Attila Péterfalvi*

Dániel Eszteri**

When Our Machines Learn Us: About the European Union's Endeavours to Regulate Artificial Intelligence-Based Decision-Making and Profiling

The first part of the paper examines the compliance of data-driven machine learning and software capable of making autonomous, automated decisions with certain provisions of the European Union's General Data Protection Regulation (GDPR) applicable from 25 May 2018. We start the topic with a general introduction to the social impact of AI. Next, we outline the basic technological background and some key concepts of machine learning than the legally relevant issues of such data processing. The relevant provisions of the GDPR will be presented later and some questions and possible solutions related to their applicability. In the second part of the study, we present a famous example of the social impact of data-driven automated profiling, thus the indirect influence of voters' will and consciousness in the so-called Cambridge Analytica scandal, in which the data protection significance of the phenomenon can be very well illustrated. In the final chapter, we briefly present the draft of the EU's new AI Code and how the new legislation would try to regulate this phenomenon generating more and more scientific and professional debate.

Keywords: *Automated decision making, profiling, GDPR, artificial intelligence, machine learning, Cambridge Analytica, AI Regulation.*

1. Introduction: Artificial Intelligence as a Phenomenon to be Regulated

Recently, active scientific discourse has begun at last also among legal scholars in connection with the development and operation of artificial intelligence (AI). While just five

* Doctor of Law, Honorary Professor of Faculty of Law and Political Sciences at Eötvös Loránd University; President of the Hungarian National Authority for Data Protection and Freedom of Information.

** Doctor of Law; Deputy Head of Department of Authorization and Data Breach Notification, Hungarian National Authority for Data Protection and Freedom of Information.

or six years ago, even raising this topic appeared futuristic or somewhat idealistic, today we are at a point where the data protection legal regulation of the European Union in force endeavours to regulate automated decision-making in separate articles; moreover, a general EU legal regulation on the development and operation of AI-based software is about to be adopted.

However, it is worth noting that a kind of primaeval fear related to the aversion from the world of software and machines capable of making autonomous decisions can still be detected in the daily news and even during the question and answer periods of scientific conferences dealing with this phenomenon.

In recent years, we arrived at a point where the legislator could no longer put off regulatory issues: AI matured into a social phenomenon whose regulation must be addressed. This has been given an excellent momentum by several cases erupting around the issue of user profiling and automated decision-making, for instance the Cambridge Analytica scandal, which we are going to cover in detail in this article.

However, let us not jump forward for so much for the time being. First, let us have a look at where the relationship between machines and data began and what sort of impact it may have on humanity and what kind of typical social and legal reactions may be linked to it.

2. Why are We Afraid of Machines? And Why We Should Not Fear Them?

As human beings we have a propensity to endow the "thinking machine" with anthropomorphic properties at some point, characterising living organisms, and ultimately to identify it as a new life form - believed to be superior – that poses a threat to humanity. In philosophy, this phenomenon was first described by the Japanese philosopher Masahiro Mori using the notion of the *uncanny valley* in the 1970s. According to him, as robots become more like humans, our sympathy increases vis-a-vis them - but beyond a point when they become very much human-like, we suddenly see them as bizarre, eerie and threatening.[1]

The roots of these pessimistic schools outlining the archetypal image of an artificial being that awakens to independent consciousness and destroys its creator can be found in pre-20th century literature and folklore (such as the Frankenstein story). Moreover, the conflict between humans and artificial beings appeared not only at the level of literary fiction. During the industrial revolution, the fear of machines "taking the work of man away" gave rise to the Luddite movement in the 1810s.[2]

Recent pessimistic or even *alarmist* theories are based primarily on the problem of "technological singularity", which according to Ray Kurzweil is a future era "*in which*

[1] *Masahiro M.,* The Uncanny Valley, In: IEEE Robotics and Automation, Vol. 19, 2012, 2.

[2] *Barthelmess U., Furbach U.,* Do We Need Asimov's Laws? In: Lecture Notes in Informatics. Bonn, Gesellschaft für Informatik, 2014, 5.

technological change is so rapid and profound it represents a rupture in the fabric of human history". According to Kurzweil, the emergence of superhuman intelligence as a result of the singularity could easily squeeze man out of existence.[3]

According to different, more optimistic theories presented in the work of Stuart Russel and Peter Norvig analysing and summarising the AI phenomenon (such as the tenets of I. J. Good or Moravec), the vision of AI enslaving humans stems from the primaeval, fundamental fear of the superhuman or supernatural, just as the earlier fear of ghosts or witches. Optimists argue that if AI is designed appropriately, i.e. as agents fulfilling the goals of their masters, then AIs arising from the step-by-step progress of current design will serve rather than enslave.[4]

According to the *navigationalist* school, bridging the two concepts, the coming of the intelligence explosion coming into being along the singularity cannot be avoided, but ultimately humanity will have a tremendous role and responsibility in its course. On this basis, the most essential challenge of the future will be the wise navigation in the appropriate direction of machine intelligence transcending human computational and problem-solving capabilities. The navigationalist view of human responsibility and objectivity projects the adulthood of AI development, the image of the responsible parent and teacher. The importance of human responsibility behind every single technological development cannot be overemphasized in relation to the processing of the topic from a legal aspect. Wise navigation and development can best be caught in relation to the data-driven teaching of intelligent software.[5]

3. Artificial Intelligence vs. Artificial Consciousness

The onset of technological singularity concomitant with the acceleration of computational capabilities (no matter in what form it happens) does not necessarily project the "thinking machine", which will eventually communicate to its human creator that it had superseded him as far as evolution is concerned.

It is primarily us, humans who give and attribute meaning to the output of the calculations carried out by the machine, we see in it a kind of intelligence believed to be conscious because of the complexity or authenticity of the presumed meaning.

According to the currently prevailing scientific position, the precondition to abstract machine thinking is not artificial intelligence, but *artificial consciousness* (AC) which,

[3] *Kurzweil R.,* A szingularitás küszöbén, 2014, in: *Marosán G.,* Mi vár ránk a szingularitáson túl? Népszava, 2019, 12, 15.

[4] *Russell St. J., Norvig P.,* Mesterséges Intelligencia – Modern megközelítésben, Budapest, Panem, 2000, Ch. 26.

[5] *Eszteri D.,* A gépek adatalapú tanításának megfeleltetése a GDPR egyes előírásainak, in: *A mesterséges intelligencia szabályozási kihívásai – Tanulmányok a mesterséges intelligencia és a jog határterületeiről*, Török *Bernát T., Ződi Zsolt Z. (szerk.),* 2021, 189, 190.

however, cannot exist without an agent capable of self-identity and self-reflection. All this requires constant referencing to the internal state and comparison with the current external state. Thousands of years ago, Plato put this that what we call thinking is the silent conversation of the soul with itself.[6]

The basis of consciousness is the existence of self-consciousness (or self-awareness), which means reflection on the self, the separation and delineation of the self from the environment and the self-image and approach evolving as a result of this. The evolution and development of self-consciousness, the separation of the self from the environment is a slow process.

For instance, infants do not yet have self-awareness. Jacques Lacan, a French psycho-analyst, for example, links the reaction of infants to the mirror stage, when they react in front of a mirror in a way that suggests self-recognition when confronted with their mirror image. According to Lacan, this "aha experience" and the sequence of events leading to the emergence self-awareness may occur in infants from the age of six months.[7]

As against this, intelligence means the capability of solving problems fast and efficiently through perceiving and processing information and storing the knowledge acquired in this way for subsequent use. While software has long been more efficient and faster than humans at modelling intelligence, it is still incapable of seeing itself as an entity separated and delineated from its environment (and not only because it does not have a mirror at hand).

Borrowing the term used by László Z. Karvalics, there is no processing of information inside the machine, only "code manipulation". The machine carries out signal operations in accordance with its program, but it does not have a "meta level" with respect to the operation itself. This is like when somebody learns how to add, subtract, multiply and divide, but does not know why, when, for what purpose it is necessary. At the level of consciousness, a software has no purpose, has no will, has no points of reference, in relation to which it would have to create new meanings with regard to the environment and the meanings created earlier, and make decision on that basis.[8]

Alva Noë, a well-known scholar of information science taking a systemic approach, calls AI *pseudo-intelligence* in order to underline the difference between living organisms and AI: "A single cell has a life story; it turns the medium in which it finds itself into an environment and it organizes that environment into a place of value. It seeks nourishment. It makes itself — and in making itself it introduces meaning into the universe. In contrast to the machine, an amoeba has information [about itself], it collects and processes it."[9]

[6] *Szathmáry Z., Barna M.,* Büntetőjogi kérdések az információk korában (mesterséges intelligencia, big data, profilozás), Budapest, HVG Orac, 2018, 44.

[7] *Lacan J.,* A tükör-stádium mint az én funkciójának kialakítója, ahogyan ezt a pszichoanalitikus tapasztalat feltárja a számunkra, Thalassa, Vol. 4, 1993, 2.

[8] *Karvalics L. Z.,* Mesterséges intelligencia – a diskurzusok újratervezésének kora, Információs Társadalom, Vol. 15, 2015, 13.

[9] Quoted by: Ibid, 14.

Conflating the problem-solving capability in the given case quite excellently modelled by AI with the human self-reflective consciousness leads to self-contradictory discourse, in which the "alarmist" party believing in the threatening onset of singularity and the other party denying singularity can easily miss the point.

Incidentally, some of the alarmist authors also underline that intelligent machines should be designed as entities "friendly" to human society with a view to preventing the coming into being of hostile AI and to that end, they call for the incorporation of ethical principles in programs.[10] However, it should be emphasized that even in these cases, the software most probably will not be aware of the true meaning of the abstract notions of friendliness or empathy and the content of their meanings at the level of, but the results of the calculations made by it within the framework of the specified objectives would be seen as friendly and supportive of human development for a human observer.[11]

In summary: (self-)consciousness and intelligence are different concepts, yet we have a propensity to conflate them in public discourse in relation to AI.

But how does the AI phenomenon relate to the processing of personal data? The following sections attempt to shed light on this.

4. The Relationship of Artificial Intelligence with Personal Data

Nowadays, the AI-based systems, software and tools used every day provide new types of solutions, which in many cases are concomitant with the processing of the users' personal data. The home robots intended for use by consumers or the smart phone applications analysing human behaviour continuously monitor the behaviour and reactions of their users in order to serve their needs as perfectly as possible. It is no accident that with tools and services using such modern technological solutions the important keyword is personalisation in virtually every case. In addition to being personalised, however, there is an increasing demand for technologies capable of foretelling the needs of the user. This presupposes much more complicated decision-making mechanisms, which can best be achieved with AI-based self-learning systems.[12]

The report of the Norwegian Data Protection Authority (Datatilsynet) on this matter describes AI as a system capable of learning based on its own experiences and applying the knowledge acquired in different situations to solve complex problems. The essence of the

[10] *Goertzel B., Pitt J.,* Nine Ways to Bias Open-Source AGI Toward Friendliness, Journal of Evolution and Technology, Vol. 22, 2011, Quoted by: *Pokol B.,* A mesterséges intelligencia társadalma, 2018, 55-56.

[11] *Eszteri D.,* A gépek adatalapú tanításának megfeleltetése a GDPR egyes előírásainak, in: A mesterséges intelligencia szabályozási kihívásai – Tanulmányok a mesterséges intelligencia és a jog határterületeiről, *Bernát T., Zsolt Z. (szerk.),* 2021, 191.

[12] Ibid, 193.

concept is that AI learns from the personal data “seen” by it (in practice the data uploaded into it) and makes decisions or “forecasts”.[13]

Frequently, AI and machine learning are used as synonyms, although the two phenomena mean different concepts. AI serves is a collective term, which includes all procedures when a software makes a decision automatically. As against this, machine learning is a narrower concept, referring to one branch of AI development. Its essence is that the system generates independent knowledge from experience. The system is able to recognise and identify regularities and rules either independently or with human assistance, based on patterns searched in example data and databases and then to make decisions based on the regularities discovered in the acquired knowledge base.[14]

5. How Do We Teach Data to Machines?

Perhaps one of the most important areas of AI operation from the viewpoint of data protection analysis is the phenomenon of “machine learning”, whereby the software “learns” based on the data uploaded to it and brings various decisions. Most of the time, this appears in the market that the technology applied is practically capable of forecasting the demands of the person using it.

In the course of machine learning, data processing carried out by the AI system can be divided into three steps as follows: [15]

a) First, a large quantity of test data is fed into the system and the algorithm attempts to find patterns and similarities in this dataset. If the algorithm finds such identifiable patterns, it notes them and saves them for subsequent use. Based on the patterns noted and saved, the system is then able to generate a so-called *model*. Then, the system is capable of processing the live data it “sees” (in practice, data uploaded into it) based on the patterns already identified with the assistance of the model.

b) Then, new “live” data are uploaded into the system, which are similar to the ones used for learning. Based on the model generated previously, AI decides which is the pattern it had learned that is the most similar to the new data.

c) Finally, the system notifies the decision it made based on the acquired patterns in relation to the new data fed into it.

It is also important to note that the model generated in the course of machine learning does not necessarily contain the source data which served as the basis of its learning. In

[13] *Datatilsynet,* Artificial Intelligence and Privacy, Report, 2018, <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf> [28.11.2022].

[14] *Szepesvári C.*, Gépi tanulás – rövid bevezetés, 2005, 22, <http://old.sztaki.hu/~szcsaba/talks/lecture1.pdf> [28.11.2022].

[15] *Datatilsynet,* Artificial Intelligence and Privacy, Report, 2018, 7, <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf> [28.11.2022].

most cases, the AI system generated in the course of machine learning is able to operate independently of the data underlying its learning.[16]

6. Relevant Terms of the European Union General Data Protection Regulation (GDPR)

Systems based on machine learning are used to make decisions related to personal data with increasing frequency. Personalised advertisements in the Internet and other contents are good examples of how the algorithms analysing human behaviour and learning from it operate and how they use our personal data to display more and more personalised, targeted content. The notion of automated decision-making is closely related to profiling as the more and more unique profile of the given person evolves along decisions made by the algorithm.

GDPR does not define what is meant by artificial intelligence or machine learning. Although the regulation refers to *automated decision-making* in several places, but does not explicitly define the term.

According to the relevant guidance of the Data Protection Working Party operating according to Article 29 (WP 29), which can be regarded as the predecessor of the European Data Protection Board, automated decision-making is a capability of making decisions with the assistance of technological tools without human intervention.[17] In other words, there is no human participation in the decision-making in the case of exclusively automated decision-making. In actual fact, machine learning can be regarded as the foreground to automated decision-making. This means that the decision made by the machine, i.e. exclusively automated decision-making must in most cases be preceded by some kind of automated evaluation of the data. This evaluation takes place in very many cases based on the patterns acquired and identified by the system in the course of machine learning.[18]

Another decisive element of GDPR is the notion of profiling, which, unlike automated decision-making, is already defined by Article 4(4) of the Regulation. According to the concept, the purpose of profiling is the assessment of the personal characteristics of a natural person. It can generally be said that profiling means the collection of information on a natural person (or a group of natural persons) and the assessment of their characteristics or behavioural patterns with a view to classifying them into certain categories or groups. The purpose of the classification is to analyse the interests, the expected behaviour or

[16] Ibid*,* 10.

[17] *Article 29 Data Protection Working Party,* Guidelines on Automated Decision-Making and Profiling for the Application of Regulation 2016/679, 2017, 8, <https://naih.hu/files/wp251rev01_hu.pdf> [28.11.2022].

[18] *Eszteri D.,* A gépek adatalapú tanításának megfeleltetése a GDPR egyes előírásainak, in: A mesterséges intelligencia szabályozási kihívásai – Tanulmányok a mesterséges intelligencia és a jog határterületeiről, *Bernát T., Zsolt Z. (szerk.),* 2021, 199-200.

certain capabilities of the data subjects.[19] Based on the personality profile set up, later it is possible to send personalised messages or services to the data subject.

It is important to note that the concepts of automated decision making and profiling are not entirely identical. There may be an automated decision-making procedure, which does not qualify as profiling and profiling may be carried out without incorporating automated decision-making mechanisms. In most cases, however, the two notions supplement one another, thus discussing them together is warranted from a data protection point of view.

7. Regulation of Automated Decision-Making and Profiling in GDPR

Article 22 of GDPR contains common requirements on the phenomena of automated decision-making and, closely related to this, profiling. Pursuant to paragraph (1) of this Article, data subject shall have the right not to be *subject to a decision* based *solely* on automated processing, including profiling, which produces *legal effects concerning him or her or similarly significantly affects him or her*. In spite of the formulation of the regulation, this provision is not in fact a right guaranteed for the data subject, but a general prohibition concerning the controller, which prohibits the use of decision-making processes based exclusively on automated processing. This prohibition stands irrespective of whether the data subject takes any measure concerning the processing of his personal data. Therefore, as a main rule GDPR sets a general prohibition on exclusively automated individual decision-making and profiling, which produces legal or similarly significant effects.[20]

Furthermore, the rules applicable to exclusively automated decision-making have to be applied only in the cases when that decision has a legal effect or similar significant impact on the data subject who is a natural person. GDPR does not define the notions of “legal effect” or “similarly significant effect”, but this wording of the regulation makes it clear that Article 22 extends only to effects constituting a severe consequence.[21]

The legal effect requires that the machine decision influence the legal rights of a person. A legal effect may be something that will influence the legal standing of a person or his rights based on contract. According to WP29, examples of such effects include those automated decisions concerning natural persons, as a result of which contracts are terminated, welfare benefits (such as child-related benefits or housing support) guaranteed by law are granted or denied, entry to a country is denied, or citizenship is denied.[22]

[19] *Article 29 Data Protection Working Party,* Guidelines on Automated Decision-Making and Profiling for the Application of Regulation 2016/679, 2017, 8, <https://naih.hu/files/wp251rev01_hu.pdf> [28.11.2022].

[20] *Veale M., Edwards L.,* Clarity, Surprises and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision Making and Profiling. Computer, Law and Security Review, Vol. 34, 2018, 2, 400.

[21] Ibid, 401.

[22] *Article 29 Data Protection Working Party,* Guidelines on Automated Decision-Making and Profiling for the Application of Regulation 2016/679, 2017, 22, <https://naih.hu/files/wp251rev01_hu.pdf> [28.11.2022].

The effect of automated decision-making on the rights of people set forth in law or contract concerns cases that can be relatively clearly delineated. In addition, however, the more vaguely worded concept of "similarly significant effect" also appears in Article 22 of GDPR, which is also constitutes grounds for prohibition.

Recital (71) of GDPR contains some guidance concerning this notion as it lists the following examples: "refusal of an online credit application" or "e-recruiting practices without any human intervention".

It is difficult to accurately define what should be regarded as *sufficiently significant* in order to reach the threshold; however, according to WP29, the following decisions could be in this category: decisions influencing an individual's financial circumstances, such as those concerning his entitlement to a credit; decisions, which influence an individual's access to health care services; decisions, which deny a person the opportunity to be employed, or expose the person to severe disadvantage; decisions, which influence access to education, such as university admission.[23]

According to WP29, automated decisions concerning targeted advertisements based on online consumer profiling do not have similarly significant impact on natural persons (e.g. advertisements of clothing) most of the time. Yet, there are certain data processing operations even in this category, which may have a significant effect on certain groups of society, such as adults in an exposed situation. For instance, if a person presumably struggles with financial difficulties based on the profile generated and he is still targeted regularly with advertisements on high interest loans, potentially he will aggregate additional debts (provided that he accepts such offers).[24] The general prohibition of Article 22 does apply to such cases. According to the main rule, a profile generated (through machine learning) of a consumer struggling with financial difficulties cannot be used to target him in an attempt to induce him to take on additional financial risk. The profilers conducting the data processing cannot claim that the decision to take out the loan is taken independently of them by the data subject, as the profiling on which the consumer's decision is based is not lawful.

As described above, Article 22(1) stipulates a general prohibition on exclusively automated individual decision-making that has a legal effect or similarly significant effect. There are, however, exemptions from this general prohibition set forth in Article 22(2). Accordingly, the prohibition does not apply if the decision:

1. is necessary for entering into or performing a contract between the data subject and the data controller;
2. *is authorised by Union or Member State law,* to which the data controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
3. is based on the data subject's explicit *consent.*

[23] Ibid, 23.

[24] Ibid, 24.

The first exemption is the performance of a contract, on the basis of which controllers may apply automated decision-making processes for purposes related to the contract in a legal relationship coming into being through the contract. According to WP29, in such a case the controller has to be able to demonstrate that the use of the automated decision-making is the most appropriate method of data processing to achieve the purposes specified in the contract. If, taking into account the state of science and technology and the costs of implementation, the objective pursued by the contract can be achieved by other means in an effective way and proportionate to the risks, it is no longer necessary and is also contrary to the principle of data protection by design and by default. [25]

The second exemption is when automated decision-making in relation to the given data processing operation is made possible by Union or Member State law. The relevant legislation must also lay down suitable measures to safeguard the data subjects' rights and freedoms and legitimate interests. According to Recital (71) of GDPR, such a case may be, for instance, when the law authorises the state to use automated decision-making mechanisms in order to prevent fraud and tax evasion.

Finally, the third exemption is when the use of the automated decision-making is based on the expressed consent of the data subject.[26]

GDPR itself does not define the notion of "expressed consent"[27], however, the very concept of "data subject's consent" requires a declaration or express act to be lawful. In addition, WP29's guidance on consent provides guidance on the interpretation of the term 'consent' as follows.

A clearest method of gaining assurance that the consent was expressed is the reinforcement of the consent in a written statement. A signed statement, however, is not the only way to obtain express consent. According to WP29, in a digital or online context it may happen, for instance, that the data subjects can issue the required statement by completing an electronic form, sending an e-mail or uploading a scanned document containing his signature or using an electronic signature. Finally, the validity of the express consent can be verified by a two-step verification of consent (use of two-factor authentication).[28]

[25] 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), OJ L 119, 4/5/2016, 1–88, Article 25.

[26] *Article 29 Data Protection Working Party,* Guidelines on Automated Decision-Making and Profiling for the Application of Regulation 2016/679, 2017, 25, <https://naih.hu/files/wp251rev01_hu.pdf> [28.11.2022].

[27] GDPR Article 4(11): "consent' of the data subject": Any freely given specific, informed and unambiguous indication of the data subject's wishes, by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

[28] *Article 29 Data Protection Working Party,* Guidance on the Consent according to Regulation (EU) 2016/679 (WP259rev.01.), 2018, 20-22, <http://naih.hu/files/wp259-rev-0_1_HU.PDF> [28.11.2022].

8. The Impact of Automated Decision-Making and Profiling on Society or the Cambridge Analytica Case

One of the best-known cases demonstrating the relationship between data-driven economy, profiling and targeted advertisements entered the public domain early in 2018. The antecedents of the case, however, took place in the early 2010s: Aleksandr Kogan, a researcher at the Department of Psychology at Cambridge University, developed an application for Facebook, calling it "This is Your Digital Life" (in brief: TIYDL). TIYDL was a program analysing personality for entertainment purposes, which made a psychological profile of the user. Facebook as the controller of the personal data provided in the course of registration to the social medium gave permission to run the application for research purposes. Incidentally, anyone can produce such an application; the rules of access to user data are defined by Facebook in the Facebook Platform Policy, which is in force at the time and is issued for application developers. If an application complies with the conditions of the rules, it becomes accessible in the social medium.[29]

The use of the application was subject to the consent of the individual data subjects to the processing and that they should be able to learn the purpose for which their data are used. About 270,000 users have used the program under the conditions.[30] Subsequently, however, it was discovered that the application had access not only to the data of the data subjects using it, but to those of their friends. The psychological profile compiled on the user and his/her friends included their political orientations, what contents or actors they followed on Facebook, what was their relationship to religion and where they were placed on the so-called OCEAN-scale[31], which is an acronym of the English names of five characteristics.[32]

Kogan also transferred the entire dataset processed by him to third persons, including Cambridge Analytica and Eunoia Technologies. This clashed with the version of the Facebook Platform Policy in force at the time of the development of the TIYDL, as it

[29] *Domokos M.,* Globális törésvonalak – a Cambridge Analytica-ügy, In: Az Infotörvénytől a GDPR-ig, *Győző S. E. (szerk.),* 2021, 119-120.

[30] *Németh S.,* A közösségi oldalak szolgáltatóinak jogi felelőssége, PhD értekezés (műhelyvitára benyújtott változat), 2021, 119, <https://ajk.kre.hu/images/doc2021/doktori/Nemeth_Szabolcs_PhD_dolgozat_muhelyvitara_FINAL.pdf> [28.11.2022].

[31] The components of the five-dimensional model of the OCEAN scale: Openness to experience (inventive/curious vs. consistent/cautious) – Conscientiousness (efficient/organised vs. extravagant/careless) – Extraversion (outgoing/energetic vs. solitary/reserved) – Agreeableness (friendly/compassionate vs. critical/rational) – Neuroticism (sensitive/nervous vs. resilient/confident). See, <http://medicalonline.hu/cikk/megelozheto_e_az_alzheimer_kor_> [28.11.2022].

[32] *Domokos M.,* Globális törésvonalak – a Cambridge Analytica-ügy, In: Az Infotörvénytől a GDPR-ig, *Győző S. E. (szerk.),* 2021, 121.

prohibited the sale of data to third persons without the consent of the user, as well as the use of the friends' data "for the developer's own purposes".[33]

Facebook noticed that the program was collecting and processing the data of the friends of the users concerned and that Kogan transferred the data to third parties in 2015 and because of this, it removed the application from the site. At the same time, they terminated their contract with Kogan and requested written confirmation from Kogan and the recipients of the data transfers about having annihilated the entire set of the personal data they unlawfully processed. The business organisations concerned allegedly submitted the requested statements to Facebook[34], but Facebook did not check the process of erasure itself.[35]

Then came March 2018 when the fact-finding articles were published in the press, according to which Christopher Wylie, a former employee making statements to the press, alleged that Cambridge Analytica not only did not erase the personal data they unlawfully processed, but using them, it actively targeted certain impressionable groups of voters with political advertisements in the 2016 US presidential campaign based on their psychological profile set up previously. As a result, they successfully influenced these voters in the so-called "swing" constituencies towards supporting Donald Trump, the Republicans' presidential candidate, in the general elections to vote for him. In the same year, the company also had an impact using psychological methods of influencing through advertisements on the UK referendum on EU membership (Brexit referendum). According to Wylie, Cambridge Analytica processed the data of about 87 million Facebook users in the course of these campaigns.[36]

Because of the Cambridge Analytica scandal, the Information Commissioner's Office (ICO), the data protection authority of the United Kingdom, imposed a maximum fine (GBP 500,000)[37] specified by the data protection regulations in force at the time of the infringement on Facebook on 24 October 2018.[38] In July 2019, the US Federal Trade Commission's Bureau of Competition (FTC) imposed a fine of USD 5 billion on Facebook as a result of their investigations launched because of the Cambridge Analytica case.[39]

[33] Facebook Platform Policy, II. point 4, <https://bit.ly/3rioTYH> [28.11.2022].

[34] *Németh S.,* A közösségi oldalak szolgáltatóinak jogi felelőssége. PhD értekezés (műhelyvitára benyújtott változat), 2021, 119, <https://ajk.kre.hu/images/doc2021/doktori/Nemeth_Szabolcs_PhD_dolgozat_muhelyvitara_FINAL.pdf> [28.11.2022].

[35] *Domokos M.,* Globális törésvonalak – a Cambridge Analytica-ügy, In: Az Infotörvénytől a GDPR-ig, *Győző S. E. (szerk.),* 2021, 123.

[36] See: <https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html> [28.11.2022].

[37] See: <https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf> [20.01.2023].

[38] See: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/facebook-issued-with-maximum-500-000-fine/> [28.11.2022].

[39] <https://www.bbc.com/news/world-us-canada-48972327> [28.11.2022].

9. A Brief Evaluation of the Cambridge Analytica Case from the Viewpoint of the Transparency of Algorithms

In relation to the evaluation of the above scandal from the viewpoint of data protection law, it is first necessary to address the concept of micro-targeting. The point of micro-targeting is that the interests of a specific target group or person can be identified based on the user profile set up on the basis of the collected personal data (e.g. browsing habits, contents viewed or liked, social media communication) and a personal message/content can be sent to them through the internet.

The data analysis and profiling necessary for micro-targeting is almost fully automated. In the course of this, based on the data collected on the data subject, the automated decision-making algorithm specifies exactly what type of content is worth sending to him or her and with what frequency thereby influencing their consumer or political decisions and habits. If, for instance, somebody likes a certain product range, listens to performers of a specific musical style or follows the activities of public actors professing to a political ideology, then the algorithm will display such and similar content for him in the future.[40]

The method of micro-targeting is closely related to *choice architecture* and *nudge theory* by Richard Thaler. Nudging means that the individual facing a decision to be made is shepherded or sensitized towards a direction using indirect methods. According to Thaler, nudge is never manipulation, it is only a "slight orientation".[41]

The above concepts have special significance in relation to the Cambridge Analytica case because the personality profiles compiled of the TIYDL users (and their friends) on Facebook were used precisely for sending such automatically micro-targeted political advertisements in order to indirectly influence the outcome of the elections by nudging the decisions of the data subjects towards a specific direction.

The exact interval of unlawful data processing by Cambridge Analytica cannot be determined on the basis of the information available; it is, however, certain that it took place prior to GDPR becoming applicable on 25 May 2018: the personal data were collected between 2010 and 2015 and the voters were influenced with targeted content in 2016. However, verification of the legal basis necessary for data processing, the requirement of transparent processing and advance notification on data processing were requirements prior to the application of GDPR under both the Hungarian data protection regulation[42] previously in force and the international data protection standards. The requirement of

[40] *Domokos M.,* Globális törésvonalak – a Cambridge Analytica-ügy, In: Az Infotörvénytől a GDPR-ig, *Győző S. E. (szerk.)*, 2021, 122.

[41] *Deli G., Kocsis B., Muhari N.,* Akarva-akaratlanul – az adatvédelem és az akaratszabadság dilemmái. In: A mesterséges intelligencia szabályozási kihívásai – Tanulmányok a mesterséges intelligencia és a jog határterületeiről, *Bernát T., Zsolt Z. (szerk.),* 2021, 237-238.

[42] Version of Act CXII of 2011 on the Right of Informational Self-Determination and the Freedom of Information, in force prior to the application of GDPR.

transparency is expressly stipulated in GDPR in Article 5(1)(a). According to this, personal data shall be processed lawfully, fairly and *in a transparent manner in relation to the data subject*.

The users have chosen to use the application and prior to using it, they have given their consent for the application and its "operator" to have access to the personal data provided by them in the course of registration. So, from the viewpoint of the processing of the users' data, the operation of the application could even be regarded as lawful. But the fact that the operator of the application had access to the personal data of a further group of data subjects other than the users using the application (the users' friends) could not be lawful. The reason for this is that the friends of the users did not give their consent to the processing of their data for such a purpose and they received no information at all on this. Thus, the transparency and lawfulness of processing was therefore compromised in this respect. Another unlawful circumstance of processing was that neither the users, nor their friends were aware of the sharing of their data with third parties.

The lack of transparency can be underlined in relation to the failings of both the service provider developing TIYDL and Facebook, which has been at the heart of criticism against the operation of the social media site for many years: the internal rules and IT framework of processing is just as unknown to the public and those applying the law, as for instance the operation of the algorithms distributing targeted advertisements.[43] GDPR itself endeavours to settle this problem when it stipulates specific requirements of transparency and information for automated decision-making and profiling.

According to this, GDPR requires the controller to provide information in relation to decision-making based exclusively on automated data processing having legal effects or similarly significant effects, made by processing personal data. The regulation includes profiling based on such data processing in this category.[44] Under this, the following three items of information must be communicated with the data subject:

1) He must be informed of the fact of such data processing;
2) He must be given meaningful information on the logic applied; and
3) Finally, he must be informed of the significance of data processing and its expected consequences for the data subject.[45]

The communication of the fact of automated individual decision-making is a relatively simple requirement; it suffices if the controller provides information that such data processing is taking place. It is important that the data subject must also be aware if automated individual decision-making also implies profiling.

The mode of providing information on the logic applied raises a number of issues. This may be a substantial challenge for the controller in the case of the machine learning

[43] *Klein T., Tóth A. (Eds.),* Technológia jog – Robotjog – Cyberjog, 2018, 50.

[44] 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), *OJ L 119, 4/5/2016, 1–88*, Article 15(1)(h).

[45] Ibid, Article 13(2)(f).

methods presented in the sections above as that is frequently based on exceedingly complex data processing processes that are very difficult to review.

According to GDPR, controllers must provide "meaningful information" on the logic applied, and using clear and plain language. If a controller communicates only in general that, for instance, it is operating a system based on a neural network may not be sufficient in itself as the data subject will have little meaningful understanding of what is happening with his personal data in the course of processing.[46]

The meaningful information does not necessarily mean that the controller should provide complicated explanations on the algorithm applied or present the algorithm in full. A detailed presentation of the technology would, in most cases, decrease the comprehensibility of the information and impede its reception.[47] In addition, GDPR itself declares that information on the logic applied does not affect business secrets or intellectual property, including the copyright guaranteeing the protection of the software.[48] Naturally, the complexity of the technology cannot be an excuse for completely avoiding the provision of information.

These GDPR provisions require controllers using profiling based on automated decision-making, including sites displaying advertisements using micro-targeting, to provide transparent information about this type of processing. Compliance with this provision is a key issue under the GDPR legal regime: the legislator has recognised the major impact these methods have on privacy. It is to be hoped that these requirements will not only be there for "window-dressing legislation", but controllers will actually comply with them in the course of profiling.

The development and operation of such systems and similar ones is not only an issue for data protection and data processing, which has also been recognised by the legislators of the European Union. The draft of the regulation of the European Commission published on 21 April 2021 foreshadows the regulation of artificial intelligence-based systems, which is briefly presented in the following section.

10. The Draft of the New Artificial Intelligence Regulation

The draft regulation published by the European Commission, which would be a directly applicable regulation similar to GDPR, would regulate the development of artificial intelligence as a uniformly enforceable regulation in every EU Member State.

[46] *Eszteri D.,* Hogyan tanítsuk jogszerűen a mesterséges intelligenciánkat, Magyar Jog, 12, 2019, 679-680.

[47] *Péterfalvi A., Révész B., Buzás P. (ed.),* Magyarázat a GDPR-ról, 2018, 158.

[48] 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), *OJ L 119, 4/5/2016, 1–88*, Recital (63).

According to the Commission's press release, the goal of the published draft is to turn Europe into a global centre of reliable AI. For classification as AI, the draft requires that three conditions are met at the same time. First, AI has to apply specific technologies; second, it has to independently pursue goals designated by man; and finally, it has to produce outputs, which "influence" the environment. According to the relevant writing by Zsolt Ződi, the latter two criteria constitute an attempt at providing an accurate definition of "autonomy". In addition to the systems based on machine learning, the draft of the new Code targets two additional technological groups to which its scope would extend. These are systems based on knowledge representation and statistical systems. According to Ződi, the reason for this may be because systems can be built in this way whose outputs do not appear to be deterministic because of their complexity and the quantity the processed data.[49]

In addition, the Code applies a risk-based approach for the classification of AIs in an attempt to divide the systems into four major categories:

a) The first risk category contains systems classified as having unacceptably high risk. These are AIs which clearly endanger the security, livelihood and rights of people. This includes, for instance, systems or applications which manipulate human behaviour with a view to "bypass the free will" of the users, as well as systems which enable "social scoring" by government.[50]

The data processing based on profiling and micro-targeting carried out by Cambridge Analytica can be put in the former category as the users were unaware that attempts were made to politically influence them through the profiles set up with their data. The latter, as a category requiring prohibition, was surely inspired by the system of so-called social credits developed and tested in the People's Republic of China.[51]

b) In the second or high-risk category, the draft Code includes AI technologies which are applied in altogether nine areas and/or for purposes that constitute high risk for certain fundamental rights of people. These areas are:

- Critical infrastructure (e.g. transportation),
- Education or vocational training (e.g. the scoring of examinations),
- Security equipment for certain products (e.g. robot surgery),
- Employment and the management of employees (e.g. selection of CVs for recruitment),
- Fundamental private and public services (e.g. credit-rating),

[49] *Ződi Z.,* A mesterséges intelligencia jogi fogalma, Blogbejegyzés, 2021, <https://www.ludovika.hu/blogok/itkiblog/2021/06/18/a-mesterseges-intelligencia-jogi-fogalma/> [28.11.2022].

[50] *European Commission,* A Digitális korra felkészült Európa: A Bizottság új szabályokat és intézkedéseket javasol a kiválóságra és bizalomra épülő mesterséges intelligencia terén, Sajtóközlemény, 2021, <https://ec.europa.eu/commission/presscorner/detail/hu/IP_21_1682> [28.11.2022].

[51] *Kollár C.,* Kína és a társadalmi kreditrendszere, Hadtudomány, 2, 2020, <https://www.mhtt.eu/hadtudomany/2020/2020_2szam/079-097_Kollar.pdf> [28.11.2022].

- Law enforcement (e.g. the assessment of the reliability of evidence),

- Asylum cases and border control (e.g. checking the authenticity of travel documents),

- Administration of justice and democratic processes (e.g. the application of laws to concrete facts of a case), finally

- All remote biometric identification systems qualify as high risk according to the draft Code. As the main rule, their use for the purposes of law enforcement in public places and in real time would be prohibited. The regulatory concept allows a departure from this prohibition only in a few exceptional cases (e.g. finding a missing child, the prevention of a direct threat of terrorism or serious criminal act), and even that is subject to the permission of a judge or other independent authority.[52]

AI systems in these categories must meet stringent obligations prior to being placed on the market. The draft requires that all such systems must undergo appropriate risk assessment and reduction processes in the course of development. The datasets used in the development of AI must be of excellent quality and every activity must be logged to ensure the traceability of results and detailed documentation must be available on compliance assessment. The draft also requires clear and comprehensible information to be provided to users, the need for human supervision and, as a matter of principle, the requirement of reliability, accuracy and safe operation of the system.[53]

c) The draft classifies AI systems as having limited risk that require users to be aware of communicating with a machine rather than with a human but (e.g. chatbots). Presumably, this transparency requirement is necessary so that users are not misled by the program and are aware of the fact that it is not another person "on the other side of the monitor".

d) Finally, the draft classifies system in the minimum risk category that constitute the vast majority of AIs, the use of which poses almost no risk to the rights and security of users. The Code allows the free use of these systems and does not include any intervening measures with respect to them, thus practically they are withdrawn from its scope. Examples of such AIs include spam filters or the use of video games.

Recently, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) expressed their joint opinion which, in general, welcomes the draft. In some areas, however, for instance in the field of remote biometric identification, the EDPB would tighten up the rules. As a main rule, the opinion would prohibit the use of remote biometric identification systems, which are capable of classifying data subjects into categories based on some characteristics, such as origin, sex or sexual orientation, as this could easily lead to discrimination.[54]

[52] *European Commission,* A Digitális korra felkészült Európa: A Bizottság új szabályokat és intézkedéseket javasol a kiválóságra és bizalomra épülő mesterséges intelligencia terén. Sajtóközlemény, 2021, <https://ec.europa.eu/commission/presscorner/detail/hu/IP_21_1682> [28.11.2022].

[53] *Ibid*.

[54] *European Data Protection Board*, *European Data Protection Supervisor*, Joint opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council laying down Harmonised Rules on

In addition to the above, the European Council also welcomed the regulation of this area. However, the Polish and the Czech Senates have also expressed their concerns about the use of biometric identification systems in public areas, which would be permitted under the draft, so similarly to the position of EDPB, they urge for a more stringent approach than the current one in their letter written to the Commission.[55]

In the coming period, the draft Code will certainly and frequently constitute the basis of professional as well as scientific discussion, until it is fully adopted by the European Union. In general, it can be said that the risk-based approach and the relatively narrow range of systems that are prohibited or classified as high risk suggests a forward-looking and sufficiently flexible regulation.

11. Summary

We have seen, through the development of artificial intelligence, including the data-driven machine learning, that decisions made by software and their behaviour depends on the datasets used for teaching them. Hence, the software developer and the system operator carry enormous responsibility for these systems. In all likelihood, this area is going to be even more emphatic in the future due to the new draft AI regulation of the EU.

In automated decision-making and profiling, it is highly important that the datasets used for teaching are of appropriate quality, which can be achieved by the careful pre-selection of databases and the appropriate labelling of the data. It is therefore a fundamental misconception that the more data a machine learning algorithm uses, the more efficiently it is going to operate and make decisions subsequently.[56] Typically, the careful pre-selection of datasets and narrowing them down to the necessary extent, will result in more efficient decision-making systems; this is confirmed by current scientific opinion and the new draft EU regulation stipulates it as a fundamental requirement, as a matter of principle. Less is therefore often more, as the saying goes…

In addition to the above, in relation to the personal data processed in the course of the live operation of the systems, it is essential to demonstrate the appropriate legal basis for processing, to take into account the principle of data minimisation and to ensure that the system operates in a transparent and accessible manner, where information on the logic used is one of the key elements.

All in all, it can be said that from a general regulatory perspective, the issue of AI and data-driven automated decision-making is still in its infancy; however, the concrete

Artificial Intelligence (Artificial Intelligence Act), 2021, <https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf> [28.11.2022].

[55] *Pethő M.,* Aranyérem a szabályozásban? Blogbejegyzés, 2021, <https://www.ludovika.hu/blogok/messzelato/2021/12/08/aranyerem-szabalyozasban/> [28.11.2022].

[56] *Datatilsynet*, Artificial Intelligence and Privacy, Report, 2018, 11. <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf> [28.11.2022].

regulatory concepts developed in the recent period seem to be forward-looking. The key issue for the coming years will be the practical applicability and the efficiency of the regulation. As far as we are concerned, we are looking forward to the developments in legal practice.

Bibliography:

1. 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), OJ L 119, 4/5/2016, 1–88.
2. Act CXII of 2011 on the Right of Informational Self-Determination and the Freedom of Information of Hungary, 2011.
3. *Article 29 Data Protection Working Party,* Guidelines on Automated Decision-Making and Profiling for the Application of Regulation 2016/679, 2017, 8, 10, 22, 23, 24, 25, <https://naih.hu/files/wp251rev01_hu.pdf>, [28.11.2022].
4. *Article 29 Data Protection Working Party,* Guidance on the Consent according to Regulation (EU) 2016/679 (WP259rev.01.), 2018, 20-22, <http://naih.hu/files/wp259-rev-0_1_HU.PDF> [28.11.2022].
5. *Barthelmess U., Furbach U.,* Do We Need Asimov's Laws? In: Lecture Notes in Informatics. Bonn, Gesellschaft für Informatik, 2014, 5.
6. *Deli G., Kocsis B., Muhari N.,* Akarva-akaratlanul – az adatvédelem és az akaratszabadság dilemmái. In: A mesterséges intelligencia szabályozási kihívásai – Tanulmányok a mesterséges intelligencia és a jog határterületeiről, *Bernát T., Zsolt Z. (szerk.),* 2021, 237-238.
7. *Domokos M.,* Globális törésvonalak – a Cambridge Analytica-ügy, In: Az Infotörvénytől a GDPR-ig, *Győző S. E. (szerk.),* 2021, 119-120, 121, 122, 123.
8. *Datatilsynet,* Artificial Intelligence and Privacy, Report, 2018, 7, 10, <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf> [28.11.2022].
9. *European Data Protection Board*, *European Data Protection Supervisor*, Joint opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2021, <https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf> [28.11.2022].
10. *Eszteri D.,* A gépek adatalapú tanításának megfeleltetése a GDPR egyes előírásainak, in: A mesterséges intelligencia szabályozási kihívásai – Tanulmányok a mesterséges

intelligencia és a jog határterületeiről, *Bernát T., Zsolt Z. (szerk.),* 2021, 189, 190, 191, 193, 199-200.

11. *Eszteri D.,* Hogyan tanítsuk jogszerűen a mesterséges intelligenciánkat, Magyar Jog, 12, 2019, 679-680.
12. *Goertzel B., Pitt J.,* Nine Ways to Bias Open-Source AGI Toward Friendliness, Journal of Evolution and Technology, Vol. 22, 2011.
13. *Karvalics L. Z.,* Mesterséges intelligencia – a diskurzusok újratervezésének kora, Információs Társadalom, Vol. 15, 2015, 13, 14.
14. *Klein T., Tóth A. (Eds.),* Technológia jog – Robotjog – Cyberjog, 2018, 50.
15. *Kollár C.,* Kína és a társadalmi kreditrendszere, Hadtudomány, 2, 2020, <https://www.mhtt.eu/hadtudomany/2020/2020_2szam/079-097_Kollar.pdf> [28.11.2022].
16. *Kurzweil R.,* A szingularitás küszöbén, 2014, in: *Marosán G.,* Mi vár ránk a szingularitáson túl? Népszava, 2019, 12, 15.
17. *Lacan J.,* A tükör-stádium mint az én funkciójának kialakítója, ahogyan ezt a pszichoanalitikus tapasztalat feltárja a számunkra, Thalassa, Vol. 4, 1993, 2.
18. *Masahiro M., The Uncanny Valley, In: IEEE Robotics and Automation, Vol. 19, 2012, 2.*
19. *Marosán G.,* Mi vár ránk a szingularitáson túl? Népszava, 2019, 12, 15.
20. *Németh S.,* A közösségi oldalak szolgáltatóinak jogi felelőssége, PhD értekezés (műhelyvitára benyújtott változat), 2021, 119, <https://ajk.kre.hu/images/doc2021/doktori/Nemeth_Szabolcs_PhD_dolgozat_muhelyvitara_FINAL.pdf> [28.11.2022].
21. *Pethő M.,* Aranyérem a szabályozásban? Blogbejegyzés, 2021, <https://www.ludovika.hu/blogok/messzelato/2021/12/08/aranyerem-szabalyozasban/> [28.11.2022].
22. *Péterfalvi A., Révész B., Buzás P. (ed.),* Magyarázat a GDPR-ról, 2018, 158.
23. *Pokol B.,* A mesterséges intelligencia társadalma, 2018, 55-56.
24. *Russell St. J., Norvig P.,* Mesterséges Intelligencia – Modern megközelítésben, Budapest, Panem, 2000, Ch. 26.
25. *Szathmáry Z., Barna M.,* Büntetőjogi kérdések az információk korában (mesterséges intelligencia, big data, profilozás), Budapest, HVG Orac, 2018, 44.
26. *Szepesvári C.*, Gépi tanulás – rövid bevezetés, 2005, 22, <http://old.sztaki.hu/~szcsaba/talks/lecture1.pdf> [28.11.2022].
27. *Veale M., Edwards L.,* Clarity, Surprises and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision Making and Profiling. Computer, Law and Security Review, Vol. 34, 2018, 2, 400, 401.
28. *Ződi Z.,* A mesterséges intelligencia jogi fogalma, Blogbejegyzés, 2021, <https://www.ludovika.hu/blogok/itkiblog/2021/06/18/a-mesterseges-intelligencia-jogi-fogalma/> [28.11.2022].
29. Facebook Platform Policy, II. point 4, <https://bit.ly/3rioTYH> [28.11.2022].

30. <https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html> [28.11.2022].
31. <https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf> [28.11.2022].
32. <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/facebook-issued-with-maximum-500-000-fine/> [28.11.2022].
33. <https://www.bbc.com/news/world-us-canada-48972327> [28.11.2022].