

DATA PROTECTION AS DATA SECURITY, - THE ECOSYSTEM OF DIGITAL MARKETS

MOZSONYI, Norbert*

One of the most dramatic processes of our times is the information explosion and the dramatic social transformation that is taking place in its wake.¹ Digital footprints allow us to reconstruct previously hidden structures and relationships, and to change the tools, methodologies and results of cognition².

The essence of technology is to be as versatile as possible, using more and more data of different categories and timings, with new solutions and operations evolving on a complex daily basis. This does not make privacy "dead", as many people think³ - it is simply that the focus may be on the rules for managing personal data rather than protecting it. In order to harness and reap the benefits of mobile devices, artificial intelligence-based big data technology⁴ and hybrid cloud services⁵, we need to facilitate data sharing and we need regulation that allows this to happen while maintaining the confidentiality of the data with the data controller. The first part of the chapter provides an overview of the approach to the protection of fundamental rights and the definition of the conceptual issues of regulation. The second part argues that our current general contract practice is convenient but not right, given the extent to which we need to enforce our fundamental constitutional rights. The third part outlines the framework of a real contractual relationship for data management. The final part offers some preliminary thoughts on the possible obligations of dominant digital platforms. Accordingly, the regulatory presumption that individuals can control the flow of their personal data should be overcome.

*Legal Counsel, Print Brokers Team Ltd.

¹ Cukier and Mayer-Schönberger, 2013 Big data: A revolution that will transform how we live, work, and think. Houghton Mifflin Harcourt

² Csepeli Gy., Dessewffy, T. (2015): Big Data. A technological change that will fulfil sociology, *Review of Sociology*

³ Here are the titles of some articles: "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms" by Kate Crawford and Jason Schultz, published in the *Boston College Law Review* in the 1st issue in 2014, pages 93-128 (Crawford-Schultz, 11th page); "Privacy in the Age of Big Data: A Time for Big Decisions" by Omer Tene and Jules Polonetsky, published in the *Stanford Law Review Online* in February 2012, pages 63-69 (Tene-Polonetsky, footnote 4).

⁴ Dessewffy and Láng define Big Data as "the collective emergence of qualitatively new social practices and modes of understanding due to the explosive growth in the quantity of digital data." According to the authors, this new paradigm of knowledge formation did not only arise from the increased volume of data in the 21st century but was also significantly shaped by the widespread adoption of digital recordings. Dessewffy Tibor and Láng László (2015): "Big Data and the Accidental Encounter with the Social Sciences on the Operating Table." *Replika* (92-93): 157-170.

⁵ IoT devices, big data processing, as well as data transmission and storage structures, all presuppose artificial intelligence. Conversely, it is also true that artificial intelligence cannot function without a robust quantity of data and adequate data transmission, storage, and computational capacity, which collectively form a particularly complex information technology system. Furthermore, for online platforms that reach the level of qualified data controllers, as defined in the draft regulation on digital services, access to the service provided in relation to them is an essential service subject to a contractual obligation, the subject of a legal relationship that constitutes a real act of data processing based on objective responsibility. The public interest in control of the digital world and accountability of data controllers is clearly articulated, but (unfortunately) very difficult to enforce, and getting harder every day. The regulation of these systems should not be a regulation of technology that respects the business interests of lobbying technology companies, but should be designed and operated as a system of norms based on the fundamental values of human dignity and democratic social order.



Introduction

Nowadays, it is evident that in the information society, almost everything leaves a digital trail, which is analysed through big data technology⁶ based on artificial intelligence. This technology facilitates the identification of previously undiscovered relationships and networks, rendering them visible and amenable to research. As technology advances, increasingly more aspects of our lives can be analysed using well-organised data sets, which can be manipulated and utilised in various ways by constantly evolving digital tools and networks.⁷ There has been a significant increase in the volume of digital information. This data is no longer solely personal data that is intentionally transferred, but is increasingly becoming personal or even special data through big data technology.⁸ As a result, it is subject to personal data processing.

We cannot avoid having a digital footprint, and we cannot avoid it being processed in different structures, because⁹ this is the basis of the service, this is the engine of the service. The possession of personalised information left behind in the digital architecture creates a particularly significant power relationship on a wide scale. This asymmetry of power and information needs to be counterbalanced by the contractual relationship. The regulation of AI-based¹⁰ data management, which is part of our everyday life, cannot be based on a contractual relationship unilaterally established by online service providers. In our view, the regulatory presumption that individuals can control the flow of their personal data should be abandoned.

⁶ In a fundamental rights-based perspective, data protection seeks to safeguard the freedom of the private sphere, where a key concept is the protection of personal data. According to the arguments of Neil M. Richards and Jonathan H. King, we have witnessed changes of significant importance in the past half-century, similar to the industrial revolution, which are reshaping our society and our lives. The latest phase of this information revolution, the big data revolution, promises even more substantial transformation – or threatens it – at an increasingly accelerated pace. They argue that the stake of the big data revolution is that big data analysis influences or threatens all sorts of human activities and decisions, from dating to shopping, from healthcare to education, from law enforcement to the fight against terrorism, to democratic elections. Neil M. Richards and Jonathan H. King: "Big Data Ethics." *Wake Forest Law Review*, 49 (2014), 2, 393–432.

⁷ For example, at the Psychometrics Centre of the University of Cambridge, an extremely efficient and fast method has been developed to accurately analyse the characteristics of an individual or a group of individuals from various data sources. Kosinski, M., Stillwell, D., Graepel T. (2013). Private traits and attributes are predictable from digital records of human behaviour. <http://www.pnas.org/content/pnas/110/15/5802.full.pdf> Published on 2022-03-10. DOI: 10.1073/pnas.1218772110.

⁸ The term "big data" refers to the vast amount of information and processing generated by companies, individual users, and networked digital devices, which is then analysed by computers. As a result, our digital footprints are transformed into personal data, and even sensitive data, which are stored and processed in computational clouds on a systemic level.

⁹ The analysis of the vast amount of data coming from billions of IoT devices is not well manageable with traditional relational databases. The phenomenon of big data is rooted in the fact that in the information society, almost everything leaves a digital trace in real-time, leading to an immeasurable amount of data generated day by day. However, it's not just the size that matters; it's the unlimited growth potential and data analysis. Unlike statistics, big data doesn't ask the individual; it monitors their behaviour without influencing the system or understanding why things happen. Big Data connects generated datasets, opening the door to conclusions and predictions that can provide insights into people's innermost thoughts. Predictive data analysis creates profiles, allowing extremely accurate forecasts about the individual's future decisions. In other words, an individual's digital footprint is pre-constructed, and they know in advance what they will do because their future actions are predictable. (Zsolt Zódi, "Privacy and Big Data," page 19. [<http://fundamentum.hu/sites/default/files>]) *fundamentum-17-1-2-02.pdf*.

¹⁰ The employment of AI-based technologies augments the possibility of personal data being misused by public authorities and in private-party legal relationships. Artificial intelligence has the potentiality to process extensive sets of data and to classify and scrutinize assorted data pertaining to individuals, thereby deriving conclusions concerning them.

The fundamental rights approach

As fundamental rights, human rights are among the most basic values of the constitutional order of individual states and of the international community, as well as the core values of constitutional democracy. Constitutional law is a system of vertical¹¹ norms that regulate the relationship between the public authority and the citizen. In recent decades, European legal development has moved beyond this clear formula and, recognising that the state is by no means the only authority that can have a decisive influence on our lives and the exercise of our rights has gone beyond the vertical scope of law in respect of certain fundamental rights. In comparison, the term 'horizontal scope' of fundamental rights refers to the situation where a citizen can assert their constitutional rights against a private party, rather than solely against the state. It is undeniable that corporations with substantial monetary power, as well as smaller businesses and individuals, may exercise their rights in ways that do not align with international human rights principles. Nowadays, the power dynamics have shifted significantly and any natural or legal person can be a potential infringer, so I see no reason to believe that the protection of our human rights should or can only be asserted against the state.¹²

Building upon a foundation of excellence and trust, the White Paper prioritises safeguarding the EU's core values, including fundamental rights, as a central requirement for the development, use and regulation of AI. Consequently, the development and use of AI is therefore not (or cannot be) an end in itself, but must be seen and regulated solely as a technological tool for the realisation and fulfilment of universal human values and fundamental rights. AI-based data processing, which is ubiquitous in daily life, must not be regulated through a contract unilaterally established by a qualified data controller. Such regulation benefits human well-being only if it promotes the fulfilment of human freedoms and the proper functioning of the constitutional institutions that guarantee such freedoms. Otherwise, we may be falling into Aldous Huxley's freedom paradox trap, a seductively comfortable, desirable and beautiful new world¹³ where we willingly sacrifice not only our freedom but also the basic conditions of our humanity, including dignity, on the altar of consumer welfare and material comfort.

Giant platforms

¹¹ Modern constitutions were created with the aim of clearly defining the framework within which state authority operates, thereby ensuring, above all, the exercise of fundamental rights. Due to this purpose, the rules of the constitution bind the state and its organs: they specify how they should act, the limits of their public power, and what they must do to ensure the adequate guarantee of human rights. In these legal relationships, individuals stand on the side of rights holders, from which they can expect the state to adhere to its operational requirements and respect their privacy and civil rights.

¹² Andrew Z. Drzemczewski: "European Human Rights Convention in Domestic Law. A Comparative Study," Oxford, Clarendon Press, 1983. Chapter 8, pages 373-377. <https://www.corteidh.or.cr/tablas/a11660.pdf>.

¹³ Aldous Huxley: *Szép új világ* ("Brave New World.") Budapest, Kozmosz, 1982.

The processing of personal data by data controllers with a significant digital presence¹⁴, also known as qualified data controllers, should move away from data controller-centric regulation towards a regulation based on contractual agreements that establish objective liability, enabling individuals to effectively assert their fundamental rights. These intermediary service providers¹⁵ are social platform providers and their services include the ranking (e.g. search engine ranking, social platform ranking) or moderation of a large amount of content. For this filtering and ranking activity, large amounts of meta¹⁶ and personal data¹⁷ are processed. And they are increasingly using complex technologies based on artificial intelligence¹⁸ to filter, rank and moderate content, which is essential for personalization.¹⁹ Today's qualified data management utilises a combination of big data technology based on artificial intelligence, wireless communication infrastructure, and hybrid cloud services²⁰. In addition to the paramount importance of data, digitalisation,

¹⁴ Due to the characteristics of the digital economy, some influential "gatekeeper" platforms have acquired invulnerable positions, enabling them to control the development directions of digital economic ecosystems. At the same time, the beneficial effects of competition have become limited. A significant milestone in the qualification of the concept of platforms to the level of qualified data controllers is the draft regulation on digital markets (DMA) and the regulation on digital services (DSA). Within platform services, these regulations create two new platform categories: one based on functionality, termed "core platform services," and the other based on size, further narrowing it down to the largest, the "gatekeepers," imposing additional obligations on them.

¹⁵ Compare: The European Parliament and Council Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (E-Commerce Directive), Section 4: Liability of intermediary service providers.

¹⁶ Artificial intelligence-based systems can be considered a particular type of existing metadata organizing search engines (such as Eur-Lex, suitable for searching legal sources and case law). Their feasibility and further development have greatly contributed to the introduction of the European Case Law Identifier (ECLI) in Europe's legal landscape (InfoCuria). Concerning Eur-Lex, the objective is to enhance the website and improve user experience through website development and search engine enhancement. During this data processing, the extensive information generated can potentially be transformed into personal data when analyzed and assessed in conjunction with other datasets and databases. (European Case Law Identifier - A program for searching the European Case Law Identifier (ECLI).)

¹⁷ In the 21st-century digital economy, platforms and their associated business models play a highly significant role, with a central focus on data, especially personal data. For a long time, the emphasis has been on regulations that ensure the protection of data, particularly personal data. With the help of automated systems (algorithms) integrated into their infrastructure, platform operators can more easily interpret user behaviour patterns and usage trends. Based on this, they can provide personalized content and make other decisions that significantly impact users. These decisions are made by platforms automatically, relying on personal data related to the user. The General Data Protection Regulation (EU) 2016/679 of the European Parliament and the Council, dated April 27, 2016, concerns the protection of natural persons regarding the processing of personal data, the free movement of such data, and the repeal of Directive 95/46/EC (General Data Protection Regulation).

¹⁸ The concept of artificial intelligence is used in various ways by many people. According to the definition provided by the European Commission: "Artificial intelligence refers to systems that exhibit intelligent behaviour by analysing their environment and taking autonomous steps to achieve specific goals." The European Commission describes artificial intelligence as a system that, through the analysis of its environment, exhibits intelligent behaviour and is capable of performing various tasks with a certain degree of autonomy in order to achieve specific objectives. This definition is sourced from "European Commission: A Definition of AI: Main Capabilities and Scientific Disciplines (April 8, 2019)." You can also refer to definitive approaches in Jan De Bruyne and Cedric Vanleenhove's "Artificial Intelligence and the Law" (Cambridge, Intersentia, 2021) and Thomas Wischmeyer and Timo Rademacher's "Regulating Artificial Intelligence" (Cham, Springer, 2020).

¹⁹ IoT devices, big data processing, as well as data transmission and storage infrastructure all presuppose artificial intelligence, and conversely, artificial intelligence also requires robust data, appropriate data transmission, storage, and computing capacity. This forms a particularly complex information technology system. The interdependence of all these standalone technologies underlines the importance of intellectual property protection. The transparency and accountability of this complex technological system face significant challenges, thereby making it nearly impossible to exercise physical control over personal data.

²⁰ Complex systems become interesting due to the emergence of the synergy phenomenon, which means that as a result of the interaction between their parts, the behaviour of the parts changes in such a way that the entire system exhibits qualitatively new behavioural patterns and new regularities different from the properties of the parts. Therefore, the impact of individual technologies comprising the system on our fundamental rights cannot be separately examined. In my opinion, real progress is primarily

through the processes described above, is creating new platforms for social and economic activity and communication that are an integral part of our daily lives, which other authors have called online platforms²¹ with a significant digital presence.

These platforms typically work with large data sets and algorithmic decisions²². Due to their significant market power and capability to manage the digital ecosystem whilst accumulating data assets, they have positioned themselves into a monopoly or oligopoly.²³ As they function as digital service platforms²⁴, they pose a significant challenge to regulate and maintain accountability. Merger control has been "under-enforced" by competition authorities in the technology sector²⁵, resulting in the emergence of this market power. Between 2008 and 2018, Google, Apple, Amazon, Facebook (Meta) and Microsoft collectively acquired more than 400 entities, which were not impeded²⁶. This practice is commonplace in the technology industry, where major corporations buy innovative start-ups - that do not possess significant market power or share - to prevent them from becoming a significant competitor.²⁷ In this manner, a potential business solution or idea is integrated into the acquiring company prior to its ability to exercise any tangible competitive force, solely expanding the portfolio of the larger technology corporation.²⁸ The operation of large platforms gives rise to concerns regarding competition, data protection, consumer protection, and

characterized not by the resource-intensive innovation of individual techniques and technologies but by the interconnection of these techniques and technologies in many areas, forming complex technological systems that complement each other. The challenges in information security of complex systems, such as artificial intelligence, are discussed in "Challenges in Information Security of Complex Systems (2019)" on pages 66-67. <https://bdi.uni-obuda.hu/sites/default/files/oldal/csatolmany/kiadvany-2019.pdf>

²¹ Regarding the Compare: Margrethe Vestager's speech on the regulatory power and antitrust implications of algorithms, titled "Algorithm and Competition," which was delivered at the Bundeskartellamt conference on March 16, 2017.

²² Compare with Margrethe Vestager's speech titled "Algorithm and competition," delivered at the Bundeskartellamt conference on March 16, 2017, discussing the regulatory power and competition-related aspects of algorithms.

²³ The common goal of copyright and industrial property protection is to grant intellectual products various, but in every case, exclusive, monopolistic, absolute protection in proportion to their significance, whether of a financial or other nature, for their right holders and, in a broader sense, for society. Intellectual property rights in the broader sense hold significant importance in the modern market economy, as in a knowledge-based society, information often holds greater value than physically tangible objects.

²⁴ The legislator aims to maintain a high level of protection by enacting criminal and misdemeanour offences in cases of intellectual property rights violations, alongside the imposition of stringent sanctions for such violations. The aim of protecting intellectual property is to grant creators of intellectual works complete rights, including the ability to exclusively use or authorize use of their work, or transfer rights or the right to use it, with some exceptions, in exchange for compensation.

²⁵ Mike Walker: Competition Policy and Digital Platforms: Six Uncontroversial Propositions. *European Competition Journal*, 16. (2020), 1. 4. <https://doi.org/10.1080/17441056.2020.1730063>

²⁶ Mike Walker: Competition Policy and Digital Platforms: Six Uncontroversial Propositions. *European Competition Journal*, 16. (2020), i.m.5. <https://doi.org/10.1080/17441056.2020.1730063>

²⁷ Pünkösty András Merre tart az európai szintű platformszabályozás? – Áttekintés a platformok szabályozásának versenyjogi ösztönzőiről, valamint a fúziókontroll lehetséges fejlesztéséről https://www.ekonyv.hu/api/get_ebook.php?shop=301&order=37079488&ebook=74859&format=pdf&time=1683213343&check=ed2cc0feaf3095d111910d15288_7fc3d (András Pünkösty Where is platform regulation at European level heading? - An overview of competition law incentives for regulating platforms and the possible development of merger control (pages 183-185), April 10, 2023)

²⁸ The FTC, in a lawsuit filed against the tech giant at a later date, objected to Facebook's acquisition of companies that could have posed a threat to its market positions, rather than engaging in competitive behaviour. This applies to the acquisition of Instagram, which was on the rise at the time of the widespread adoption of smartphones and was based on image sharing, as well as the purchase of WhatsApp, which was nearing a tipping point in the market. For the original lawsuit, see *Federal Trade Commission v. Facebook, INC.* Case No.: 1:20-cv-03590, January 13, 2021

privacy, prompting the question of whether enforcement will be capable of responding adequately to the evaluation of activities at the intersection of these areas.²⁹ Additionally, it remains unclear whether the situation will favour platforms, given that the evaluation of their intricate activities, which unavoidably involve several jurisdictions' approaches simultaneously, must conform to a narrower narrative due to jurisdictional limitations.³⁰

Data management - algorithmic decision making as a new technology

Data processing has expanded far beyond our basic personal information such as date of birth, mother's name, address, and ID number. Nowadays, terabytes of digital footprints³¹ are processed on a daily basis. To provide a comprehensive overview without limiting the scope, algorithms are now able to perform various tasks such as spam filtering from emails³², facilitating online shopping³³, drafting contracts, assessing loan applications, making medical diagnoses, driving vehicles, guarding borders, selecting job candidates, and even aiding criminal judges in determining whether to deprive one's liberty. The range of sectors and societal impacts is extensive, encompassing ICT, finance, HR decisions, healthcare, insurance, law enforcement, and numerous other areas of daily life. It is important to emphasise that our digital footprints³⁴, in the form of metadata, can be transformed into personal data, and in some cases this personal data can even be classified as sensitive data³⁵ after processing.

²⁹ Intersection of Competition, Consumer Protection, and Privacy. International Competition Network. www.internationalcompetitionnetwork.org/news-events/intersection-sept2021/ March 15, 2022

³⁰ *ibidem*

³¹ Among the characteristics describable with the 6 Vs of Big Data, this is the "Variety" – the sum of both online and offline activities enhances an individual's digital footprint (e.g., monitoring online activities, CCTV, GPS, IoT [Internet of Things], banking transactions, etc.).

³² Thiago S. Guzella – Walimir M. Caminhas: A review of machine learning approaches to spam filtering. *Expert Systems With Applications*, 36. (2009), 10206.

³³ Mikella Hurley – Julius Adebayo: Credit scoring in the era of big data. *The Yale Journal of Law and Technology*, 18. (2016), 1. 148.

³⁴ These emerged as a result of deliberate human actions, rather than passive observation or academic intent. Their genesis lies in the utilization of services provided on digital platforms. Hitherto concealed structures and relationships can be reconstructed from digital footprints. (Dessewffy Tibor and Láng László, 2015: The Chance Encounter of Big Data and the Social Sciences on the Operating Table. *Replika*, (92-93), p. 158.)

³⁵ In the context of big data technology, the juxtaposition of data sets allows for the construction of sensitive data from the underlying data, to which data protection regulations have afforded enhanced safeguards, proving highly effective at the time (35 Data Protection Act 3. § (2), EU Directive Article 8, Privacy Act 5. § (2), GDPR Article 9. § (1)-(2)). Through automatic data processing, personally identifiable information can be stored without technical limitations and can be seamlessly linked to create a comprehensive profile, without the data subject being able to adequately verify its accuracy and use. Consequently, this also results in unrestricted access to sensitive data, as even data that is individually insignificant can acquire new value. The level of information sensitivity should no longer depend solely on the fact that they pertain to be stored without technical limitations and can be seamlessly linked to create a comprehensive profile, without the data subject being able to adequately verify its accuracy and use. Consequently, this also results in unrestricted access to sensitive data, as even data that is individually insignificant can acquire new value. The level of information sensitivity should no longer depend solely on the fact that they pertain to confidential events. Mező István Személyes adatok védelme az Európai Unió jogában és Magyarországon. (2009). Deák Ferenc Állam-és Jogtudományi Doktori Iskola 132-134.o (István Mező, The Protection of Personal Data in European Union Law and Hungary, 2009, Deák Ferenc School of Law and Political Sciences, pp. 132-134.). <http://midra.uni-miskolc.hu/document/5522/1411.pdf>.

The industry of collecting, linking, marketing and analysing digital footprints is rapidly evolving. Satellites, Wi-Fi and mobile networks track the daily routines, movements, communication habits, social contacts and web searches of hundreds of millions of people. Unfortunately, there seems to be no alternative³⁶ as we have no choice but to accept it. It is impossible to continuously monitor the processing of personal data by an online platform provider, who is also known as a qualified data controller³⁷.

Digital ecosystem - a new world dominated by digital platforms

In the context of big data, certain fundamental data protection principles may lose their relevance, and notions like personal data, purpose limitation requirement³⁸, or informed and voluntary consent may become irrelevant. It is difficult to achieve transparency in practice and monitoring the digital operations of even the largest platforms is a challenge, making accountability and oversight more difficult³⁹. The processing of data by online service providers is usually based on the data subject's consent. However, in this scenario, service providers place users in a "take it or leave it" position, as they unilaterally determine their processing and its conditions beforehand. In addition, the privacy notice is merely a component of the controller's general contractual conditions, with data subjects having little control over its specifics. It is common for established online services to have a cumulative⁴⁰ advantage, as greater data leads to improved

³⁶ In the formation of today's concept of a platform, Gillespie identifies a specific turning point, namely, the moment when Google acquired YouTube in 2006. According to Gillespie, these corporate giants seek to create an advantageous environment for themselves not only through political influence, lobbying, and subtle shaping of the regulatory framework but also through "discursive work." As part of this discursive work and conscious framing, Google consistently began referring to YouTube as a "platform" in its post-acquisition marketing communication, gradually replacing the terms "website," "service," "forum," and "community" with the uniform use of the word "platform."

³⁷ Online giant platforms pose a significant risk in terms of the dissemination of illicit content and societal harm. Special regulations apply to those platforms that reach at least 10% of the 450 million consumers living in Europe. The Digital Services Act, Regulation (EU) 2022/2065 of the European Parliament and of the Council (October 19, 2022) on the internal market for digital services and amending Directive 2000/31/EC (the Digital Services Regulation) addresses this issue. [Link to the regulation: <https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32022R2065>, retrieved on February 16, 2021.]

³⁸ Not everyone is part of the network, but even for those excluded from the network, their relationship with the network is determinant. This is how the so-called fourth world emerges as a result of the impact of information development. The fourth world represents all those who are not participants in value-producing exchange networks but are instead excluded from them. In every society, to varying degrees, the excluded are present, including long-term unemployed individuals, the "disconnected," and the marginalized. For them, global network development signifies nothing more than a new form of capitalist exploitation. (Manuel Castells, 1998: *The End of the Millennium, The Information Age: Economy, Society and Culture. Volume III*. Hoboken, Wiley-Blackwell. In Hungarian: Castells, Manuel (2007). *Az évezred vége*. Translated by Berényi Gábor, Rohonyi András. Budapest, Gondolat-Infonia.

³⁹ A The decision of the German competition authority, known as the Facebook Decision, concluded that Facebook abuses its dominant position when it essentially forces its business partners (users) to accept terms that allow almost unlimited data collection and are also legally objectionable from a data protection perspective. Bundeskartellamt, Case B6-22/16, Facebook Case, paragraphs 526-527. The unique German approach is perhaps most noticeable in a paragraph of the Facebook Decision where the authority derives from a previous case that if one party, due to its dominant position, imposes contractual terms on the other party that restrict fundamental constitutional rights, such as the right to informational self-determination and the protection of personal data, then intervention under competition law is necessary and justified. Bundeskartellamt, Case B6-22/16, Facebook Case, paragraphs 527-529.

⁴⁰ Szőke Gergely László: *Az európai adatvédelmi jog megújítása. Tendenciák és lehetőségek az önszabályozás területén*, Pécs, 2014, Pécsi Tudományegyetem Állam-és Jogtudományi Kar, Doktori Iskola (Gergely László Szőke: *The Renewal of European Data*

service provision, increased user uptake, higher expenditure on development, and reduced market entry for competitors. The acquisition of personal data by online services contributes to market power or leverage, as highlighted in a March 2014 paper⁴¹ by the EDPS. With the increasing proportion of free services in specific sectors, it is evident that these services have amassed immense power through the possession of users' data.

There can frequently be a noticeable power imbalance between the controller and the data subject, resulting in a potential significant impact on the data subject's rights. Additionally, the contract may not be considered valid, as it is improbable to be voluntary⁴². According to the Article 29 Working Party, the existence of a choice cannot be justified by the fact that the data subject has the possibility to choose between the service of the controller, i.e. the service requesting consent for the use of personal data, and an equivalent service offered by another controller. Indeed, in such a case, the freedom of choice is not determined by the controller: it depends on what a market actor independent from the controller does and on whether the data subject considers the competitor's service as equivalent. If this "choice" were accepted as a situation of voluntary consent, it would also mean that the controller would be obliged to modify its own service in line with the market behaviour of its competitors in order to ensure the continued validity of the consent. Therefore, consent based on such an argument would not comply with the General Data Protection Regulation⁴³. As the reader knows, we have no choice about whether we participate in this digital environment or whether we use these digital services. There is little real room for manoeuvre for the user, where Richterich is concerned not so much about the opaque data management practices of the platforms, but rather that people do not have the freedom to choose whether or not to use these platforms. He sees this as practically inescapable for certain social status or expectations of living standards. It raises the question of what bargaining power the person concerned has beyond leaving the platform. Let us be under no illusions that the right to information self-determination as a fundamental right, a legal protection tool in the hands of the individual, may no longer be adequate in today's technological ecosystem.

Summary

The processing of personal data in the traditional sense - such as the drawing up of a contract or the disclosure of your personal data in the minutes of a general meeting - is different from the processing of too

Protection Law. Trends and Opportunities in the Field of Self-Regulation, Pécs, 2014, University of Pécs Faculty of Law, Doctoral School, pages 60-61. February 27, 2023.)

⁴¹ Veronica Moro: Privacy and competitiveness in the age of big data. European Data Protection Supervisor.

⁴² See: The GDPR, especially its Article 6, and in particular, paragraphs (1)(c) and (e),

⁴³ See: Working Party 29's guidance on consent under Article 29, WP259 rev.01, regarding Regulation (EU) 2016/679, specifically in section 3.1.2. Dated February 27, 2023. https://naih.hu/files/wp259-rev-0_1_HU.PDF

much digital data with today's big data technology, just as the functioning of online markets is different⁴⁴ from that of traditional "tangible" markets. In the big data technology environment, it is primarily the processing of data that is directly generated, but not consciously transmitted, during the life and activity of natural persons that leads to outstanding economic results, and constantly improved convenience services provided at a high level without any financial reward. The resultant datasets document and monitor traces of human conduct, facilitating the simulation of natural and social phenomena on a previously inconceivable scale and intricacy⁴⁵. Even though they are typically mere by-products of our daily routine, these data qualify as personal data under the General Data Protection Regulation. An enormous volume of automatic and intellectual metadata⁴⁶ about individuals is processed every day without their awareness, which makes it an opaque process. According to Tene and Polonetzky and Crawford and Schultz⁴⁷, in the era of big data, nearly all aspects of traditional data protection are being challenged and altered. Personal data, proportionality, purpose limitation, and the significance of consent are all assuming new significance. As an illustration of the initial issue, various cases have recently demonstrated that when depending on big data analytics, the separation between an individual and the data may be remedied. This can be achieved, for instance, by the use of formerly unprotected metadata. It is worth noting that while big data is often not classified as personal data (at most it can be re-identified in new ways), evidence suggests that it can cause information overload, particularly when allowing for conclusions to be drawn from it and predictions⁴⁸ to be made. The predictive capabilities of technology are integral to most studies for good reason. Those who know the future possess a form of power that gives them an almost divine power⁴⁹. Technology-driven decision-making challenges substantive investigation and accountability, which are fundamental prerequisites for a fair process within

⁴⁴ Rob Frieden: Challenges to the Conventional Wisdom About Mergers and Consumer Welfare in a Converging Internet Marketplace. The 48th Research Conference on Communication, Information and Internet Policy, 2020.

⁴⁵ Csepeli György (2015): A szociológia és a Big Data. (Sociology and Big Data) *Replika* (92–93): 171–177.

⁴⁶ Metadata can be generated automatically or intellectually. A single metadata may encompass a multitude of information that may not be immediately evident. Some metadata is inherently available and easily accessible, while others require a few steps to become accessible. To illustrate with a simple example, when taking a digital photograph with a digital camera, a variety of digital information is generated at the moment of capture. This can include file type, size, capture timestamp, or image resolution. In the example provided, these details constitute automatically generated metadata (URI3). In our everyday activities, we inadvertently create metadata, such as when we organize our saved documents on a computer, group them into folders, or rename them. In such cases, we are dealing with intellectually generated metadata. Gyarakí R. (2018). *A számítógépes bűnözés nyomozásának problémái. Doktori értekezés. Pécsi Tudományegyetem.* (Challenges in Investigating Computer Crime. Doctoral Dissertation. University of Pécs.)

⁴⁷ Kate Crawford and Jason Schultz: "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms" in the *Boston College Law Review*, 2014/1, pp. 93–128, p. 94.

⁴⁸ Big Data: Seizing Opportunities, Preserving Values" (Page 3) 50, or Phil Simon: "Big Data Lessons from Netflix," available at www.wired.com/insights/2014/03/big-data-lessons-netflix/. The discussion concerns profiling and highly personalized advertising.

⁴⁹ Regarding its predictive capabilities in general: Eric Siegel, "Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die" (New Jersey: Wiley 2013). Concerning purchasing habits: Veronica McGregor, Sophia Helena Calderon, and Roberta Tonelli, "Big Data and Consumer Financial Information," *Business Law Today* 2013/11, 1–4. In the context of police work: Andrew Guthrie Ferguson, "Big Data and Predictive Reasonable Suspicion," *University of Pennsylvania Law Review* 2015/2, 327–410, or Jin-ho Jeon and Seung-Ryul Jeong, "Designing a Crime-Prevention System by Converging Big Data and IoT," *Journal of Internet Computing and Services* 2016/3, 115–128.

the legal framework⁵⁰. This challenge extends beyond mere difficulty in accountability, as in many instances, these entities operate from a monopolistic position, leaving affected parties with limited alternatives for similar services. Furthermore, qualified data controllers, such as online service providers, establish contractual relationships based on their own terms, thereby placing data subjects in a vulnerable position regarding the contractual content. Essentially, they can decide only whether to accept or reject the offered terms without meaningful negotiation. Defining the substantive elements of data processing contracts in a non-negotiable manner does not conflict with the fundamental principles of contract law. This approach ensures the fullest realization of the parties' autonomy in data processing relationships. While contractual relationships in contract law are inherently two-sided in nature, data processing relationships should be similarly characterised. In order for contractual freedom to prevail, it is essential for the legislator to establish a balanced position in favour of the weaker party, essentially restoring and reinforcing the foundation of the contractual principle. The familiar spaces and constraints, along with guiding and coordinating mechanisms that were once present in everyday life and the offline computer world, have weakened or, in some cases, entirely lost their significance. This includes, among other things, the process of personal data management, where informed consent that comprehensively covers the entire data processing procedure has become essential. Information asymmetry, power imbalances between parties, a lack of genuine competition, and the distorting effects of network effects⁵¹ are all factors that, in unregulated market conditions, we consider to be unfair and inequitable in the case of any product. Hence, we empower the legislator to intervene and assist the "invisible hand" in its insufficient work.⁵²

⁵⁰ Ari Ezra Waldman: Power, process, and automated decision-making symposium. Rise of the machines. Artificial intelligence, robotics, and the reprogramming of law. *Fordham Law Review*, 88. (2019), 2. 613–632.

⁵¹ The so-called network effect is a feature of services where users are compelled to use the services of a company with a certain monopoly, as the value of those services is derived from others also using them. The more users on a platform, the more attractive it becomes for others to join, and developers can leverage the accumulated data more effectively in product development with greater amounts of data at their disposal. Consequently, both service providers and users benefit from network effects. Network effects also occur when a corporate group develops and offers multiple services and devices to individuals, allowing them to process data of different content, timing, and structure in order to enhance cross- development. As a result of network effects, rejecting the service imposes a form of cost – the cost of exclusion – on the user, which many users often cannot bear or afford. Consequently, the real choice is questionable, ultimately raising doubts about the voluntariness of consent.

⁵² Chase, Daniel: "Who owns the data – an argument for a property rights approach to transatlantic data protection." In: Medium, 2018, May 22. Part VI. https://medium.com/@Daniel_Chase_/who-owns-the-data-an-argument-for-a-property-rights-approach-to-transatlantic-data-protection-ddc5cc8fc212.