



INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL
ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

WHITE BLACK
LEGAL

EDITORIAL **TEAM**

Raju Narayana Swamy (IAS) Indian Administrative Service **officer**



Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru

and a professional diploma in Public Procurement from the World Bank.

diploma in Public

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.



Senior Editor

Dr. Neha Mishra



Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.



Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.



Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM

Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.

More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

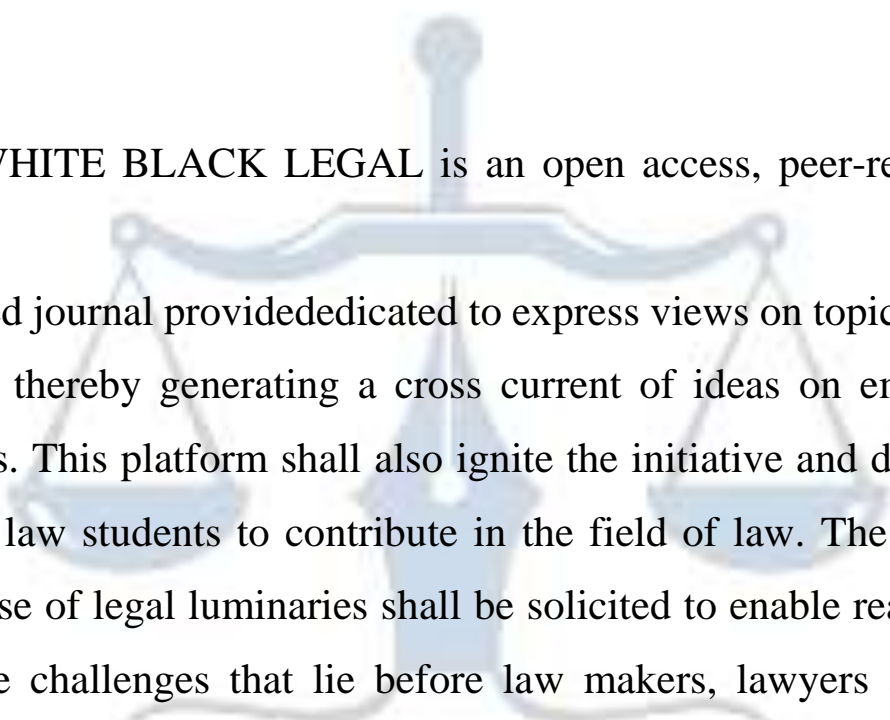


Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US



WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

USE OF AI IN CYBER SECURITY - DIGITAL AGE

AUTHORED BY - MR. ABHISHANK KUMAR

BBA LLB (Honours)

School of Law, Christ University, Lavasa Campus, Pune – 412112,
Maharashtra, India.

Abstract

Artificial intelligence (AI) is an indispensable part of the cybersecurity equation, helping to provide solutions for complex digital threats. In this research paper, the authors explore the importance of the role of AI in cybersecurity in three key areas, including social media, banking and medical sciences. AI-powered tools are used on social media platforms to identify and reduce cyber threats like misinformation, phishing, data breaches, and other malicious attempts, in addition to enhancing user safety by enhancing content moderation. Nevertheless, the widespread adoption of AI to track what we do in the world creates a privacy crisis of its own, complete with algorithmic biases and the potential for surveillance. AI has actually changed the banking sector by automating fraud detection, monitoring transactions, and improving customer authentication through methods such as biometric verification. Even so, the sophistication of AI-assisted cybercrime poses major threats to financial institutions and, as a result, strong security protocols are essential. AI is not only keeping most sensitive patient data safe, but it is also making interconnected healthcare systems less vulnerable to cyberattacks while simultaneously improving accuracy in diagnosis and operational efficiency in the arena of medical sciences. But these systems are threatened by this reliance on these networked infrastructures and the ability to overtake their data integrity. This paper discusses the opportune and non-opportune uses of AI in these areas and the best practices for developing fair policies, explainable algorithms, strong, and effective regulatory measures for embracing the potential of AI, together for a safer digital future.

Keywords: Artificial Intelligence, Cybersecurity, Social Media, Banking, Medical Sciences, Fraud Detection, Data Privacy, Ethical AI, Regulatory Frameworks, Digital Threats.

1.0 Introduction

From communication and commerce to healthcare and entertainment, the evolution of technology has changed nearly every facet of human activity in the digital age. But such a transformation has led to our dependence on connected systems massively increasing, and Cyber Security has become a vital element that should concern individuals, organizations and governments alike. The complexity and scale of cyber threats have changed, with cyber attackers using advanced tactics to target vulnerabilities. With conventional security mechanisms unable to cope, Artificial Intelligence (AI) entered the scene, transforming the methodology that powers threat detection, avoidance and prevention.

Cybersecurity is among the fields where AI has a two-way impact. It provides systems with the advantage of analysing large quantities of data, spotting anomalies and dealing with threats in real time. On the other hand, also offers another approach for the attackers in order to use the AI for performing more complex cyber-attacks. The fact that AI has both the potential to enhance and threaten digital security has now placed it as a focus of research and development across many industries.

AI possesses immense power in all domains, but in the present paper, we explore its utility in the domains of social media → spanning privacy, misinformation → and domain of banking and domain of medical sciences → of course, these three domains are critical domains that are being drastically impacted due to digital transformation. Social media platforms which billions of users across the world connect to, were been targeted for phishing, misinformation and data breaches. In Content moderation, User Authentication, and Anomaly detection, AI is a critical component to enable them, hence maintaining a safer online environment. Due to the risk involved in banking, where financial assets and sensitive data are at stake, AI detects fraud, monitors transactions and improves the authentication system of various banking applications on all these banking solutions AI is very effective in the long term. On the flip side of this development, the complexity involved behind the functional side of AI provides additional layers towards adaptive malware and phishing schemas that are likely to break the resolve of even the strongest security systems available.

AI has become integrated into diagnostics, treatment planning and patient care in the medical sciences with a focus on reliance on networks and big data. However, this same level of

connectivity exposes our healthcare organizations to cyber threats, and if breached, patient information is compromised, and essential functions are at risk. Of course, applying anomaly detection and predictive analytics for cybersecurity purposes is already a very useful direction underway, but these methods present ethical and regulatory issues that cannot be dismissed.

In this paper, through a detailed consideration of these domains, the author will demonstrate both the potential and the issues presented by AI in the context of cyber security. He argues the tide requires the greatest command to grasp how something should work so that we find the most benefit from it. And that brings us to the end in which we stress the need for transparency and accountability as well as interdisciplinary collaboration to address the diversity of conditions in which AI is applied to cybersecurity in the digital age.

2.0 AI in Social Media

Even cyber security has greatly improved due to the introduction of AI applications and solutions to serve social media platforms. Social media, the epicenter of communication across the globe, is inundated with AI-driven advanced mechanisms to solve the problems of content moderation, safety of users and privacy of data.

2.1 Hate Speech Detection and Content Moderation

Content moderation has been revolutionized by AI algorithms that can scour the waters to find platforms with objectionable or harmful material and eliminate it from circulation. Artificial intelligence models, especially NLP-based machine learning, perform post, comment, and message scrutiny for hate speech, fake news, and cyberbullying. For example: deep meaning systems have established subtle nuances in language in the sense of identifying sarcasm versus actual hate speech. This will evolve with the models, which learn from previously introduced content to better identify. These systems are helpful in moderating the undesirable aspects of online conduct but have their shortcoming, for example, the training sets are often biased. This is why sampling across datasets to overcome these biases is needed when enforcing community guidelines or local laws fairly. ¹

¹ Joseph, M.A., et al., *A Theoretical Workflow for the Verification of Embedded Threats on Mobile Devices*, in *Proceedings of the 2021 2nd International Conference on Computing, Automation, and Knowledge Management* 67–73 (2021).

2.2 Privacy Issues with Personalization

AI is utilized by social media platforms to deliver the feed that will show the users post that they are interested in. This is done by recommendation engines, which watch the activity, likes and links to other users, of the user. As much as this customization is useful in keeping the user interested, it poses a lot of privacy concerns. High-end AI models also scrape and compile large amounts of user data, and if the data is stolen, it can lead to data breaches and illegal profiling of the user. Privacy-preserving AI techniques (for example, federated learning) reduce these risks by processing data locally without transmitting it to be processed otherwise. ²

2.3 Fake News Detection and Mitigation

Social media has become overcome with fake news. AI algorithms, especially graph-based ones, will automatically flag fake news by monitoring source credibility, data users, and extensive content dispersion trends. Adversarial machine learning methods are also deployed instead of reacting to the new evolution of misinformation mechanisms. However, the problem of misinformation has not been solved; in fact, the ability for misinformation to spread quickly and easily means that fighting misinformation is still a difficult and ongoing battle, as there is no universal standard for verification of truth. ³

2.4 Cybersecurity Issues and their Resolutions

Cyber-attacks including phishing, account takeovers, and data breaches are rising against social media platforms. AI anomaly detection systems can detect when a user behaves suspiciously, as they are trained on patterns of normal usage. For example, since bot accounts typically have different interaction behavior compared to human accounts, graph neural networks have been employed to find such bots. Moreover, AI enhances the process of encoding that safeguards users' conversation and other content that should remain secret from tapping. However, at the same time, attackers are using AI to make better phishing that still proves that we also need to improve our defenses constantly. ⁴

² Khalid, Z., et al., *Forensic Analysis of the Cisco WebEx Application*, in *Proceedings of the 2021 5th Cyber Security in Networking Conference* 12–14 (2021).

³ Ho Choi, H., et al., *Forensic Recovery of SQL Server Database: Practical Approach*, 9 *IEEE Access* 14564, 14564–14575 (2021).

⁴ Lo, W. W., et al., *XG-BoT: An Explainable Deep Graph Neural Network for Botnet Detection and Forensics*, 22 *Internet Things* 100747 (2022).

2.5 AI Ethics and Transparency

The addition of AI in social media necessitates the addition of ethical consideration. Transparency is necessary to be achieved concerning AI governance so that responsibility for AI can be established and misuse can be avoided. Platforms should also be transparent about the role of AI in content curation and moderation design, and allow users the ability to contest automated decisions. Explainable AI can increase transparency even more by explaining, or at least giving an insight, on how the AI made its decision, which in turn can build trust in the users.⁵

2.6 Future Prospects

So, the future of AI in social media will be focusing on the technology related to those dramas, other ones are real-time system translation, AR, and virtual assistants. These innovations are intended to enhance the user's experience and at the same time, counter the new growing threat in cybersecurity. It is therefore important that governments, academia and the private sector come together to address the need of coming up with strong regulations that would ensure that AI in Social Media is ethical.

3.0 The State of AI in Banking

AI has brought a lot of disruption to the banking segment with its new features. AI is already in use in banking where it can provide recommendations or support to the decision-making procedure, enhance security or offer personalized service.⁶

3.1 Improving Customer Service via AI

Artificial Intelligence has enhanced customer engagement through computerized representatives and virtual collaborators, allowing round-the-clock help. NLP systems that determine the customer questions and give responses correctly and accurately in real-time. For instance, through the application of AI in loans, it is possible to ease the flow of credit application as well as offer timely response to customer inquiries were traditionally time-consuming processes thereby enhancing client satisfaction and processes productivity. They are also able to handle several language formats, which is quite useful for the international bank clients.⁷

⁵ Taherdoost, H., *Understanding Cybersecurity Frameworks and Information Security Standards* (2022).

⁶ Taherdoost, H., *Understanding Cybersecurity Frameworks and Information Security Standards* (2022).

⁷ Djenna, A., et al., *Internet of Things and Critical Cyber Infrastructure Security* (2021).

3.2 Enhancing Fraud Detection and Prevention

AI has been extremely helpful in preventing fraud in banking as they use machine learning algorithms to identify any patterns that deviate from normal transaction behavior which are potential signs of fraud⁸. The systems that get used in real-time monitoring analyze the data streams and detect possible threats with very little latency, thus minimizing financial loss and increasing the belief in digital banking platforms. Instead of relying on existing rule-based systems, it uses analytics such as anomaly detection models and predictive analytics to assess and avert risks beforehand in an efficient manner. ⁹Studies show that AI solutions for fraud detection are more than 90% accurate as compared to legacy systems. These developments lower false positives that earlier resulted in customer dissatisfaction and operations delays.

3.3 Make Better and Faster Credit Risk Assessment

Artificial intelligence systems in banking consider unique datasets, beyond traditional metrics, when assessing creditworthiness such as social behavior and digital footprints. Banks can use AI-based credit scoring models to target economic services to unserved segments with little or non-conventional credit history, facilitating financial inclusion. ¹⁰As long as there is a commitment to ethical AI and credit access for all, these models are also less biased.

Hopefully, we flip the other way with Operational Efficiency and Process Automation

AI in RPA: RPA, a part of AI, aids in the automation of monotonous tasks within an organisation, these include, inputs, verification and executions of some contractual tasks. This reduces human intervention and cost of operations; it allows employees to be more productive in higher value added activities. The present work also showed that AI could be employed in AML checks, which would help improve the compliance with international regulations while simultaneously reducing the amount of time required for the processing.¹¹

3.4 Criticism and Moral Issues

On the same note of AI in Banking having benefits it also comes with the following disadvantages; Data security, data bias, data ethical issues. ¹²Data breach is still possible hence

⁸ Li, Y., Han, J., & Liu, H., *A Survey on Deep Learning for Financial Fraud Detection*, 6 *IEEE Access* 69355, 69355–69367 (2018).

⁹ Anshari, M., et al., *AI in Financial Sector: Balancing Innovation and Regulation* (2024).

¹⁰ IEEE, *Cybersecurity in Financial Services* (2024).

¹¹ Saputra, M. P., et al., *Digital Banking Transaction Risk Analysis* (2022).

¹² Huang, Z., Zhang, H., & Chen, H., *A Review of Artificial Intelligence in Customer Service*, 36 *J. Intelligent & Fuzzy Sys.* 2743, 2743–2753 (2019).

the need for strong cybersecurity like the use of new encryption techniques and block chain technology among others. ¹³There's also an ethical part to it if those AI algorithms aren't audited because they could be biased against some group which leads to discrimination.

3.5 International Use Cases and Scenarios

The banks that have embarked in the use of AI have achieved on critical fronts. For instance, an AI feature of a fraud detection system has cut the false-positive rate by 30% explaining the efficiency of the system. ¹⁴Also, global large institutions use the models to fine tune investment strategies and optimize their portfolio performance. Such development reechoes the social constructive nature of AI in banking through the building of sound and innovative consumer-oriented financial systems. ¹⁵

3.6 Conclusion

Banks are using AI, which underpins the significance of AI in the future of Banking. However, in return it poses no superior benefits when it comes to efficiency and security it opens up some ethics and regulatory concerns that need to be considered and worked around to fully unlock its potential. With the potential to unlock innovation and collaboration among stakeholder classes, a responsible approach to AI can benefit the banking sector through transformation, continuity, and progression, benefitting consumers through sustainable growth and high-quality performance.

4.0 Use of AI in Medical Sciences

The advancement of AI in the medical sciences is rapid, and can bring about fruitful revolutions in the field, ranging from the improvement in the quality of the medical services, to the acceleration of medical research advancements, to the total transformation of the medical services sector. AI is going to revolutionize medicine — from diagnosis to the choice of the further therapy strategy.

Medical imaging is among the most important aspects of AI applications of medical sciences.

¹³ Mittelstadt, B., Floridi, L., Taddeo, M., & Floridi, L., *Artificial Intelligence and the Ethics of Care*, 34 *AI & Soc'y* 121, 121–131 (2019).

¹⁴ Buolamwini, J., & Gebru, T., *Gender Shades: Intersectional Accuracy Disparities in Commercial Face Recognition Systems*, in *Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency* 77–91 (2018).

¹⁵ Bahnsen, A. C., Aouada, D., & Stojanovic, N., *Detecting Financial Fraud with Deep Learning*, 6 *IEEE Access* 61545, 61545–61553 (2018).

With the help of AI algorithms, medical images such as X-rays, CT scans, MRI can be evaluated incredibly fast and at high accuracy in most cases as compared to human beings.¹⁶ This is because the outcome of the patient can be easily predicted through early diagnosis and management.

One more exciting field with a major contribution from AI is drug discovery and development. Drug discovery has been an old and time-consuming and labor-expensive process. However, AI approaches are speeding things up by mining large datasets of biological and chemical data to find new drug candidates¹⁷. By using machine learning algorithms, doctors can predict which drug molecules will work best and will be the safest, saving years of trials and money. And this could get life-saving medicines to market sooner and more cheaply.¹⁸

Personalized medicine is another area where AI is making a significant impact, enabling the customization of treatment plans to each patient's needs. Personalized medicine is another area where AI is making a big difference, because it is possible to develop individual approaches to treatments¹⁹. Finally, AI algorithms can cause patient's genetic data, medical history, and lifestyle further and estimate the likelihood of certain diseases in order to provide treatment plan. This is what a precision medicine strategy allows, to have more specific and reliable therapies, which avoid unwanted side effects and improve the patient's results.

Moreover, AI-powered chats and virtual assistants have also become distinctive competitors when it comes to patient's treatment with round-the-clock assistance and data. Smart systems that can answer questions from the patient, set appointments and even give a patient basic medical advice. The others include the capacity to track the health status of the patient through some kind of telemetry this means that the health care provider get notified when there are any issues that may lead to complications.

As well as these applications AI is also being utilized to streamline healthcare operations, costs

¹⁶ Zou, L., Li, J., Yang, K., Liu, Z., Li, Y., Wang, L., & Shen, H. T., *Artificial Intelligence in Healthcare: Past, Present and Future*, 88 *Artificial Intelligence in Med.* 55, 55–67 (2018).

¹⁷ Wang, Z., Song, L., Leung, K. S., & Yao, X., *Deep Learning for Medical Image Analysis: A Review*, 14 *Int'l J. Computer Assisted Radiology & Surgery* 949, 949–964 (2019).

¹⁸ Wang, Z., Song, L., Leung, K. S., & Yao, X., *Deep Learning for Medical Image Analysis: A Review*, 14 *Int'l J. Computer Assisted Radiology & Surgery* 949, 949–964 (2019).

¹⁹ Jiang, F., Jiang, Y., Zhi, H., & Yu, Y., *Deep Learning for Computational Biology*, 19 *Briefings in Bioinformatics* 33, 33–44 (2017).

as well as efficiency. AI systems, for example, can process and analyze millions of documents of medical data, learning the different data to identify patterns as well as trends, which allows doctors, hospitals and all businesses related to healthcare to make data-driven decisions. It assists in achieving the best use of resources, minimizing administrative costs and improving the administration of health care.²⁰

AI has great potential in medical sciences as does the question of the moral and the legal.²¹ These are; Data protection and security issues, self-biases in AI, and issues of applying AI in clinical practice.²²

Therefore, AI is an innovative technology in the sphere of medical sciences resulting in changes in disease diagnosis, treatment, and prevention.²³ It is an opportunity to improve the quality of the patient's treatment, advance the investigations, and save people's lives. However, AI implementation should also be done very cautiously and with ethical sense to make healthcare with AI sustainability and positive.²⁴

5.0 Conclusion

AI, or artificial intelligence, remains the innovative way through which alterations to functions in areas such as healthcare, finance, social media, among others, can be made. In medical sciences AI is going to revolutionize diagnosis, treatment and drug discovery. When large amounts of medical data are introduced into the system, the AI models can detect specifics that are not easily noticeable by a human analyst. That results in early diagnosis, differentiation of patients and often unique treatment strategies.

However, the integration of the AI in the healthcare system is not devoid of merits or demerit as it may be summarised on the following bases. Nevertheless, we must address these issues: privacy of data, problems with algorithms and possible loss of jobs. A little common sense in

²⁰ Lipton, Z. C., Kale, D. C., Elkan, C., & Wetzell, R., *Learning to Diagnose with Deep Learning*, in *International Conference on Learning Representations* (2016).

²¹ Rajkomar, A., Dean, J., Kohane, I. S., & Chen, H., *Machine Learning in Medicine: A Primer*, 378 *New Eng. J. Med.* 346, 346–358 (2018).

²² Miotto, R., Li, L., Wang, L., Dudley, J. T., & Shah, S. H., *Deep Learning for Healthcare: Review, Opportunities and Challenges*, 19 *Briefings in Bioinformatics* 1237, 1237–1246 (2017).

²³ Topol, E. J., *Deep Medicine: How Artificial Intelligence Can Make Healthcare Smarter* (2019).

²⁴ Hussain, M. A., Khan, M. A., & Farooq, U., *Artificial Intelligence in Healthcare: A Comprehensive Review*, 51 *Artificial Intelligence Rev.* 1, 1–32 (2018).

AI The guide is to address these issues among many others and create proper guidelines and rules for AI creating and deployment in healthcare.

AI in the financial industry is making it more effective as fraud detection, risk assessment and customer service are working on these new technologies. By analyzing financial data at scale and in real time, AI will identify anomalies and possible threats. In addition, artificial intelligence can be used for the offering of personal financial advice and support for customers through chatbots and virtual assistants.

Artificial intelligence continues to be very important in the field of social media; it includes content moderation, recommendation systems, and also cybersecurity, and more.. AI algorithms help identify and take down harmful content, including hate speech and misinformation. That said, using AI in social media also raises concerns like privacy, surveillance, and manipulation.

With the progression of AI, a balance should be commensurate between innovation and ethics. This will continue so that as long as we are careful of transparency, accountability, and fairness we can leverage the potential of AI for good and build a brighter future for humankind.