International Journal of Control and Automation
Vol. 13, No.3 (2020), pp.460 -470

# Ethical Considerations in AI-Enabled Big Data Research: Balancing Innovation and Privacy.

**[1]Surendranadha Reddy Byrapu Reddy, [2]Sarath Babu Dodda, [*3]Mohan Raparthi, [4]Srihari Maruthi.**

[1]Sr. Analyst, Information Technology, Northeastern University, Lincoln Financial Group, Atlanta, GA, USA.

[2]Software Engineer, Central Michigan University, United States.
ORCID: 0009-0008-2960-2378.

[*3]Software Engineer, Google Alphabet (Verily Life Science), Dallas, Texas, 75063.
ORCID :0009-0004-7971-9364.

[4]Senior Technical Solutions Engineer, University of New Haven, United States.

[*]Corresponding Author: - Mohan Raparthi.

**Abstract: -** The convergence of Artificial Intelligence (AI) and Big Data research has catalyzed unprecedented advancements across diverse sectors, revolutionizing the way data is analyzed, interpreted, and utilized. However, this rapid progress brings to the forefront a myriad of ethical considerations, particularly concerning privacy rights and individual autonomy. This paper delves into the intricate intersection of AI-enabled Big Data research and ethical considerations, aiming to strike a delicate balance between fostering innovation and safeguarding privacy. Ethical frameworks provide the foundational principles guiding researchers and practitioners in

maleficence, and justice underscore the importance of prioritizing societal welfare, minimizing potential harms, and ensuring equitable access and distribution of benefits. These frameworks serve as ethical compasses, guiding researchers towards responsible and ethical conduct throughout the research process. Privacy concerns loom large in AI-enabled Big Data research, fueled by the unprecedented scale, scope, and granularity of data being collected and analyzed. The identification, aggregation, and inference of sensitive information from vast datasets raise significant privacy risks, challenging traditional notions of privacy protection. Moreover, the opacity of AI algorithms and the lack of transparency in decision-making processes exacerbate privacy concerns, undermining individuals' ability to understand and control the use of their personal data. Regulatory approaches play a crucial role in addressing ethical concerns in AI-enabled Big Data research, providing a framework for legal compliance and accountability. Regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) impose obligations on organizations regarding data collection, processing, and consent, aiming to empower individuals with greater control over their personal data. However, regulatory frameworks must evolve in tandem with technological advancements and emerging ethical challenges, ensuring effective protection of privacy rights in the digital age. Emerging technologies offer promising solutions to mitigate ethical concerns in AI-enabled Big Data research while enabling innovation to flourish. Techniques such as differential privacy, federated learning, and explainable AI enhance privacy preservation, transparency, and interpretability of AI systems, fostering trust and accountability. By leveraging these technologies, researchers can uphold ethical principles while harnessing the transformative potential of AI and Big Data for societal benefit.

ISSN: 2005-4297IJCA

**Keywords: -** Artificial Intelligence, Big Data, Ethical Frameworks, Privacy Rights, Data Analytics, Regulatory Compliance, Transparency, Emerging Technologies.

**1.Introduction: -** The rapid evolution of Artificial Intelligence (AI) technology, coupled with the proliferation of Big Data, has ushered in a new era of unprecedented innovation and transformative potential across diverse domains. From healthcare and finance to marketing and education, AI-enabled Big Data research has revolutionized research methodologies, decision-making processes, and societal interactions. However, this remarkable progress also brings forth profound ethical considerations that demand careful examination and navigation.

At the heart of AI-enabled Big Data research lies the quest for knowledge extraction, pattern recognition, and predictive modeling from vast and heterogeneous datasets. [1] Leveraging advanced machine learning algorithms and computational techniques, researchers can uncover valuable insights, make informed decisions, and drive innovation at an unprecedented scale. Yet, amidst the excitement and promise of these technological advancements, ethical concerns loom large, particularly in the realm of privacy rights and individual autonomy.

Ethical frameworks provide essential guidance for researchers and practitioners engaged in AI-enabled Big Data research, offering a set of principles and guidelines to navigate the complex ethical landscape. Central to these frameworks are principles such as beneficence, which emphasizes the importance of maximizing societal welfare and minimizing harm, and non-maleficence, which underscores the imperative to mitigate risks and avoid causing harm to individuals. Additionally, principles of justice demand equitable access to the benefits of research and the fair distribution of burdens across diverse populations. By adhering to these ethical principles, researchers can uphold integrity, responsibility, and respect for human dignity throughout the research process.

Privacy concerns emerge as a prominent ethical challenge in AI-enabled Big Data research, fueled by the unprecedented scale, scope, and granularity of data being collected and analyzed. The aggregation, inference, and utilization of sensitive information raise significant risks of privacy breaches, data misuse, and discriminatory practices. Moreover, the opacity of AI algorithms and the lack of transparency in decision-making processes exacerbate privacy concerns, limiting individuals' ability to understand and control the use of their personal data.

In response to these ethical challenges, governments and regulatory bodies have implemented various measures to address privacy concerns and promote ethical conduct in AI-enabled Big Data research. Regulations such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States impose stringent requirements on organizations regarding data collection, processing, and consent, aiming to empower individuals with greater control over their personal data while holding organizations accountable for ethical and legal compliance.

Furthermore, emerging technologies offer promising solutions to mitigate ethical concerns in AI-enabled Big Data research while enabling innovation to flourish. Techniques such as differential privacy, federated learning, and explainable AI enhance privacy preservation,

ISSN: 2005-4297IJCA

transparency, and interpretability of AI systems, fostering trust and accountability in data analytics and decision-making processes.

**2. Ethical Frameworks in AI and Big Data Research: -** Ethical considerations lie at the core of AI and Big Data research, guiding researchers and practitioners in navigating complex moral dilemmas and ensuring responsible conduct throughout the research process. [2] Ethical frameworks provide essential principles and guidelines to promote integrity, transparency, and explores the foundational ethical frameworks relevant to this field, highlighting their application and significance in guiding ethical decision-making.

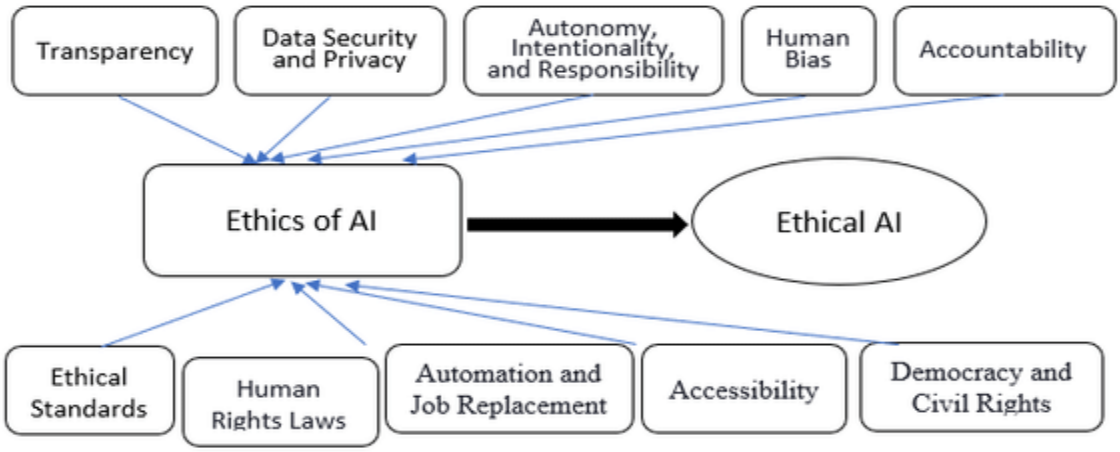


Figure 1 AI-Ethical Considerations

**2.1Beneficence:** Beneficence emphasizes the ethical imperative to maximize benefits and promote societal welfare while minimizing potential harms. In AI-enabled Big Data research, beneficence entails leveraging data and AI technologies to advance knowledge, improve decision-making processes, and enhance societal well-being. Researchers strive to develop AI models and data analytics techniques that yield meaningful insights, facilitate innovation, and address pressing societal challenges, such as healthcare disparities, climate change, and economic inequality. Moreover, beneficence requires researchers to prioritize the interests and welfare of individuals and communities affected by their research, ensuring that the benefits outweigh potential risks and harms. By upholding the principle of beneficence, researchers can contribute to positive societal outcomes while minimizing adverse consequences associated with AI-enabled Big Data research.

**2.2Non-maleficence: 2**Non-maleficence underscores the ethical obligation to avoid causing harm or inflicting injury on individuals and communities. In the context of AI-enabled Big Data research, non-maleficence requires researchers to mitigate risks associated with data collection, analysis, and utilization, thereby minimizing the potential for unintended negative consequences. Risks of harm may arise from various sources, including privacy breaches, data misuse, algorithmic biases, and discriminatory practices. [3] Researchers must implement robust safeguards and ethical guidelines to prevent and mitigate these risks, ensuring that AI systems and data analytics methods do not perpetuate harm or exacerbate existing social

ISSN: 2005-4297IJCA

inequalities. By prioritizing non-maleficence, researchers can uphold ethical integrity and protect the rights and well-being of individuals impacted by AI-enabled Big Data research.

**2.3Justice:** Justice emphasizes the ethical imperative to ensure fairness, equity, and inclusivity in the distribution of benefits and burdens associated with research. In AI-enabled Big Data research, justice requires researchers to consider the societal implications of their work and strive for equitable outcomes across diverse populations. This entails addressing issues of data bias, algorithmic fairness, and representation to mitigate disparities and promote social justice. Additionally, researchers must ensure that the benefits of AI-driven research are accessible and available to marginalized communities, thereby promoting inclusive innovation and equitable access to opportunities. By upholding principles of justice, researchers can contribute to building a more equitable and inclusive society while fostering trust and collaboration in AI-enabled Big Data research.

**2.4 Autonomy:** Autonomy emphasizes the ethical principle of respect for individuals' rights to self-determination, privacy, and informed decision-making. In AI-enabled Big Data research, autonomy requires researchers to uphold individuals' rights to control their personal data, make informed choices about data collection and use, and maintain autonomy over their digital identities. This entails obtaining informed consent from research participants, respecting privacy preferences, and providing transparency and accountability in data handling practices. Moreover, researchers must empower individuals with tools and resources to exercise autonomy and agency in their interactions with AI systems and data analytics platforms. By respecting autonomy, researchers can foster trust, empower individuals, and uphold fundamental human rights in AI-enabled Big Data research.

**2.5 Transparency:** Transparency emphasizes the ethical imperative to provide openness, clarity, and accountability in AI-enabled Big Data research practices and decision-making processes. Transparency requires researchers to disclose information about data sources, collection methods, analytical techniques, and model assumptions, enabling stakeholders to understand, evaluate, and critique research findings and conclusions. Moreover, transparency entails providing explanations for AI-driven decisions and predictions, thereby enhancing trust, accountability, and interpretability. By promoting transparency, researchers can foster public trust, enhance reproducibility, and facilitate responsible innovation in AI-enabled Big Data research.

**2.6 Accountability:** Accountability underscores the ethical obligation of researchers and organizations to take responsibility for their actions, decisions, and impacts in AI-enabled Big Data research. Accountability requires researchers to adhere to ethical principles, regulatory requirements, and professional standards, thereby ensuring ethical conduct and integrity throughout the research process. [4] Moreover, researchers must be prepared to acknowledge and address the potential consequences of their research, including unintended harms, biases, and ethical violations. By embracing accountability, researchers can demonstrate ethical leadership, build trust, and promote responsible innovation in AI-enabled Big Data research.

ISSN: 2005-4297IJCA

Ethical frameworks provide essential guidance for researchers and practitioners engaged in AI-enabled Big Data research, guiding ethical decision-making and promoting responsible conduct throughout the research process. By upholding principles of beneficence, non-maleficence, justice, autonomy, transparency, and accountability, researchers can navigate the ethical complexities of AI-enabled Big Data research responsibly, ensuring that their work advances knowledge, fosters innovation, and promotes societal well-being while upholding ethical integrity and respect for individuals' rights and dignity.


Figure 2 Ethical Framework for Big Data Research

**3. Privacy Concerns in AI-Enabled Big Data Research:** The integration of Artificial Intelligence (AI) with Big Data analytics has enabled unprecedented capabilities in extracting insights, predicting behaviors, and optimizing decision-making processes. However, this convergence raises significant privacy concerns, stemming from the vast quantities of data being collected, analyzed, and utilized in AI-enabled Big Data research. This section examines the multifaceted privacy challenges inherent in AI-enabled Big Data research and explores strategies to mitigate these concerns while fostering innovation and societal benefit.

**3.1 Data Collection and Aggregation:** One of the primary privacy concerns in AI-enabled Big Data research relates to the collection and aggregation of vast quantities of personal data from diverse sources. With the proliferation of sensors, devices, and online platforms, individuals generate immense volumes of data through their digital interactions, encompassing personal information, behavioral patterns, and preferences. [5] The aggregation of these data streams enables researchers to gain comprehensive insights into individuals' lives, behaviors, and preferences. However, it also raises concerns about data ownership, consent, and control, as individuals may lack awareness of the extent to which their data are being collected and utilized for research purposes. Moreover, the aggregation of disparate data sources increases the risk of re-identification and unauthorized access, potentially compromising individuals' privacy and security.

**3.2 Privacy Risks in Data Analysis and Inference:** AI-driven data analysis techniques pose additional privacy risks, as they enable researchers to infer sensitive information and predictive models from large datasets. [6] Machine learning algorithms can identify subtle correlations, patterns, and associations within data, often without human intervention or oversight. While

ISSN: 2005-4297IJCA

these capabilities offer valuable insights and predictive power, they also raise concerns about the potential for unintended disclosure of sensitive information and privacy breaches. Moreover, the opacity and complexity of AI algorithms make it challenging to assess their fairness, transparency, and potential biases, further exacerbating privacy concerns. Researchers must implement robust privacy-preserving techniques, such as differential privacy and federated learning, to mitigate these risks and ensure that individuals' privacy rights are protected during data analysis and model training processes.

**3.3 Algorithmic Bias and Discrimination:** Another significant privacy concern in AI-enabled Big Data research relates to algorithmic bias and discrimination, whereby AI systems may perpetuate or amplify existing social inequalities and biases present in the underlying data. Biased data inputs, flawed algorithms, and skewed training datasets can lead to discriminatory outcomes and decision-making processes, particularly in sensitive domains such as healthcare, criminal justice, and financial services. Moreover, AI systems may inadvertently encode and perpetuate societal biases, resulting in unfair treatment and disparate impacts on marginalized communities. Researchers must adopt rigorous methods for identifying, mitigating, and addressing algorithmic bias and discrimination, ensuring that AI systems promote fairness, equity, and inclusivity while respecting individuals' privacy and dignity.

**3.4 Lack of Transparency and Control:** The opacity and lack of transparency surrounding AI algorithms and decision-making processes pose additional challenges to privacy protection in AI-enabled Big Data research. Many AI models operate as "black boxes," making it difficult for individuals to understand how their data are being used, analyzed, and interpreted. Moreover, individuals may lack control over the collection, processing, and sharing of their personal data, leading to concerns about loss of autonomy and privacy infringement. Researchers must prioritize transparency, accountability, and user control in AI-enabled Big Data research, providing individuals with meaningful insights into data handling practices and empowering them with tools and mechanisms to exercise control over their personal data.

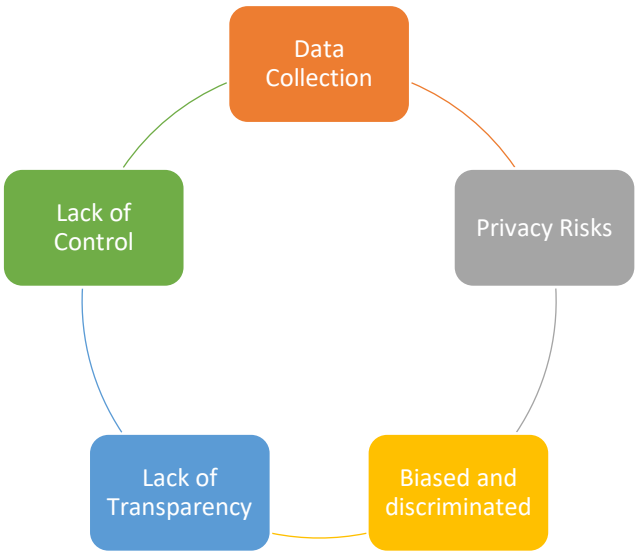


Figure 3 Privacy Concerns for AI- Enabled Big data Research

ISSN: 2005-4297IJCA

Privacy concerns loom large in AI-enabled Big Data research, driven by the vast quantities of data being collected, analyzed, and utilized in research endeavors. By addressing these privacy challenges through robust privacy-preserving techniques, algorithmic fairness measures, transparency mechanisms, and user-centric approaches, researchers can mitigate privacy risks while fostering innovation and societal benefit. Ultimately, safeguarding privacy rights and upholding ethical principles are essential prerequisites for responsible and ethical AI-enabled Big Data research, ensuring that individuals' privacy and autonomy are respected and protected in the digital age.

**4. Regulatory Approaches to Addressing Ethical Concerns:** The rapid advancement of AI-enabled Big Data research has prompted governments and regulatory bodies worldwide to enact legislation, standards, and guidelines aimed at addressing ethical concerns and promoting responsible conduct in data-driven research endeavors. Regulatory approaches play a crucial role in safeguarding individuals' privacy rights, ensuring algorithmic fairness, and fostering transparency and accountability in AI-enabled Big Data research. [7] This section examines key regulatory frameworks and initiatives that aim to mitigate ethical concerns in this rapidly evolving field.

**4.1 General Data Protection Regulation (GDPR):** The General Data Protection Regulation (GDPR), implemented by the European Union (EU) in 2018, represents one of the most comprehensive and influential regulatory frameworks governing data privacy and protection. The GDPR establishes strict requirements for organizations regarding data collection, processing, storage, and consent, aiming to empower individuals with greater control over their personal data. Under the GDPR, organizations are required to obtain explicit consent from individuals before collecting and processing their data, disclose the purposes and legal basis for data processing, and implement robust security measures to protect personal data from unauthorized access and misuse. Moreover, the GDPR imposes stringent penalties for non-compliance, including fines of up to 4% of annual global turnover or €20 million, whichever is higher. By establishing a harmonized framework for data protection across the EU, the GDPR enhances individuals' privacy rights and promotes ethical conduct in AI-enabled Big Data research.

**4.2 California Consumer Privacy Act (CCPA):** The California Consumer Privacy Act (CCPA), enacted in 2018 and enforced in 2020, represents a landmark piece of privacy legislation in the United States, akin to the GDPR in Europe. The CCPA grants California residents with enhanced rights and protections concerning their personal data, including the right to know what personal information is being collected, the right to opt-out of the sale of their data, and the right to request deletion of their data. [8] Similar to the GDPR, the CCPA imposes strict requirements on organizations regarding data transparency, consent, and security, aiming to empower individuals with greater control over their personal data. Additionally, the CCPA enables individuals to pursue legal remedies and seek damages for violations of their privacy rights, thereby holding organizations accountable for ethical and legal compliance in AI-enabled Big Data research.

ISSN: 2005-4297IJCA

**4.3 Sector-Specific Regulations and Guidelines:** In addition to overarching data protection laws such as the GDPR and CCPA, various sector-specific regulations and guidelines address ethical concerns in AI-enabled Big Data research within specific domains. For example, regulations in healthcare (e.g., Health Insurance Portability and Accountability Act - HIPAA), finance (e.g., Payment Card Industry Data Security Standard - PCI DSS), and education (e.g., Family Educational Rights and Privacy Act - FERPA) impose additional requirements and safeguards for protecting sensitive personal data and ensuring ethical conduct in research and data analytics practices. Moreover, industry associations, professional organizations, and research institutions often develop voluntary guidelines and best practices to promote ethical behavior and responsible innovation in AI-enabled Big Data research within their respective sectors.

**5. Emerging Technologies for Ethical AI-Enabled Big Data Research: -**The rapid advancement of technology continues to reshape the landscape of AI-enabled Big Data research, offering innovative solutions to address ethical concerns while fostering responsible and transparent data-driven practices. This section explores key emerging technologies that hold promise for enhancing privacy, transparency, fairness, and accountability in AI-enabled Big Data research endeavors.

**5.1 Differential Privacy:** Differential privacy is a privacy-preserving technique that enables researchers to analyze sensitive data while protecting individuals' privacy and confidentiality. Differential privacy achieves this by adding noise to query responses or data outputs, thereby obscuring individual contributions to the dataset while preserving aggregate statistical properties. [9] By incorporating differential privacy techniques into data analysis workflows, researchers can mitigate the risk of re-identification and unauthorized disclosure of sensitive information, enabling robust and privacy-preserving data analysis in AI-enabled Big Data research.

**5.2 Federated Learning:** Federated learning is a decentralized machine learning approach that enables model training across distributed data sources without centralizing data in a single location. [10] In federated learning, machine learning models are trained collaboratively on data stored locally on edge devices or servers, with model updates aggregated and refined centrally. This decentralized approach to model training preserves data privacy and confidentiality, as sensitive data remains under the control of data owners and is not shared or transferred externally. Federated learning is particularly well-suited for applications in healthcare, finance, and other sectors where data privacy and security are paramount, enabling collaborative research and model development while respecting individuals' privacy rights.

ISSN: 2005-4297IJCA

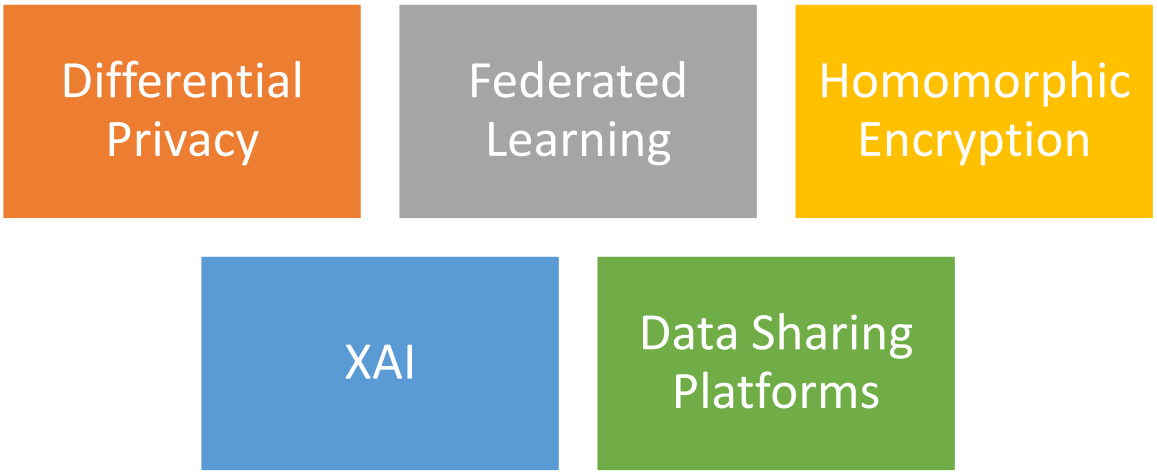


Figure 4 Emerging Technologies for Ethical AI-Enabled Big Data Research

**5.3 Homomorphic Encryption:** Homomorphic encryption is a cryptographic technique that allows data to be encrypted while still enabling mathematical operations to be performed on the encrypted data. This enables researchers to analyze sensitive data in its encrypted form without decrypting it, thereby preserving data privacy and confidentiality throughout the analysis process. [11] Homomorphic encryption offers a secure and privacy-preserving solution for conducting data analysis and computation in AI-enabled Big Data research, enabling researchers to leverage sensitive datasets while protecting individuals' privacy rights and confidentiality.

**5.4 Explainable AI (XAI):** Explainable AI (XAI) refers to the development of AI systems and algorithms that provide explanations for their decisions, predictions, and recommendations in a transparent and interpretable manner. [12] XAI techniques enable researchers and stakeholders to understand the underlying logic and reasoning processes of AI models, thereby enhancing transparency, accountability, and trust in AI-enabled Big Data research. By incorporating XAI techniques into AI systems and data analytics workflows, researchers can mitigate concerns about algorithmic opacity, bias, and discrimination, enabling stakeholders to scrutinize and evaluate AI-driven decisions and outcomes.

**5.5 Privacy-Preserving Data Sharing Platforms:** Privacy-preserving data sharing platforms provide secure and privacy-preserving mechanisms for sharing and collaborating on sensitive datasets in AI-enabled Big Data research. [13] These platforms leverage cryptographic techniques, access control mechanisms, and privacy-enhancing technologies to ensure that sensitive data remains protected and confidential throughout the data sharing process. By facilitating secure and privacy-preserving data sharing, these platforms enable collaborative research and knowledge exchange while safeguarding individuals' privacy rights and confidentiality.

**6.Conclusion: -** Ethical considerations are paramount in AI-enabled Big Data research, as the integration of advanced technologies with vast datasets brings forth profound implications for

ISSN: 2005-4297IJCA

privacy, fairness, transparency, and accountability. Striking a balance between fostering innovation and protecting individuals' privacy rights requires a multidimensional approach that integrates ethical frameworks, regulatory compliance, and emerging technologies. Throughout this paper, we have explored the ethical challenges inherent in AI-enabled Big Data research and proposed strategies to address these concerns while promoting responsible conduct and ethical integrity. Ethical frameworks provide essential guidance for researchers and practitioners, emphasizing principles such as beneficence, non-maleficence, justice, autonomy, transparency, and accountability. By adhering to these ethical principles, researchers can prioritize societal welfare, minimize harm, ensure fairness and equity, respect individuals' autonomy, and promote transparency and accountability throughout the research process. Regulatory approaches play a crucial role in addressing ethical concerns in AI-enabled Big Data research, with laws such as the GDPR, CCPA, and sector-specific regulations establishing requirements and safeguards for data protection, consent, and accountability. Compliance with these regulations is essential for upholding individuals' privacy rights and promoting ethical conduct in data-driven research endeavors.[14],[15] Emerging technologies offer promising solutions to mitigate ethical concerns and enhance privacy, transparency, fairness, and accountability in AI-enabled Big Data research. Techniques such as differential privacy, federated learning, homomorphic encryption, explainable AI, and privacy-preserving data sharing platforms enable researchers to conduct robust and privacy-preserving data analysis while respecting individuals' privacy rights and confidentiality. In conclusion, navigating the ethical landscape of AI-enabled Big Data research requires a collaborative and interdisciplinary approach that prioritizes ethical principles, regulatory compliance, and technological innovation. By embracing ethical frameworks, adhering to regulatory requirements, and leveraging emerging technologies, researchers can foster responsible innovation, promote societal welfare, and uphold individuals' privacy rights in the rapidly evolving field of AI-enabled Big Data research. Ultimately, by balancing innovation with privacy protection, we can ensure that the benefits of AI and Big Data are realized while respecting ethical principles and promoting the common good.

**References: -**

[1] Floridi, L. (2018). Soft ethics, the governance of the digital, and the general data protection regulation. Philosophy & Technology, 31(1), 1-8.

[2] Mittelstadt, B. D., & Floridi, L. (2016). The ethics of big data: current and foreseeable issues in biomedical contexts. Science and Engineering Ethics, 22(2), 303-341.

[3] European Union. (2016). 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.

[4] California Legislative Information. (2018). California Consumer Privacy Act of 2018. Assembly Bill No. 375.

[5] Pasquale, F. (2015). The black box society: The secret algorithms that control money and information. Harvard University Press.

[6] Dwork, C. (2008). Differential privacy: A survey of results. In Theory and Applications of Models of Computation (pp. 1-19). Springer.

ISSN: 2005-4297IJCA

[7] McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). Communication-efficient learning of deep networks from decentralized data. arXiv preprint arXiv:1602.05629.

[8] Gilpin, L. H., Bau, D., Yuan, B. Z., Bajwa, A., Specter, M., & Kagal, L. (2018). Explaining explanations: An overview of interpretability of machine learning. In 2018 IEEE 5th International Conference on Data Science and Advanced Analytics (DSAA) (pp. 80-89). IEEE.

[9] Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In Privacy Enhancing Technologies (pp. 36-58). Springer.

[10] Federal Trade Commission. (2016). Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues.

[11] Vayena, E., & Gasser, U. (2016). Strictly biomedical? Sketching the ethics of the big data ecosystem in biomedical research. In Yearbook of medical informatics (Vol. 25, No. 01, pp. 8-14). Georg Thieme Verlag KG.

[12] Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. UCLA Law Review, 57, 1701.

[13] Chouldechova, A. (2017). Fair prediction with disparate impact: A study of bias in recidivism prediction instruments. Big Data, 5(2), 153-163.

[14] Shokri, R., & Shmatikov, V. (2015). Privacy-preserving deep learning. In Proceedings of the 22nd ACM SIGSAC conference on computer and communications security (pp. 1310-1321).

[15]Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., ... & Wallach, H. (2017). Accountable algorithms. University of Pennsylvania Law Review, 165(3), 633-705.

ISSN: 2005-4297IJCA