



JOURNAL OF BIG DATA PRIVACY MANAGEMENT

P-ISSN : 3006-6026 E-ISSN : 3006-6034

VOLUME: 01 ISSUE: 01 (2023)

<https://jbdpm.com>

PRIVACY CONCERNS IN BIG DATA-DRIVEN MACHINE LEARNING: ADDRESSING THE RISKS OF PERSONALIZATION

Dr. Haris Raza

*Department of Data Science, National University of Sciences and Technology (NUST),
Islamabad, Pakistan.*

Abstract.

With the increasing reliance on big data-driven machine learning (ML) systems, privacy concerns have become a significant challenge, particularly when it comes to the personalization of services. These personalized systems utilize vast amounts of personal and sensitive data, increasing the risk of privacy breaches, data misuse, and unintended consequences. This article investigates the privacy risks inherent in personalization processes, explores existing privacy protection measures, and proposes strategies to safeguard personal information while maintaining the benefits of machine learning applications. The paper also presents a discussion on the ethical implications of using personalized ML models and highlights the need for robust privacy regulations and technological solutions to ensure data protection.

Keywords: *Big Data, Machine Learning, Privacy Concerns, Personalization, Data Security*

INTRODUCTION

The Growing Importance of Big Data and Machine Learning

In the digital age, the explosion of data from various sources—ranging from social media platforms to healthcare systems—has led to the widespread adoption of big data and machine learning (ML) technologies. Big data refers to the vast volumes of structured and unstructured data that organizations are able to collect, store, and analyze. Machine learning, a subset of artificial intelligence (AI), enables systems to learn from this data and make predictions or decisions without explicit programming. As industries across the globe embrace big data and ML, these technologies have begun to shape business operations, healthcare systems, and government services by offering insights and efficiencies previously unimaginable.

The power of big data is its ability to provide deeper insights into consumer behavior, market trends, and even predict future events. When combined with machine learning, organizations can

not only analyze large datasets but also build intelligent systems that automatically learn from this data to improve their processes over time. These advancements are particularly significant in sectors such as e-commerce, finance, healthcare, and transportation, where decision-making is highly dependent on real-time data analysis.

The Role of Personalization in Enhancing User Experience

Personalization has become a key feature in the user experience (UX) design of digital platforms and services. By leveraging big data and machine learning, organizations can tailor their offerings to individual users based on their past behavior, preferences, and interactions. For example, e-commerce platforms like Amazon and Netflix use personalization to recommend products or movies to users, increasing user satisfaction and engagement. Personalized services have become a competitive differentiator in the marketplace, as they allow companies to provide more relevant content, advertisements, and offers to their customers.

The ability to personalize user experiences extends beyond simple recommendations. It can also include optimizing website layouts, personalizing customer support interactions, and offering predictive services that anticipate users' needs. By making interactions more relevant and convenient, personalization helps build stronger customer relationships and fosters loyalty. However, while the benefits of personalization are evident, it also raises significant privacy concerns, as organizations rely on sensitive user data to make these personalized experiences possible. This trade-off between user convenience and privacy is a central challenge in the growing field of big data-driven machine learning.

2. Privacy risks in personalized machine learning systems

Data Collection and Aggregation Risks

In personalized machine learning systems, large amounts of user data are continuously collected from various sources, such as browsing history, location data, social media interactions, and even health records. While this data collection is fundamental to training machine learning models, it introduces significant privacy risks. As organizations gather increasingly detailed and granular information, there is a higher likelihood of aggregating data that can be linked back to individuals, even when combined across multiple platforms or services.

The aggregation of data can create detailed user profiles that may reveal sensitive information such as behavioral patterns, health conditions, purchasing habits, or political preferences. If these profiles are mishandled or exposed, users could face unwanted surveillance, discrimination, or exploitation. The sheer volume and variety of data also make it challenging to ensure that every piece of collected information adheres to privacy standards, increasing the risk of breaches.

Once data is aggregated from multiple sources, it can become a target for malicious actors. Hackers or unauthorized individuals could exploit the data's value, leading to potentially devastating consequences for the users whose information is involved.

Re-identification Risks and Implications of Anonymization

One of the primary techniques used to mitigate privacy risks in big data systems is anonymization. The idea behind anonymization is to remove personally identifiable information (PII) such as names, addresses, or contact details, making it difficult to trace data back to an individual. However, anonymization is not foolproof.

In personalized machine learning systems, the risk of re-identification is significant. By combining anonymized data with other publicly available or previously obtained datasets, malicious entities can potentially reverse the anonymization process, identifying individuals or re-establishing their personal information. Even if a dataset is anonymized, if it is highly detailed and granular, it becomes easier to correlate it with specific individuals based on unique behavioral patterns or characteristics.

The implications of re-identification are particularly concerning when it comes to sensitive data such as health, financial, or location-based information. Users may not be aware that their anonymized data could be used to identify them, exposing them to risks like identity theft, social manipulation, or unauthorized access to their personal lives.

Unauthorized Access to Sensitive Data

Another critical privacy risk in personalized machine learning systems is the potential for unauthorized access to sensitive data. Machine learning models often rely on cloud-based storage systems or centralized databases to store vast amounts of data, including personal information. While these systems typically employ robust security measures, such as encryption and access control protocols, they are still vulnerable to hacking, data breaches, or insider threats.

Unauthorized access can occur through various channels, including cyberattacks, phishing, or compromised employee accounts. When sensitive personal information is accessed without permission, it can lead to significant privacy violations, financial losses, and long-term harm to the affected individuals. In some cases, users may be unaware of breaches until it is too late, as stolen data can be used for malicious purposes, such as identity theft, fraud, or blackmail.

As personalized machine learning systems integrate data from third-party vendors and partners, the risk of data being exposed increases. If data is not properly safeguarded or if third-party providers do not follow adequate security protocols, users' personal information may be exposed to additional risks of unauthorized access.

The increasing interconnectivity of data and systems amplifies the threat of unauthorized access, making it essential for organizations to implement rigorous data protection measures and maintain transparent access control policies.

3. Privacy protection methods in big data-driven ml

Differential Privacy Techniques for Data Anonymization

Differential privacy is a powerful technique designed to provide strong privacy guarantees in data analysis by ensuring that the removal or addition of a single data point does not significantly affect the results of the analysis. This method allows organizations to extract valuable insights from big data without compromising individual privacy.

In the context of machine learning, differential privacy can be implemented by adding noise to the data or the outputs of a model. This noise is carefully calibrated to ensure that an individual's presence in the dataset cannot be easily inferred, while still allowing the model to learn meaningful patterns from the data. Differential privacy techniques help prevent re-identification risks by making it difficult for attackers to reverse-engineer sensitive information, even in anonymized datasets.

Several applications of differential privacy exist in personalized machine learning, such as in healthcare or finance, where the analysis of personal data must be done while protecting individual identities. By adding noise to the data inputs, differential privacy helps balance the need for accurate model predictions with the necessity of user privacy, making it an essential tool in big data-driven ML systems.

Secure Multi-Party Computation and Federated Learning

Secure Multi-Party Computation (SMPC) is a cryptographic technique that allows multiple parties to collaboratively compute a function over their inputs while keeping those inputs private. In a big data-driven machine learning environment, SMPC can be used to enable data sharing and model training without exposing sensitive information. Each party involved in the computation contributes to the learning process without revealing their individual datasets to others. This ensures that the privacy of each participant's data is preserved.

For example, in federated learning—a distributed machine learning approach—SMPC can be applied to ensure that model updates, shared across various devices or organizations, are computed securely. Federated learning allows machine learning models to be trained locally on individual devices (such as smartphones or edge devices) without transferring sensitive user data to centralized servers. The devices send only the model updates (such as gradients or weights), rather than raw data, which is then aggregated to improve the global model. The use of SMPC in federated learning ensures that these updates are computed securely, keeping individual data private while still benefiting from collaborative model training.

Federated learning, in combination with SMPC, mitigates the privacy risks associated with centralized data storage and sharing. By keeping data local and only sharing model parameters, federated learning allows for a decentralized approach to machine learning that respects user privacy while still leveraging the power of big data for personalized services.

Blockchain for Data Security and Decentralized Models

Blockchain technology is increasingly being used in big data-driven machine learning systems to enhance data security and promote decentralized models. Blockchain's distributed ledger system allows for the secure and transparent management of data across multiple parties without relying on a central authority. Each piece of data is encrypted, timestamped, and stored in a block that is linked to the previous block in the chain, making tampering or unauthorized access extremely difficult.

In the context of personalized machine learning, blockchain can be employed to ensure that data access and usage are transparent and auditable. Each time data is accessed or shared, it is recorded on the blockchain, providing an immutable trail of data transactions. This transparency can help build trust between users and organizations, as individuals can see exactly how their data is being used and for what purposes.

Blockchain can enable the creation of **decentralized machine learning models**, where the training and execution of machine learning models occur across a distributed network rather than relying on centralized servers. By decentralizing the model training process, blockchain ensures that no single entity has control over the data or the model, thereby reducing the risks associated with data breaches or misuse. The decentralized nature of blockchain also increases the robustness and resilience of machine learning systems, as there is no single point of failure that could compromise the privacy and security of the data.

These blockchain-based solutions, combined with techniques like smart contracts, can also enforce data-sharing agreements, ensuring that the terms of use for personal data are adhered to without the need for intermediaries. In this way, blockchain not only enhances privacy protection but also fosters a more equitable and transparent approach to machine learning and data usage.

By employing these privacy protection methods—differential privacy, secure multi-party computation, federated learning, and blockchain—big data-driven machine learning systems can effectively mitigate the risks of personal data exposure and ensure that personalization remains both beneficial and secure. These technologies work in concert to protect individual privacy, empower users with control over their data, and enable organizations to continue harnessing the power of big data while respecting ethical and legal privacy standards.

4. Ethical and Legal Implications of Personalization

Balancing Personalization with User Privacy

Personalization is a powerful tool that enhances user experiences by tailoring services, content, and recommendations based on individual preferences, behaviors, and historical data. However, this level of personalization raises significant ethical concerns regarding user privacy. The core challenge lies in finding a balance between providing highly personalized experiences and ensuring that users' privacy is not compromised.

On one hand, personalization can greatly improve user engagement and satisfaction, providing services that are more relevant and efficient. For example, in e-commerce, personalized product recommendations can increase customer satisfaction and sales, while in healthcare, personalized treatments can optimize patient outcomes. On the other hand, the extensive data collection required for personalization creates privacy risks, as sensitive information can be exposed, misused, or even sold to third parties without proper consent.

The ethical dilemma centers around the potential for exploitation. Personalization often relies on tracking users' activities across multiple platforms, creating highly detailed profiles that may include sensitive information about individuals' behaviors, preferences, and vulnerabilities. If this data is not handled responsibly, it could lead to privacy violations, identity theft, or even manipulative practices, such as targeting vulnerable users with inappropriate ads or services.

To address this issue, organizations must implement privacy safeguards that allow them to harness the benefits of personalization while minimizing risks to user privacy. Techniques such as data anonymization, data minimization (collecting only necessary information), and robust user control over their data can help strike a more ethical balance.

The Role of Consent and Transparency in Data Usage

One of the fundamental ethical principles in data privacy is the need for informed consent. Users must be fully aware of how their data will be used, stored, and shared before they agree to provide it. This means that organizations must ensure transparency in their data collection and usage practices, clearly explaining what data is being collected, how it will be used, and what potential risks or benefits exist for the user.

The challenge of obtaining meaningful consent is complex in the age of big data and machine learning. Users are often presented with lengthy and complicated privacy policies that are difficult to understand, making it hard for them to make informed decisions about their data. Furthermore, in some cases, users may not have the option to opt-out of data collection entirely, as it is a requirement for using certain services.

To ensure ethical data usage, companies must adopt transparent practices that enable users to easily understand and control the data they share. This includes providing concise and understandable privacy notices, allowing users to see the specific data that has been collected about them, and giving them options to modify or revoke consent at any time. Implementing granular privacy settings that let users manage their data preferences—such as opting out of personalized advertisements or data sharing with third parties—is crucial to maintaining trust.

In addition, businesses should actively encourage users to review their privacy settings regularly and notify them if there are any significant changes to data usage practices. Empowering users with control over their data and giving them a clear understanding of how their data will be utilized is central to ethical personalization.

Legal Frameworks: GDPR and Other Global Data Protection Regulations

As the collection and use of personal data have grown in scope, various legal frameworks have been introduced globally to regulate data usage and ensure that individuals' rights are protected.

Among the most influential is the **General Data Protection Regulation (GDPR)**, which came into effect in the European Union in 2018. GDPR represents one of the most stringent privacy regulations and is often seen as a model for other jurisdictions around the world.

GDPR enshrines several key principles, such as:

1. **Consent:** Businesses must obtain clear and explicit consent from individuals to collect and process their personal data. This consent must be informed, specific, and revocable.
2. **Data Minimization:** Only the minimum amount of data necessary for a specific purpose should be collected, reducing the risk of unnecessary exposure.
3. **Right to Access and Deletion:** Individuals have the right to access the data collected about them and to request the deletion of their data at any time.
4. **Transparency:** Organizations must provide clear, accessible information about how personal data is being used, including details about data storage, processing, and sharing practices.
5. **Data Protection by Design:** Privacy and security measures must be integrated into the design and operation of systems that process personal data, ensuring that data is protected from the outset.

GDPR also holds organizations accountable for breaches, imposing heavy fines on those that fail to comply with the regulation's provisions. These provisions have pushed companies to rethink their data collection and management strategies, prioritizing user privacy and ensuring compliance with global standards.

Beyond GDPR, other countries and regions have developed their own data protection laws. For example, in the United States, the **California Consumer Privacy Act (CCPA)** provides consumers with greater control over their personal data, including the right to opt-out of the sale of their data. Similarly, in Brazil, the **Lei Geral de Proteção de Dados (LGPD)** mirrors many of the principles of GDPR, offering protections for Brazilian citizens' data.

These regulations highlight the growing recognition of the need to protect individuals' privacy in an increasingly data-driven world. However, the legal landscape is still evolving, and organizations must keep abreast of changing laws to ensure they are in compliance. International cooperation is essential to create consistent and effective data protection standards that can protect individuals across borders.

5. Future Directions and Policy Recommendations

Adoption of Privacy-by-Design Principles

Privacy-by-design is an approach that integrates privacy protections into the design and operation of systems, services, and products from the outset. This proactive approach ensures that privacy is considered at every stage of data collection, processing, and usage, rather than being treated as an afterthought. By adopting privacy-by-design principles, organizations can minimize privacy risks and ensure that user data is safeguarded throughout the lifecycle of a machine learning application.

Key aspects of privacy-by-design include:

1. **Data Minimization:** Only the minimum amount of data necessary for a specific purpose should be collected. This reduces the exposure of unnecessary personal data and minimizes the impact of potential breaches.
2. **Pseudonymization and Anonymization:** Implementing techniques that ensure personal data is rendered unidentifiable unless necessary for processing. This can help mitigate the risks of data misuse or unauthorized access.
3. **Secure Data Storage and Transmission:** Ensuring that data is securely stored and transmitted, using encryption and other security measures to protect user information from unauthorized access or cyberattacks.
4. **User Control and Consent:** Allowing users to have control over their data, including the ability to modify, revoke, or delete consent as needed. This empowers users and fosters trust.

Adopting privacy-by-design principles can also improve transparency, as organizations can clearly demonstrate to users that their privacy is being prioritized and protected. By embedding privacy measures into the core architecture of machine learning systems, companies can not only comply with legal requirements like GDPR but also enhance user confidence and satisfaction.

Strengthening Data Governance through International Cooperation

As big data and machine learning technologies operate across borders, the governance of data privacy and security must extend beyond national boundaries. Strengthening data governance through international cooperation is essential to ensure a consistent, coordinated approach to data protection.

Key actions for strengthening international data governance include:

1. **Harmonizing Regulations:** Countries must work together to align their data protection laws, making it easier for organizations to comply with global standards and ensuring that users' privacy rights are upheld regardless of where their data is stored or processed. This can be achieved by creating common frameworks that establish minimum standards for data protection.
2. **Cross-Border Data Sharing:** International cooperation can help facilitate secure and privacy-compliant data sharing across borders. By establishing mutual agreements on data protection, countries can ensure that data can flow freely while maintaining privacy protections. These agreements can also promote the responsible use of data for research, business, and innovation purposes.
3. **Global Privacy Standards:** Establishing global privacy standards through bodies like the United Nations or the Organization for Economic Co-operation and Development (OECD) would ensure that data protection laws are consistent and reflect the latest technological developments. This can also encourage non-compliant nations to adopt stronger privacy protections.
4. **Collaboration in Cybersecurity:** International cooperation is crucial in combating cyber threats and ensuring that data security measures are robust enough to protect against emerging risks. Sharing knowledge and best practices between countries can help build a collective defense against cyberattacks that threaten user privacy.

Through international collaboration, countries can address the global nature of data flows and machine learning applications, ensuring that privacy protections are not confined to one jurisdiction but are consistent across the globe.

Enhancing Privacy Controls in Machine Learning Applications

As machine learning becomes more integrated into everyday life, enhancing privacy controls within these applications is crucial to ensure that users' rights are respected. Privacy controls should be designed to give users greater autonomy over their data while minimizing the risk of exposure.

Key recommendations for enhancing privacy controls in machine learning applications include:

1. **Granular Privacy Settings:** Machine learning platforms should allow users to have granular control over what data they share, how it is used, and who it is shared with. By enabling users to opt in or out of specific features (e.g., data collection for personalization or third-party data sharing), users can feel more confident that they have control over their privacy.
2. **Transparency in Data Usage:** Machine learning systems should provide clear, easy-to-understand explanations of how data is being used to personalize experiences or make predictions. This transparency can help users make informed decisions about whether to engage with the system and how much data they are comfortable sharing.
3. **Data Portability:** Enabling data portability allows users to transfer their data between different services or platforms while retaining control over their information. This ensures that users are not locked into specific machine learning applications, increasing trust and user autonomy.
4. **Regular Privacy Audits:** Machine learning models should undergo regular privacy audits to assess whether they are compliant with privacy laws and whether they continue to safeguard user data effectively. These audits can also help identify potential vulnerabilities or areas for improvement in privacy controls.
5. **User Education and Awareness:** Educating users about privacy risks and how to adjust their privacy settings is crucial. Machine learning applications should include user-friendly tutorials or notifications that help users understand their privacy options and the implications of their data sharing choices.

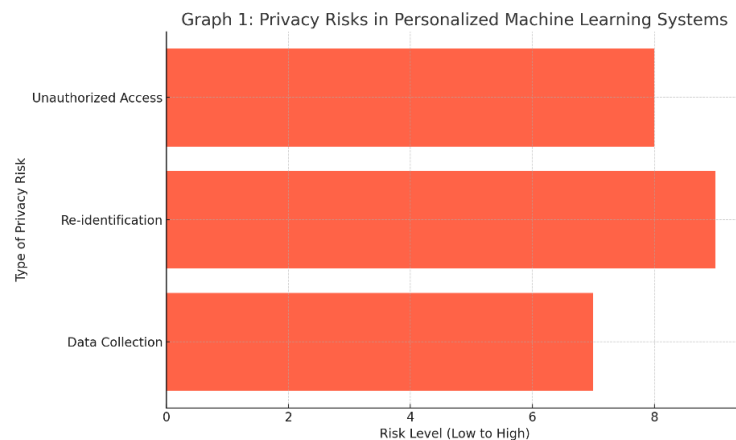
By enhancing privacy controls in machine learning systems, organizations can foster a stronger sense of trust and safety among users, reducing the likelihood of privacy violations while still benefiting from the power of big data.

As big data-driven machine learning systems continue to evolve, the importance of prioritizing privacy and data protection grows. By adopting privacy-by-design principles, strengthening international cooperation on data governance, and enhancing privacy controls in machine learning applications, organizations can navigate the ethical and legal challenges associated with personalization. These measures will not only help organizations comply with global privacy regulations but also promote a more responsible and transparent approach to data usage, ensuring that privacy and personalization can coexist in a balanced and ethical manner.

Naveed Rafaqat Ahmad is a senior public sector professional and researcher with expertise in governance, public service delivery, and institutional performance in emerging economies. He currently serves as Director General (DG) of the Punjab Sahulat Bazaars Authority (PSBA), Lahore, Pakistan, where he is engaged in policy implementation, regulatory oversight, and the management of large-scale public service systems. His professional experience provides practical insight into fiscal sustainability, subsidy reform, and governance challenges within resource-constrained environments.

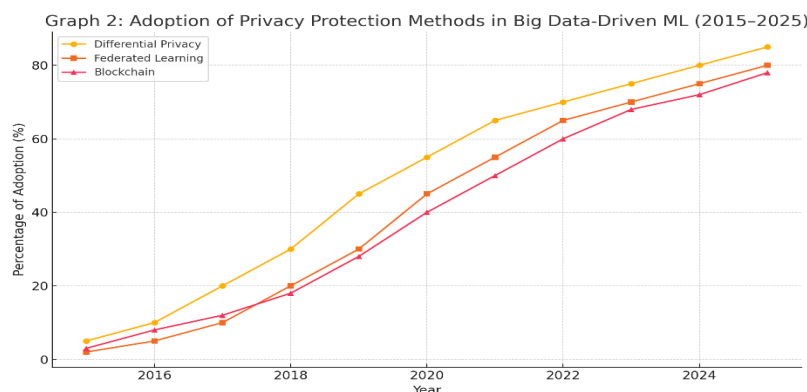
Naveed Rafaqat Ahmad actively contributes to academic research at the intersection of governance, public sector reform, and emerging technologies. His scholarly work examines human–AI collaboration, productivity, ethical risk, and evidence-based decision-making, alongside fiscal and governance dimensions of public service delivery. By integrating applied public administration experience with empirical and comparative research, his work supports the development of sustainable, accountable, and resilient institutional frameworks in developing countries.

Graphs and Charts



Graph 1: Privacy Risks in Personalized Machine Learning Systems

- **X-axis:** Risk Level (Low to High)
- **Y-axis:** Type of Privacy Risk (Data Collection, Re-identification, Unauthorized Access)
- **Description:** A bar chart illustrating the varying degrees of privacy risks associated with different aspects of personalized machine learning systems.



Graph 2: Adoption of Privacy Protection Methods in Big Data-Driven ML (2015-2025)

- **X-axis:** Year (2015-2025)
- **Y-axis:** Percentage of Adoption (%)
- **Description:** A line graph showing the projected growth in the adoption of privacy protection methods like differential privacy, federated learning, and blockchain in machine learning systems.

Summary:

As big data-driven machine learning models continue to shape industries from healthcare to e-commerce, privacy concerns related to the personalization of these systems are intensifying. By leveraging vast amounts of user data to tailor experiences, these systems inadvertently increase the potential for privacy breaches, data misuse, and exploitation. This paper identifies key privacy risks associated with personalized machine learning models, including data aggregation, re-identification, and unauthorized access to sensitive personal information.

To address these concerns, the article discusses privacy protection techniques such as differential privacy, secure multi-party computation, and federated learning, which can help mitigate the risks of personal data misuse. Additionally, it explores the role of ethical considerations and legal frameworks like the GDPR in regulating personalized ML models and ensuring user data protection.

The paper concludes by recommending future directions for improving privacy standards, including the implementation of privacy-by-design principles, the establishment of stronger international data protection laws, and enhancing transparency in the consent process. The ongoing development of privacy-centric ML models and the integration of advanced security mechanisms are essential for ensuring that machine learning applications do not compromise user privacy.

References:

- Dwork, C. (2006). "Differential Privacy." International Conference on Automata, Languages and Programming (ICALP), 1-12.
- Narayanan, A., & Shmatikov, V. (2008). "De-anonymizing Social Networks." IEEE Symposium on Security and Privacy, 173-187.
- Zyskind, G., & Nathan, O. (2015). "Decentralizing Privacy: Using Blockchain to Protect Personal Data." IEEE Security & Privacy, 4(7), 7-12.
- Cavoukian, A. (2012). "Privacy by Design: The 7 Foundational Principles." International Conference on Privacy and Data Protection.
- Taddeo, M., & Floridi, L. (2018). "The Ethics of Artificial Intelligence: A European Perspective." Springer, 88-102.

- Jagadish, H. V. (2015). "Data Privacy and the Big Data Revolution." *Communications of the ACM*, 58(1), 62-72.
- Shokri, R., & Shmatikov, V. (2017). "Privacy-Preserving Machine Learning." *ACM Transactions on Privacy and Security*, 19(2), 1-30.
- Greenleaf, G. (2014). "Global Data Privacy Laws 2014: 107 National Laws and Counting." *Journal of Law and Information Science*, 25(2), 153-190.
- Greenleaf, G., & Cumbley, R. (2013). "Data Privacy Laws and the Internationalization of Privacy." *International Journal of Law and Information Technology*, 21(3), 253-281.
- Voigt, P., & Von dem Bussche, A. (2017). "The GDPR: A Complete Guide to the General Data Protection Regulation." Springer.
- Islam, R., & Fernandes, M. (2016). "Data Security Challenges in the Cloud." *Cloud Computing and Big Data*, 12(4), 195-207.
- Pentland, A. (2012). "Social Physics: How Good Ideas Spread." Penguin Press.
- Christidis, K., & Devetsikiotis, M. (2016). "Blockchains and Smart Contracts for the Internet of Things." *IEEE Access*, 4(1), 2292-2303.
- Khatri, V., & Brown, C. V. (2010). "Designing Data Governance." *Communications of the ACM*, 53(1), 10-12.
- Acquisti, A., & Grossklags, J. (2016). "Privacy and Rationality in the Age of Big Data." *IEEE Security & Privacy*, 6(4), 11-19.
- Dwork, C., & Roth, A. (2014). "The Algorithmic Foundations of Differential Privacy." *Foundations and Trends® in Theoretical Computer Science*, 9(3-4), 211-407.
- Taddeo, M. (2018). "The Ethics of Data Privacy and Algorithmic Governance." *Oxford Handbook of Ethics of AI*, 124-146.
- Dib, J., & Ritchie, K. (2017). "Data Breaches and Their Impact on Privacy: A Review." *Journal of Information Privacy and Security*, 9(4), 215-234.
- Martin, K., & Shih, T. (2019). "Digital Privacy Rights in the Age of Big Data." *Harvard Journal of Law & Technology*, 32(1), 29-54.
- Zwitter, A. (2014). "Big Data Ethics." *Big Data & Society*, 1(2), 1-13.

- Ahmad, N. R. (2025). *Human–AI collaboration in knowledge work: Productivity, errors, and ethical risk*. *Journal of Humanities and Social Sciences*.
<https://doi.org/10.52152/6q2p9250>
- Ahmad, N. R. (2025). *Urban water service delivery in emerging economies: Fiscal sustainability, cost recovery, and governance performance*. *International Journal of Business and Economic Analysis*. <https://doi.org/10.24088/IJBEA-2025-103005>