintettel a könyvtárakra és levéltárakra.
Debreceni jogi műhely. 15 (1-2), 63-75, 2018. EISSN: 1786-5158.
DOI: http://dx.doi.org/10.24169/DJM/2018/1-2/8

MTA Állam- és Jogtudományi Bizottsága: B

8. **Tóth, F.**: Az informatikai bűnözéshez kapcsolódó kényszerintézkedések.
Büntetőjogi szemle. 6 (1), 75-88, 2017. ISSN: 2063-8183.

MTA Állam- és Jogtudományi Bizottsága: C

MTA Állam- és Jogtudományi Bizottsága irányelvei szerint:

„B" kategóriás folyóiratban megjelent publikációk: 5, melyek közül az értekezés alapjául szolgál: 5

„C" kategóriás folyóiratban megjelent publikációk: 1, melyek közül az értekezés alapjául szolgál: 1

A DEENK a Jelölt által a Tudóstérbe feltöltött adatok bibliográfiai és tudománymetriai ellenőrzését a tudományos adatbázisok és a Journal Citation Reports Impact Factor lista alapján elvégezte.

Debrecen, 2026.04.27.

DEBRECENI EGYETEM Egyetemi és Nemzeti Könyvtár