SECURITY AND DATA PROTECTION IN ARTIFICIAL INTELLIGENCE

Marko MARKOVIĆ[1*], Dragan SOLEŠA[2]

[1]University Business Academy in Novi Sad, Faculty of Applied Management, Economics and Finance, Belgrade, Serbia, marko.markovic@mef.edu.rs
[2]University Business Academy in Novi Sad, Faculty of Economics and Engineering Management, Novi Sad, Serbia, dragan.solesa@fimek.edu.rs

Abstract: *The development of artificial intelligence contributes to the digital transformation of the entire society, improving numerous processes, automation and better decision-making. In addition to the many opportunities it offers, it also brings with it great risks in data security. The problem is further complicated by unauthorized access to data processed by artificial intelligence models, data theft, ethical dilemmas and lack of algorithm transparency. This paper analyzes artificial intelligence through different fields and the problems it can cause. A special emphasis is on the research into user attitudes, which shows us what kind of knowledge respondents have about artificial intelligence and all the risks it can cause. The results help us to see what the biggest problems regarding the use of such models are. The work provides guidelines for minimizing risks and creating problems, while dictating the trend for responsible use of artificial intelligence for legally correct purposes.*

Keywords: *Artificial intelligence, data security, ethical dilemmas, transparency of algorithms, security aspects*

Type of paper: Original scientific paper
Received: 15.05.2025
Accepted: 19.06.2025
Available online: 22.06.2025
DOI: 10.5937/jpmnt13-58872

1. Introduction

Data is the greatest asset of today, upon which all processes, activities, and jobs depend. Data sources are varied, often intended to manipulate information and confuse the end user when making decisions. Since every piece of data is very important to the organization, it must carefully and with the utmost integrity safeguard that data from various influences or third parties. In addition to this, it is important that the data be stored in secure databases that are adequately protected from unauthorized access or modification. Modified data that loses its quality can have a significant impact on social and economic activities, so companies must focus on the accuracy of their data when selecting it for decision-making (Wang & Strong, 1996). In the current era of artificial intelligence, attention must be paid to data security and its impact on artificial intelligence models. If we give a model access to learn from our data that may be of

[*] Corresponding author

significant importance to our business, we call into question the fact that the artificial intelligence model could compromise that data.

Artificial intelligence is not a concept that has only been known in the past few years; it actually dates back to the mid-19th century. To test the operation of machines and their automation in the process, Turing devised the algorithm "Computing Machinery and Intelligence." Turing aimed to demonstrate how a machine could respond like a human, thereby confusing the user in the process. The test was conducted in such a way that one user communicated with a machine that could be a program or a computer. The examiner, by asking questions, must discern which responses are given by a human and which by a machine. Through a terminal or another means, the examiner communicates and tries to determine who is providing the answer on the other side (Castelfranchi, 2013). Today, we can observe this kind of test in artificial intelligence tools, which, when providing answers, try to imitate human speech and thus bring the user all the necessary information they require. Due to its capabilities, speed, and manner of responding, users consider it productive because it boosts their motivation. While another part of this tool is seen as entertainment (Brandtzaeg & Følstad, 2017).

In the region of Western Europe and America, job openings are emerging for query engineers who know how and in what way they can obtain all the necessary information from artificial intelligence by sending accurate and precise queries to a tool. It also states that all administrative tasks performed by humans can be done significantly faster and more easily by artificial intelligence.

With the popularization of this field, there are tools that can be used in every sector of the economy. This tells us that these models have a very wide range of applications and that the algorithms adapt very quickly to specific user requirements. We most often encounter artificial intelligence in one of the following areas:

Computing, as the home of artificial intelligence, is actually the most popular place where artificial intelligence models are used. Given that this field is rapidly evolving, it serves as a solid foundation for the development of machine learning and natural language processing. We can observe that artificial intelligence has rapidly developed and been implemented in smart devices, web browsers, social networks, and personal assistants in a way that enhances the performance of these systems, personalization, and speed (Niskanen et al., 2023). But it's not all that simple, as evidenced by the fact that the use and processing of data, which often comes from various disorganized sources, leads to an increasing application of unsupervised learning that is becoming more significant and applicable. We come back to the algorithms that are updated and improved by solving each of these problems using predictive techniques. In order to use such models seamlessly, a high level of data security is required for the data used in predictive techniques; this way, artificial intelligence will be able to have a safe and broad application (Niskanen et al., 2023).

Through trend prediction techniques, credit risk assessment, or trade automation, artificial intelligence can also be found in the financial sector. Machine learning analyzes large amounts of data, which can include user behavior and consumption patterns, allowing for a very precise assessment of users' creditworthiness (Cao, 2021). It has also proven effective in fraud detection, using advanced techniques to identify the potential for user fraud. It detects all unusual changes in real time that are not the result of consumer activity (Danielsson et al., 2023). However, although these are all the benefits that artificial intelligence offers, it can also bring challenges in terms of algorithm transparency, which significantly affects the level of trust among end users and regulatory bodies (Zheng et al., 2018).

A key role in the modernization and improvement of medicine is played by artificial intelligence, which uses algorithms for diagnostic techniques and the early detection of certain diseases. Machine learning analyzes medical data from patient records in detail and with great precision, enabling highly reliable analysis and subsequently more effective patient treatment (Esteva et al., 2019). It has proven effective in analyzing medical findings where algorithms have surpassed human capabilities in detecting certain patient conditions, some of which include melanoma and pneumonia (Topol, 2019). In addition to diagnostics, it enables advancements in the analysis of genetic data, allowing therapies to be tailored to the specific needs of patients (Rajpurkar et al., 2018).

With the increasing application of artificial intelligence, there are also issues arising regarding the security of user data. Data security is the process of protecting all the data owned by an individual, system, or company in order to prevent that data from leaving its initial environment through any method or means that could misuse that data. A lack of data protection leads to security risks that can undermine data privacy and compromise it. As noted in their research, privacy and data encryption are the only means to ensure that data remains secure (Shokri & Shmatikov, 2015). Data that leaves systems often ends up as a commodity. We must adequately educate ourselves about the importance of data protection and how to properly safeguard ourselves, our data, and all our digital assets.

Every piece of data is sensitive and can cause significant harm to a company or user. In addition to business data, it is important to pay attention to personal data, which should not be entered into artificial intelligence systems. It often happens that the privacy policy of a certain platform specifies how data is handled, but users skip over that information and do not pay attention to how their data will be treated in that system. In the process of solving certain tasks, these models retain all the input data and analyze it during communication, but what happens to that data after the session ends? The data remains as a tool for training such models. Since they are capable of processing large amounts of data, there is a possibility that the same data could be misused. A key challenge is ethics, as it calls into question moral principles and programming. There are two principles regarding ethical norms in this case, and these models most often rely on them. The "top-down" model implements predefined ethical norms into the model itself and thus sets a standard, while the "bottom-up" model does the opposite and tries to learn through observing the user and their behavior towards the model in terms of ethics and morality. Both models face the same issue, which is the very philosophy that guides them in their moral principles and moral reasoning when considering human demands. (Etzioni, 2017). That's why there is a "bot ethics" that does not rely on machine ethics, but rather exclusively transfers human moral patterns of behavior onto itself.

To avoid complications with data, it is necessary to store it properly. Companies must protect their business and their data during communication and transfer to any of the artificial intelligence models. It is necessary to use protective protocols such as Transport Layer Security (TLS) and Secure Sockets Layer (SSL). End-to-end encryption is essential for data transmission, ensuring that the data we send to the algorithm will be protected. There are several essential measures we can implement to avoid unwanted data loss:

A secure data warehouse represents a secret and highly secure location where all data is stored. It is necessary to implement certain mechanisms that would detect undesirable factors and threats for better protection.

Access control provides an additional layer of data protection in artificial intelligence systems. Access control mechanisms use special algorithms that dynamically adjust access permissions and privileges within systems, thereby reducing the risks associated with data access (Kandolo, 2024).

The greatest attention should be paid to information systems that have implemented some form of artificial intelligence tools for their automation and process acceleration. It is necessary to analyze the algorithm that the tool uses before its actual implementation in any of the information systems.

2. Methodology

Artificial intelligence models have become a part of everyday life, and it is becoming unimaginable not to use them in daily business operations. However, the most important factor of security is given the least significance, and very often we grant these models access to all data. It is essential to thoroughly research the model before using it and to approach it in a way that ensures the privacy of all entered data during communication. The model's privacy policy indicates whether the models adhere to data protection and ethical codes, so it is necessary to research the model's documentation before using it. As we live in a time where it is very important for us to obtain all the necessary information in the shortest possible time, we must first familiarize ourselves with the tool that will shorten the execution time of the process.

Table 1. Basic characteristics of students and their answers to research questions (in %)

Variable	Category	Frequencies	Percentage	Average value
Gender	Male	112	59.9	
	Female	75	40.1	
AI model usage time				2.75
Scientific field	IT	93	49.7	
	Management	60	32.1	
	Economics	34	18.2	
Are you familiar with artificial intelligence?	Yes, completely	60	32.1	
	Partially	90	48.1	
	No	37	19.8	
Experience in using artificial intelligence	Yes	117	62.6	
	No	70	34.7	
Do you think that the artificial intelligence tool you use should be implemented in information systems?	Yes	94	50.3	
	No	56	29.9	
	I'm not sure.	37	19.8	

Source: Author’s research

For the purposes of this work, a survey was conducted at the Faculty of Applied Management, Economics, and Finance. The survey serves as the primary instrument of the research, structured in the form of a questionnaire divided into two parts.

In the first part, respondents answered questions that presented the control variables of the research (gender structure, duration of use of any artificial intelligence models, the scientific field they belong to, whether they are familiar with artificial intelligence, which models or tools of artificial intelligence they have used, their experience in using artificial intelligence, and whether they believe that the artificial intelligence tool they use should be implemented in information systems).

In the second part of the research, fifteen questions were formulated using a Likert scale. These questions relate to the impact of artificial intelligence, with a particular emphasis on its usefulness and safety. It examines how it contributes to efficiency and automation, as well as what the potential risks are. Particular importance is given to protective measures, algorithm transparency, and user education to ensure safe and responsible application.

The target group of this research consisted of undergraduate students who are the most frequent users of such models. A sample of 187 respondents was selected. From the total sample of respondents, we can determine the following control variables: 59.9% of the respondents are men, while a slightly smaller percentage, 40.1%, are women. The respondents also indicated how much they use artificial intelligence tools daily, and we see that it averages 2.75 hours per day. The vast majority of respondents are partially familiar with it at 48.1%, while a further 32.1% of respondents are familiar with artificial intelligence. A significantly smaller percentage, 37 of them, are not familiar with artificial intelligence. Experience in using artificial intelligence was reported by 50.3% of respondents who mentioned some of the popular artificial intelligence models (ChatGPT, Copilot, Google AI…).

3. Results and discussion

This paper explores students' attitudes toward the perceived usefulness and data security in artificial intelligence. Special emphasis is placed on analyzing the factors that influence the use of artificial intelligence, including the most important aspects of data security and protection, decision-making efficiency, and the automation of business processes. Additionally, the goal is to examine the factors that influence students' attitudes toward the application of artificial intelligence in information systems, along with the motivation and determination of respondents to use artificial intelligence in a professional environment.

Table 2. Results of factor analysis and reliability analysis

Items		F1	F2	F3
	Cronbach's alpha	0.802	0.830	0.779
Artificial intelligence enables more efficient analysis of large data sets by tracking and evaluating		0.802		
Artificial intelligence makes it possible to improve processes and decision-making		0.785		
Artificial intelligence helps detect security threats within an information system		0.753		
The implementation of artificial intelligence contributes to the automation of processes performed by humans		0.718		
Artificial intelligence tools increase productivity in business and reduce time to perform certain processes		0.703		
There is a risk of unauthorized access to data processed by artificial intelligence within the system			0.823	
Transparency of AI algorithms is key to end-user trust			0.798	
AI tools/models must be compliant and trained to comply with legal regulations			0.782	
Insufficient data protection in artificial intelligence tools erodes user trust in them			0.765	
Cryptographic techniques (data encryption) should be standard practice in artificial intelligence			0.742	
Access to artificial intelligence systems should be restricted to authorized users only				0.801
Artificial intelligence models need to be updated regularly				0.778
Data access control is a key measure in artificial intelligence				0.764

Artificial intelligence models should have ethical guidelines implemented	0.741
User education about security risks in artificial intelligence is needed	0.728

Source: Author's research

When determining the dimensionality of the data, factor analysis of the data was used (Table 2). The relevance of the sample was tested using the Kaiser-Meyer-Olkin (KMO) indicator, which in this case was 0.842, which exceeds the recommended relevance value of 0.7. Also, Bartlett's sphericity test is statistically significant (χ^2 (105) = 1245.67, p < 0.001), which means that the correlation matrix is suitable for factor reduction. The factors were extracted using the method of principal components (Đurica & Soleša, 2017), and the varimax technique was used for their rotation. Based on the Scree plot, the number of dimensions and latent factors was determined using eigenvalues greater than 1 (according to the Kaiser criterion).

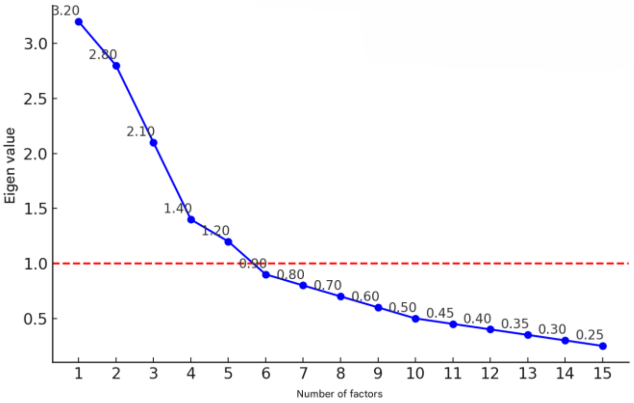

Figure 1. Scree diagram

Source: Author's research

The values of Cronbach's alpha indicate the internal consistency of the scales, as all three values for the factors are above 0.7 (0.802, 0.830, 0.779), which suggests good reliability of the factors and that the items comprising each of the dimensions are interrelated.

Table 3. Descriptive statistics of items associated with the three obtained factors (n=187)

Items	Average value	Median	Standard Deviation
F1: Perceived usefulness			
Artificial intelligence enables more efficient analysis of large data sets by tracking and evaluating	3.92	4.00	0.96
Artificial intelligence makes it possible to improve processes and decision-making	3.86	4.00	0.93
Artificial intelligence helps detect security threats within an information system	3.81	3.00	0.91
The implementation of artificial intelligence contributes to the automation of processes performed by humans	3.68	3.00	0.87
Artificial intelligence tools increase productivity in business and reduce time to perform certain processes	3.73	4.00	0.94
F2: Security aspects of artificial intelligence			
There is a risk of unauthorized access to data processed by	4.12	4.00	0.86

artificial intelligence within the system			
The transparency of AI algorithms is key to end-user trust in remote locations and at any time	4.07	4.00	0.82
AI tools/models must be compliant and trained to comply with legal regulations	4.03	4.00	0.83
Insufficient data protection in artificial intelligence tools erodes user trust in them	4.01	3.00	0.79
Cryptographic techniques (encrypting data) should be standard practice in artificial intelligence	3.97	3.00	0.81
F3: Organization of access and security measures of artificial intelligence			
Access to artificial intelligence systems should be restricted to authorized users only	3.82	4.00	0.89
Artificial intelligence models need to be updated regularly	3.87	3.00	0.90
Data access control is a key measure in artificial intelligence	3.76	3.00	0.91
Artificial intelligence models should have ethical guidelines	3.70	3.0	0.88
Education about security risks in artificial intelligence	3.80	3.00	0.90

Source: Author's research

In the second part of the research, the questions served as an instrument for examining students' attitudes about the impact of artificial intelligence and aspects of its usefulness and safety. This table presents the calculated descriptive statistical dimensions for this part of the research.

For the first factor, Perceived Usefulness, we observe the highest score for the item "Artificial intelligence enables more efficient analysis of large data sets through monitoring and evaluation" (M=3.92, SD=0.96) and "Artificial intelligence allows for the improvement of processes and decision-making" (M=3.86, SD=0.93). According to this analysis, we can determine that the main advantages of artificial intelligence are the ability to analyze large amounts of data and the improvement of decision-making, which essentially means that the algorithm will continuously make decisions based on the processed data sets.

For the second factor, the security aspects of artificial intelligence, we can conclude that the following stands out: "There is a risk of unauthorized access to the data processed by artificial intelligence within the system" (M=4.12, SD=0.86) and "The transparency of artificial intelligence algorithms is crucial for trust among end users in remote locations and at any time" (M=4.12, SD=0.86). The results confirm that a large number of respondents agree that unauthorized access to data and the transparency of algorithms regarding security are very important. Data privacy is the most important segment, as users do not want these models to share their data with third parties. In algorithms, the bias of the parties and the methodology by which they make decisions are crucial (the most important aspect of the decision-making process).

For the third factor, Organization of access and security measures for artificial intelligence, the following statements stand out: "It is necessary to regularly update artificial intelligence models" (M=3.87, SD=0.90) and "Access to artificial intelligence systems should be restricted to authorized users only" (M=3.82, SD=0.89).

Table 4. Reasons for using and not using artificial intelligence

Items	Number of respondents	Percentage based on responses	Percentage based on respondents
Artificial intelligence allows me to automate my processes	98	18.4	52.4
Artificial intelligence increases the accuracy of the analysis of my data sets	85	15.9	45.4
In the process of making a decision, artificial intelligence helps me with its suggestions	80	15.0	42.8
Artificial intelligence can reduce operational costs	70	13.1	37.4
I get personalized recommendations that allow me to test multiple hypotheses	65	12.2	34.8
I am concerned about the privacy of my data	75	14.1	40.1
I believe that the lack of transparency of algorithms can create a problem for users	60	11.3	32.1
In total	533	100.0	285.0

Source: Author’s research

The table presents the results of the question "Reasons for using and not using artificial intelligence?" A total of 153 respondents (out of 187 respondents) answered the question, which constitutes a sample of 82%. The question allowed for multiple-choice answers. The table shows the percentages of responses divided into two categories: the percentage based on responses and the percentage based on respondents. Our 153 respondents provided a total of 533 answers.

We observe that the largest number of respondents, 52.4%, indicated that process automation is the reason for using artificial intelligence. This trend shows that this technology has gained significant popularity among all target groups. Additionally, 45.8% believe that artificial intelligence increases the accuracy of data analysis, indicating that machine learning algorithms and advanced predictive techniques are doing a good job in decision-making. Another significant indicator is that 42.8% of respondents see improved decision-making as a key advantage of artificial intelligence. On the other hand, 40.1% of respondents expressed concerns about data privacy, highlighting the challenges related to information security and ethical use.

Table 5. The results of the study of the influence of gender on the factors obtained from the research

Factors	Gender	n	Average value	Standard deviation	df	t	*p*
F1- Perceived usefulness	Male	112	4.05	0.951	185	2.50	0,01*
	Female	75	3.80	1.00			
F2- Security aspects	Male	112	4.10	0.801	185	1,20	0.23
	Female	75	3.94	0.854			
F3 – Organization of access and security measures	Male	112	3.90	0.902	185	1,50	0,14
	Female	75	3.70	0.955			

Source: Author’s research

The table shows the mean values and standard deviations for each dimension based on the gender of the respondents. In the further analysis of the data, the results of the analysis of variance (ANOVA) were also used to explore differences in the perception of usefulness, safety, and access organization based on various demographic factors, including gender. The table below presents the results of the t-test examining the impact of gender on the perception of these factors. The results show that there is a statistically significant difference in the perceived usefulness of artificial intelligence between genders (t(185) = 2.50, p = 0.01). Male respondents rated it slightly higher on average. The other two factors related to security aspects and organizational access do not show a significant difference.

4. Conclusion

Modern trends show that artificial intelligence is being increasingly applied, and there is hardly anyone who hasn't heard of the term. There is a massive expansion in the use of artificial intelligence models and an adaptation to their use for the purpose of facilitating various tasks. When it comes to security, we need to be cautious in our usage because we don't know how our entered data will be handled. It happens that users assign the writing of confidential business reports, providing all business data. These sessions can be compromised, and someone may still gain access to them (Shokri & Shmatikov, 2015). We can't stay on the sidelines for much longer, because artificial intelligence has gained significant momentum in society and technology. Unfortunately, we must slowly get used to the presence and increasingly widespread use of such models. Practice shows that, alongside large companies, smaller startup companies are launching their own systems and models of artificial intelligence for specific tasks. As the time for the widespread application of artificial intelligence approaches, we simply need to learn how to cope with it and be mindful of the data we provide to it. What we have is unpredictable logic that we can and must use, and these models have a couple of algorithms created by human beings. The research we conducted showed that our respondents are familiar with the concept of security, and if all other users become similarly informed, a community can be built that can influence changes in artificial intelligence.

The research conducted in this study showed that respondents recognize the usefulness of artificial intelligence, most often in analyzing large amounts of data and improving decision-making. We can conclude this because these two items received the highest ratings in the factor analysis (M=3.92 and M=3.86), which confirms that respondents recognize the advantages of artificial intelligence. On the other hand, when we analyze data security, we conclude that respondents are most concerned about unauthorized access to data (M=4.12) and the transparency of algorithms (M=4.07). Furthermore, the results showed that there is a statistically significant difference in perceived usefulness between genders, with male respondents rating the usefulness of artificial intelligence higher (t(185) = 2.50, p = 0.01). This difference may indicate disparities in the level of technology use or access to modern tools between genders.

Respondents recognize the potential of artificial intelligence, but they also express concern for the security of their data. This highlights the need for user education and the implementation of legal and regulatory frameworks to ensure the responsible development and application of artificial intelligence.

References

Brandtzaeg, P. B., & Følstad, A. (2017). Why do people use chatbots? Internet Science, 377–392. https://doi.org/10.1007/978-3-319-70284-1_30

Cao, L. (2022). AI in finance: Challenges, techniques, and opportunities. ACM Computing Surveys, 55(3), 1–38. https://doi.org/10.1145/3502289

Castelfranchi, C. (2013). Alan Turing's "Computing Machinery and Intelligence". Topoi, 32(2), 193–199. https://doi.org/10.1007/s11245-013-9182

Danielsson, J., Macrae, R., & Uthemann, A. (2019). Artificial intelligence and systemic risk. SSRN Electronic Journal, 1–9. https://doi.org/10.2139/ssrn.3410948

Diligenski, A., Prlja, D., & Cerović, D. (2018). Pravo zaštite podataka. Institut za uporedno pravo.

https://www.rts.rs/magazin/tehnologija/5208016/cetbot-zanimanja-vestacka-inteligencija-radna-mesta.html (29.01.2025)

Đurica, N., & Soleša, D. (2017). Percepcija i stavovi studenata prema obrazovanju na daljinu. Ekonomija: teorija i praksa, 10(3), 1–15. https://doi.org/10.5937/etp1703001D

Esteva, A., Kuprel, B., Novoa, R. A., Ko, J., Swetter, S. M., Blau, H. M., & Thrun, S. (2019). Dermatologist-level classification of skin cancer with deep neural networks. Nature, 542(7639), 115–118. https://doi.org/10.1038/nature21056

Etzioni, A., & Etzioni, O. (2017). Incorporating ethics into artificial intelligence. The Journal of Ethics, 21(4), 403–418. https://doi.org/10.1007/978-3-319-69623-2_15

Kamaruddin, S., Mohammad, A. M., Mohd Saufi, N. N., Wan Rosli, W. R., Othman, M. B., & Hamin, Z. (2023). Compliance to GDPR data protection and privacy in artificial intelligence technology: Legal and ethical ramifications in Malaysia. 2023 International Conference on Digital Transformation (ICDT), Greater Noida, India, 11–12 May 2023, 11–12. https://doi.org/10.1109/ICDT57929.2023.10150615

Kandolo, W. (2024). Ensuring AI data access control in RDBMS: A comprehensive review. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) Workshops, 8400–8407.

Martinelli, F., Marulli, F., Mercaldo, F., Marrone, S., & Santone, A. (2020). Enhanced privacy and data protection using natural language processing and artificial intelligence. 2020 International Joint Conference on Neural Networks (IJCNN), Glasgow, UK, 19–24 July 2020, 1–8. https://doi.org/10.1109/IJCNN48605.2020.9206801

Mitrou, L. (2018). Data protection, artificial intelligence and cognitive services: Is the General Data Protection Regulation (GDPR) "artificial intelligence-proof"? SSRN, 1–10. https://doi.org/10.2139/ssrn.3386914

Niskanen, T., Sipola, T., & Väänänen, O. (2023). Latest trends in artificial intelligence technology: A scoping review. JAMK University of Applied Sciences, 1–26. https://doi.org/10.48550/arXiv.2305.04532

Rajpurkar, P., Irvin, J., Ball, R. L., Zhu, K., Yang, B., Mehta, H., et al. (2018). Deep learning for chest radiograph diagnosis: A retrospective comparison of the CheXNeXt algorithm to practicing radiologists. PLoS Medicine, 15(11), e1002686. https://doi.org/10.1371/journal.pmed.1002686

Sartor, G., & Lagioia, F. (2020). The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. European Parliament, Brussels. https://doi.org/10.2861/293

Shokri, R., & Shmatikov, V. (2015). Privacy-preserving deep learning. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS), 1310–1321. https://doi.org/10.1145/2810103.2813687

Topol, E. J. (2019). High-performance medicine: The convergence of human and artificial intelligence. Nature Medicine, 25(1), 44–56. https://doi.org/10.1038/s41591-018-0300-7

Wang, R. Y., & Strong, D. M. (1996). Beyond accuracy: What data quality means to data consumers. Journal of Management Information Systems, 12(4), 5–33. https://doi.org/10.1080/07421222.1996.11518099

Zha, D., Bhat, Z. P., Lai, K.-H., Yang, F., Jiang, Z., Zhong, S., & Hu, X. (2024). Data-centric artificial intelligence: A survey. ACM Computing Surveys. https://doi.org/10.1145/3711118

Zheng, X., Zhu, M., Li, Q., Chen, C., Tan, Y., & Hide. (2018). FinBrain: When finance meets AI 2.0. arXiv, 1–12. https://doi.org/10.48550/arXiv.1808.08497