DATA PROTECTION CHALLENGES IN THE ERA OF ARTIFICIAL INTELLIGENCE

Vivien Kardos[1]

DOI: 10.24989/ocg.v341.21

Abstract
Nowadays, various applications of artificial intelligence (AI) are clearly seen in many fields, therefore, it may seem like a technological achievement of the 21st century. However, its origin dates back to the middle of the last century.

The questions arise as to how AI can be illuminated from the perspective of data protection, and especially what the main data protection concerns are, moreover, what kind of data protection risks it poses, and what practical solutions are known about the topic. The purpose of this paper is to provide an insight into the data protection approach to AI through some practical examples.

Based on the results it can be established that this futureproofing technological solution poses several challenges for data protection. As a learning algorithm based on poor foundations can also lead to erroneous conclusions, AI requires a fair amount of appropriate data in order to provide reliable results. It should also be highlighted that profiles can be created from enormous amounts of data and conclusions may be drawn about our habits, which raises concerns. Additionally, its reliability is in question, not only due to the basic data, but due to the self-learning, "black-box" system. The knowledge on which it bases assertions about "something" is very limited. It is obviously a high risk from a data protection perspective.

1. Introduction

In the 21st century, it is becoming more and more apparent that AI is having an increasing effect on people's everyday lives, not just on the side of technology. However, it should not be forgotten that the origin of AI dates back to the mid-1950's. [19] The pace of development has been strengthened by the fact that a few decades after laying the cornerstones of AI, in September 2020, an article by GPT-3, Open AI's language generator, was published in The Guardian. The question may arise as to why it is different from any other articles. As it is a cutting-edge language model, which uses machine learning to aid "its" performance, it can write texts like humans. [9]

Today, we can find solutions based on AI in many areas of everyday life. Some examples are listed as follows. In the field of social media AI has key impacts, we only have to think of the deep learning of Facebook, which helps to draw value from a larger portion of its unstructured datasets to update the over 2,7 billion monthly active users' [28] statuses. [21] In the case of Instagram, AI is applied - with the use of big data - to target advertising, fight cyberbullying and delete offensive comments. Another social networking site, namely Twitter, uses AI from tweet recommendations to fight inappropriate or racist content and intensify the user experience, furthermore, learning over time what the preferences of the users are. In the context of self-driving and parking cars, deep

[1] Department of Statistics and Demography, University of Szeged, Hungary, kardos.vivien.kata@szte.hu

learning is used for recognizing the space around a vehicle. AI-powered functions can be found in email communications as well, for instance in Gmail smart responses, which help users to respond in an easy way by accepting the typical, brief responses offered. In Google's predictive searches the reflection of AI can be seen by typing search terms and then finding recommendations to choose from. The search engine of the above-mentioned company learns from the results and AI is used to help in the determination of the quality of the content and match it to the questions of the users. [21] It can be observed that in recommender systems (e.g. music, film, product and service) various AI techniques have been applied in order to enhance the user experience in a personalised way and increase user satisfaction, thereby making the decision process easier for users. [33] During the difficult and challenging times of the Covid-19 pandemic it can be established according to Vaishya et al. that applying AI can help in the early detection and diagnosis of the infection, monitoring the treatment, contact tracing of the individuals, the projection of cases and mortality, the development of drugs and vaccines, reducing the workload of healthcare workers and in the prevention of the disease. [31]

The question arises as to how AI is assessed from the perspective of data protection, with particular regard to the challenges, risks and, principles of processing personal data, and what practical solutions are known about the topic in the legal sphere. The purpose of this paper is to provide an insight into the data protection aspect of AI through literature and practical examples, and provide responses to the above-mentioned questions as well.

2. Issues of AI

This paper is not intended to provide a broad definition of AI. However, briefly, the approach used is that AI is able to make independent decisions (decision-making system) based on data and its environment, and that it comprises self-learning algorithms as well. In 1985, the concept of AI was determined as "the theory that a mechanism can perform those functions of human intelligence: reasoning, problem-solving, pattern recognition, perception, cognition, understanding, and learning" by Waldman. [32] According to Kaplan and Haenlein, AI is defined as "a system's ability to interpret external data correctly, to learn from such data, and to use those learnings to achieve specific goals and tasks through flexible adaptation". [17] It should be noted that further definitions and classifications are known in the literature. In this particular case, the focus is not on the regulatory issues of AI from a technological point of view, but rather on data forming the basis of the learning algorithm, which is a key element of its operation, drawing attention to some data protection issues. Basically, three issues can be viewed in connection with AI systems: input, operating principle (algorithm), and output.

2.1. Input data

Just as the structure of a building depends on its foundation, the quantity and quality of data is crucial for the outcome of AI. The reliability of the data table and/or the methodology applied can lead to biased results, which pose several challenges and potential risks, its relevance being extremely high.

On this issue it is important to briefly provide an insight into the term of input data. When deploying an algorithm, it is fed with new, unseen features, which is the input data. These are evaluated against the parameters of the model for taking actions or making decisions. The browsing history of people without yet knowing if they would click on a certain ad can be mentioned as an example. [7]

2.2. The "black-box" problem

Having regard to the fact that the AI system will be a self-learning algorithm at a later stage, its operating principles can be compared to a black-box. Bathaee draws attention to a significant concern and potential risks of AI that if an Al program is a black box, it will make predictions and decisions as humans do, but - the difference is - without being able to communicate its reasons for doing so. Moreover, the thought process of the AI may be based on patterns that human thought cannot perceive. With regard to this finding only a "little can be inferred about the intent or conduct of the humans that created or deployed the Al, since even they may not be able to foresee what conclusions the Al will reach or what decisions it will make". [2]

2.3. Output issues

There is serious relevance to how reliable the output is. For example, if the input data and the question waiting to be answered do not completely cover each other. Hence, if someone intends to analyse the movements (location) of people in general, then in this case conclusions can only be drawn for those who have constantly enabled this feature, for those who have not, or may not have continuously enabled it, it cannot be done.

From an international dimension, the importance of monitoring the software was highlighted in the case of Wisconsin v. Loomis in 2016. The defendant claimed that his constitutional right to due process was violated by the court's reference to the risk assessment report at sentencing. The report contained scores estimating the risk of recidivism that were calculated by the proprietary algorithm. The defendant also stated that the software used at sentencing by the Wisconsin authorities had not been cross-validated on (i.e. tested against) a Wisconsin population. The significance of this case was underlined as despite no violation was found in this case, the Wisconsin Supreme Court ruled that any pre-sentence investigation report must contain information on the limitations of the software, including notification that the algorithm compares defendants to a national sample, and not to the population of Wisconsin. In addition, the court also noted that the software must be constantly monitored and re-normed for accuracy due to changing populations and subpopulations. [30; 7]

The importance of data protection issues becomes truly emphasized in the context of the consequences, as if the pattern does not correspond to the whole picture, it distorts the outcome, which related to all. It is highlighted that if an AI system that has been trained on biased or misguided data it will formalize and amplify errors. [16]

3. Data protection challenges

Based on the data table and the methodology applied, there are a several significant issues concerning data protection, which can lead to serious legal problems. The purpose of the following parts is to provide insights into some of the data protection-related issues. Today, AI is surrounded by an enormous number of regulatory questions, many of which have not been answered yet. Nevertheless, it can be established that various recommendations have been published, and a white paper has been issued on the subject as well.

The White Paper on Artificial Intelligence – An European approach to excellence and trust (hereinafter referred to as 'White Paper') of the European Commission expressly determines the following as main risks: fundamental rights, including personal data and privacy protection and

non-discrimination. The White Paper explicitly highlights risks in the field of data protection indicating potential cases: "[t]hese risks might result from flaws in the overall design of AI systems (including as regards human oversight) or from the use of data without correcting possible bias (e.g. the system is trained using only or mainly data from men leading to suboptimal results in relation to women)".[8] In the following sections of the current paper some of the relevant issues from the perspective of data protection will be presented, drawing attention to the challenges of AI.

3.1. AI in the context of data protection

The Regulation (EU) 2016/679 of The European Parliament and of the Council (General Data Protection Regulation; hereinafter referred to as 'GDPR') [24] determines the concept of personal data in a broad sense in Article 4(1), which means any information relating to an identified or identifiable natural person. This includes the conclusions to be drawn as well. Moreover, the GDPR explicitly specifies the term of profiling in Article 4(4). Technology seems capable of inferring certain personal attributes based on data not instantaneously related thereto. [29] For this reason, it is extremely important that the data used as the basis of the learning algorithm is appropriate in order to avoid distortions, bias and discrimination. Notwithstanding to the fact that processing of special categories of personal data (e.g. race, political opinions, religious beliefs, trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, sexual orientation) is prohibited based on Article 9(1) of the GDPR, algorithms are capable of deriving this information through other data respecting for privacy boundaries. [5; 29]

According to Article 22 of the GDPR, the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling. Thus, individuals may object to any kind of processing of their data, which is conducted without any human oversight or involvement. In accordance with Articles 13-15 of the GDPR, related to information and access to personal data, it is required of all organisations which intend to put data into an algorithm that will afterwards make a decision affecting an individual, to inform the individual that such processing will take place . Based on the provisions of the GDPR, automated individual decision-making is not under a total prohibition, some exceptions are determined in Article 22(2): this kind of decision-making is necessary for entering into, or the performance of, a contract between the data subject and a data controller; it is authorised by Union or Member State law; or the explicit consent of the data subject has been given to the automated decision-making. In case of special categories of personal data, the level of protection, including the restrictions on automated decision-making established by the GDPR, is much higher. Approaching automated decision-making in another way Araujo et al. established in their study that data from a scenario-based survey experiment with a national sample (N = 958) interestingly shows that people often evaluate decisions taken automatically by AI on a par with or even better than human experts for specific decisions. [1]

The provisions of the GDPR affect the issue of profiling, including the rights of the data subject in this question. Nevertheless, several risks are confirmed. Data mining can be used to create digital profiles, permitting substantial decisions to be made without the knowledge of the individual. [15] It is underlined in case of profiling as "the construction or inference of patterns by means of data mining and as the application of the ensuing profiles to people whose data match with them". [13] Ishii pointed out that "if the resultant data misrepresent the individual's personal aspect, or the data reveal excessively intimate behaviors of the individual, such data would greatly transgress the person's expectation of privacy. Automated decisions would distort others' reasonable evaluations of the person". [15]

3.2. Principle of data minimisation and accuracy

Article 5(1)(c) of the GDPR determines the principle of data minimisation, that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Potential risks and further questions arise to comply with this principle, as in case of AI it is precisely the fact that a large amount of data is required and processed. In this case there is a collision, as according to the GDPR personal data should be minimised, however, AI needs a great amount of data, - and of course an appropriate algorithm - which can contain personal data as well. At first glance it can seem to be a real challenge, but in practice this may not be the case. The key point of the principle of data minimisation that you can only process the personal data you need in accordance with the purpose, so there is no provision in this case, which prohibits processing personal data. The terms "adequate, relevant and limited" are also case specific in the context of AI systems. A number of techniques exist, which can be adopted in order to develop AI systems that process only the data you need, while remaining functional. The individuals accountable for the risk management and compliance of AI systems play a major role in it. [14]

According to Article 5 (1)(d) of the GDPR, personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. It should be noted that it is also necessary to comply with this principle regarding the processing of personal data when using AI systems.

The Information Commissioner's Office, which is the UK's independent authority set up to uphold information rights in the public interest, promoting openness in public bodies and data privacy for individuals, published a guideline that underlines that accuracy in AI refers to how often an AI system fathoms the correct responses, measured against correctly labelled test data. It is important to emphasize that in many contexts, the responses provided by the AI system become personal data. For instance, based on their behaviour on social networking sites an AI system can infer the individuals' demographic information or their interests as well. [14] In this context, it is important to know how the outcome can be examined and checked, if an AI system predicts something regarding an individual, as well as, how misstatements can be detected? Another challenge is the reliability of the systems, it is likely that latency is high on this issue; where applicable, the controllability of how frequently the system makes mistakes, and how this can be measured.

Challenges surrounding AI also include the issue of liability [16], if an injury or any harm occurs "due to a decision of AI", in which case who can be held liable. This issue draws attention to the importance of the need for regulation.

3.3. Face recognition

The concept of face recognition technology is determined according to Berle as: [it] "is a biometric software application designed to identify a specific person in a digital image. This involves the capture of facial biometrics, to create a searchable biometric database of facial images to verify the identity of an individual". [3] It is also important to comply with the aspect of data protection, since data is one of the key elements of it with the self-learning algorithm in AI. This statement is also underlined with real cases from the United States. Last year it came to light that two black men were arrested in the Detroit area due to the mistakes of facial recognition technology. It is known that facial recognition is less accurate for darker-skinned people. However, this technology-based support is widely used by police departments in the United States. [25]

In a new study [23], researchers have established that due to the exploding data requirements of deep learning, requesting the consents of individuals has been abandoned by degrees. A further challenge is related to surveillance and potential discrimination, due to this "practice" more and more personal photos of individuals were incorporated into systems of surveillance without their knowledge. It can cause unforeseeable consequences with these data sets, which may unwittingly comprise photos of minors, use racist and sexist labels, or have poor quality and lighting. [11; 23] One of the legal bases of data processing is the individual's consent, that is the reason why the results of the study draw attention to these new risks, since they can be harmful to fundamental rights.

There is nothing new in the finding that language-generation algorithms can contain racist and sexist ideas. [10] However, based on Steed and Caliskan's new study [27] it can also be true for image-generation algorithms. In a photo of a man cropped right below his neck, he will automatically be dressed in a suit in 43% of the cases by the algorithm. When there is a woman in the cropped photo, it will autocomplete her at a rate of 53% wearing a low-cut top or bikini. These results highlight the importance of this issue, image-generation is just one element, which impacts on all computer-vision applications, for instance, the previously mentioned facial recognition. [10]

From an international perspective, it is worth mentioning the case of China, where facial recognition technology is widely used in parallel with privacy concerns. In October 2019, China had its first lawsuit over the use of facial recognition technology, which was followed by many debates. In line with the changing circumstances, last February, China introduced such facial recognition technology that can identify faces even wearing a mask, but it should be noted with a slightly lower accuracy rate. [18]

3.4. Bias and discrimination

Using AI can pose a number of risks of discrimination, given that it is based on data, moreover AI learns from it, which may be unbalanced and/or reflect discrimination, it may create outputs which have discriminatory impacts on people based on their gender, race, age, health, religion, disability, sexual orientation or other attribute. [14]

It should be noted that the output could lead to discriminatory consequences. At different stages of the process, "the data used to train and test AI systems, as well as the way they are designed, and used, might lead to AI systems which treat certain groups less favourably without objective justification". [14] One approach in the context of big data, underlining the importance of the quality of data, establishes that if the training data reflect existing biases for instance against a minority, the algorithm probably incorporates these biases, which can lead to less auspicious decisions for members of these minority groups. [12] Bias should be interpreted in a broad sense, many types of it can occur. For instance, algorithmic bias, can be experienced when a machine-learning model produces a systematically wrong result. Just as an example of it, bias is a reflection of how the authors of the data algorithm choose to use their data blending methods, practices of model construction, and additionally how results are applied and interpreted. It should be kept in mind that these processes are driven by human judgments. [22]

It is apparent that the field of human resources has changed a lot in recent years, digital transformation has greatly facilitated effectiveness, for instance using AI to help to decide which candidate would be the best for a position. On the other hand, AI-based tools have challenges from the point of view of data protection and discrimination. It is important to emphasize that if the basis

(e.g. data table, data set) is not appropriate, the algorithm will learn from incorrect data, which may cause further biased consequences.

With regard to decision-making based on AI, the importance of the quality and quantity of data should be emphasized, as the results provided by AI depend on all this. This idea brings us to the issue of privacy. As Kaplan and Haenlein wrote: "external data and AI go hand in hand". [16] In this context it should also be underlined that it was pointed out that "[t]he power of AI is driven by the amount of input data present and the performance of algorithms and hardware to learn from such data". [16] The question arises, why all these are so important. The response can be given by a practical example. If AI is biased due to training and processed data, then the outcome will have errors. It should also be mentioned that they might not be noticed at first glance, and it could happen that these errors will only come to light when it is too late, having caused further errors. In 2018, Amazon used an AI Recruitment System for hiring. The algorithm had been built on historical job performance data, when white men had been the best performers in the company. The reason for the biased outcome was that most of the employees were white men and white male candidates were given higher scores by the algorithm and women candidates were discriminated against, even though the sex of the candidates was not used as a criteria. [4; 20] Cappelli et al. highlighted that several questions arise in the case of retrospective analyses applied by algorithms, which can cause biases based on the data set. If this happens it may lead to a disproportionately high selection of white men and discrimination against women candidates in the process of hiring as in the example of Amazon. [4] The programs were edited by Amazon to make them neutral to these particular terms. However, because there was no guarantee that the machines would not devise other ways of sorting candidates that could prove discriminatory, the Seattle company stopped this project. [6]

Avoiding bias also has a key role to play in the field of criminal law, considering the principle of fair trial and non-discrimination. AI can be used for this purpose as well. In this context, an example of good practice can be found in San Francisco, where technology helps the work of prosecutors in avoiding bias. According to the description it is a "blind-charging" tool, which was built by the Stanford Computational Policy Lab, which "removes racial information from police reports when prosecutors are deciding whether to criminally charge suspects". [26]

4. Conclusion and future-related questions

In different areas of life, it has already become apparent what great opportunities AI holds, especially in the case of repetitive tasks, where it can greatly accelerate processes and advance efficiency. However, it should be noted that there are many risks in its use. This paper is focused on the current challenges of it from a data protection point of view, with special regard to compliance with the principle of data minimisation and accuracy of the GDPR, issues of face recognition technology, discrimination and biased outcome. The aforementioned examples underline in practice, the importance of data and the methodology applied in the context of AI, as it includes self-learning algorithm(s). It poses major challenges and can generate serious problems in real life if the self-learning system is not based on the right foundation.

To sum up, the broad sense of personal data also covers the conclusions that can be drawn from it, which is the reason why it is particularly important for AI to focus on data sets and the protection of additional personal data resulting from them. As a self-learning algorithm based on poor foundations can also lead to erroneous conclusions, which is a high risk from the perspective of data protection.

AI may also raise further questions from a data protection perspective for the future as to whether it can take over the humans' personality, combined with inappropriate information, if someone talks to a self-learning AI-powered robot instead of a human being. Moreover, the extent to which it can be substituted.

5. References

[1] ARAUJO, T., HELBERGER, N., KRUIKEMEIER, S., H. DE VREESE, C., In AI we trust? Perceptions about automated decision-making by artificial intelligence, AI & Society 35, 611-623, 2020.

[2] BATHAEE, Y., The Artificial Intelligence Black Box and the Failure of Intent and Causation, Harvard Journal of Law & Technology, 31 (2), 889-938, Spring 2018.

[3] BERLE, I., Face Recognition Technology. Compulsory Visibility and Its Impact on Privacy and the Confidentiality of Personal Identifiable Images, Law, Governance and Technology Series 41, 2, Springer, 2020.

[4] CAPPELLI, P., TAMBE, P., YAKUBOVICH, V., Artificial Intelligence in Human Resources Management: Challenges and a Path Forward, 1-34, April 8, 2019. (Retrieved from https://ssrn.com/abstract=3263878 – 13. 02. 2021.)

[5] CRAWFORD, K., SCHULTZ, J., Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, in: Boston College Law Review 93 (55), 93-128, 2014. (Retrieved from http://lawdigitalcommons.bc.edu/bclr/vol55/iss1/4 – 15. 02. 2021.)

[6] DASTIN, J., Amazon scraps secret AI recruiting tool that showed bias against women, Reuters, October 11, 2018. (Retrieved from https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G – 28. 03. 2021.)

[7] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA), Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights, Publications Office of the European Union, 1-18, 2019. (Retrieved from https://fra.europa.eu/sites/default/files/ fra_uploads/fra-2019-data-quality-and-ai_en.pdf – 25. 03. 2021.)

[8] EUROPEAN COMMISSION, White Paper on Artificial Intelligence - A European approach to excellence and trust, Brussels, 1-26 February 19, 2020. (Retrieved from https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb 2020_ en.pdf – 20. 01. 2021.)

[9] GPT-3 (OpenAI's language generator), A robot wrote this entire article. Are you scared yet, human?, in: The Guardian, September 8, 2020. (Retrieved from https://www.theguardian. com/commentisfree/2020/sep/08/robot-wrote-this-article-gpt-3 – 25. 01. 2021.)

[10] HAO, K., An AI saw a cropped photo of AOC, It autocompleted her wearing a bikini, in: MIT Technology Review, January 29, 2021. (Retrieved from https://www.technology review.com/2021/01/29/1017065/ai-image-generation-is-racist-sexist/ – 17. 02. 2021.)

[11] HAO, K., This is how we lost control of our faces, in: MIT Technology Review, February 5, 2021. (Retrieved from https://www.technologyreview.com/2021/02/05/1017388/ai-deep-learning-facial-recognition-data-history/ – 17. 02. 2021.)

[12] HARDT, M., How big data is unfair, in: Medium, September 26, 2014. (Retrieved from https://medium.com/@mrtz/how-bigdata-isunfair-9aa544d739de – 14. 02. 2021.)

[13] HILDEBRANDT, M., KOOPS, BJ., The Challenges of Ambient Law and Legal Protection in the Profiling Era, in: Modern Law Review, 73 (3), 428-460, May 7, 2010. (Retrieved from https://onlinelibrary.wiley.com/doi/full/10.1111/j.1468-2230.2010.00806.x – 18. 02. 2021.)

[14] INFORMATION COMMISSIONER'S OFFICE, Guidance on AI and data protection, July 30, 2020. (Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protect ion-themes/guidance-on-artificial-intelligence-and-data-protection/ – 10. 02. 2021.)

[15] ISHII, K., Comparative legal study on privacy and personal data protection for robots equipped with artificial intelligence: looking at functional and technological aspects, in: AI & Society, 34, 509-533, 2019.

[16] KAPLAN, A., Haenlein, M., Rulers of the world, unite! The challenges and opportunities of artificial intelligence, in: Business Horizons 63 (1), 37-50, 2020.

[17] KAPLAN, A., Haenlein, M., Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence, in: Business Horizons 62 (1), 15-25, 2019.

[18] LEE, S., Coming into Focus: China's Facial Recognition Regulations, Center for Strategic & International Studies, May 4, 2020. (Retrieved from https://www.csis.org/blogs/trustee-china-hand/coming-focus-chinas-facial-recognition-regulations – 27. 03. 2021.)

[19] MCCARTHY, J., MINSKY, M. L., ROCHESTER, N., SHANNON, C. E., A proposal for the Dartmouth summer research project on artificial intelligence, 1955. (Retrieved from http://www-formal .stanford.edu/jmc/history/dartmouth/dartmouth.html – 20. 01. 2021.)

[20] MEYER, D., Amazon Reportedly Killed an AI Recruitment System Because It Couldn't Stop the Tool from Discriminating Against Women, in: Fortune. October 10, 2018. (Retrieved from https://fortune.com/2018/10/10/amazon-ai-recruitment-bias-women-sexist/ – 16. 02. 2021.)

[21] MIHAJLOVIC, I., How Artificial Intelligence Is Impacting Our Everyday Lives - And How You Already Encounter It Every Day, June 13, 2019. (Retrieved from https://towardsdatascience.com/how-artificial-intelligence-is-impacting-our-everyday-lives-eae3b63379e1 – 26. 03. 2021.)

[22] NELSON, G., S., Bias in Artificial Intelligence, North Carolina Medical Journal, 80 (4), 220-222, July 5, 2019.

[23] RAJI, I. D., FRIED, G., About Face: A Survey of Facial Recognition Evaluation, Presented at AAAI 2020 Workshop on AI Evaluation, 1-11, February 1, 2021. (Retrieved from https:// arxiv.org/pdf/2102.00813.pdf – 16. 02. 2021.)

[24] 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) Official Journal of the European Union | L 119/1.

[25] RYAN-MOSLEY, T., Why 2020 was a pivotal, contradictory year for facial recognition, in: MIT Technology Review, December 29, 2020. (Retrieved from https://www.technology review.com/2020/12/29/1015563/why-2020-was-a-pivotal-contradictory-year-for-facial-recognition/ – 17. 02. 2021.)

[26] SERNOFFSKY, E., SF DA Gascón launching tool to remove race when deciding to charge suspects, in: San Francisco Chronicle, June 12, 2019. (Retrieved from https://www.sf chronicle.com/crime/article/SF-DA-Gasc-n-launching-tool-to-remove-race-when-13971721.php – 15. 01. 2021.)

[27] STEED, R. and CALISKAN, A., Image Representations Learned With Unsupervised Pre-Training Contain Human-like Biases, 1-15, January 27, 2021. (Retrieved from https://arxiv.org/ pdf/2010.15052.pdf – 16. 02. 2021.)

[28] STATISTA, Number of monthly active Facebook users worldwide as of 4th quarter 2020, January 2021 (Retrieved from https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ – 26. 03. 2021.) 2,797 billion monthly active Facebook users worldwide.

[29] TODOLÍ-SIGNES, A., Algorithms, Artificial Intelligence and Automated Decisions Concerning Workers and the Risks of Discrimination: The Necessary Collective Governance of Data Protection, June 30, 2018, in: Transfer: European Review of Labour and Research, 25 (4), 1-17, 2019. (Retrieved from https://ssrn.com/abstract=3316666 – 15. 01. 2021.)

[30] UNITED STATES, Supreme Court of Wisconsin, State of Wisconsin v. Eric L. Loomis, No. 2015AP157– CR, July 13, 2016. (para 100)

[31] VAISHYA, R., JAVAID, M., HALEEM KHAN, I. and HALEEM, A., Artificial Intelligence (AI) applications for COVID-19 pandemic, in: Diabetes & Metabolic Syndrome: Clinical Research & Reviews, 14 (4), 337-339, 2020.

[32] WALDMAN, H., Dictionary of robotics, Collier Macmillan, 1985.

[33] ZHANG, Q., LU, J., JIN, Y., Artificial intelligence in recommender systems, Complex & Intelligent Systems, 7, 439-457, 2021. (Retrieved from https://link.springer.com/content/pdf/ 10.1007/s40747-020-00212-w.pdf – 27. 03. 2021.)