SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

Predictive Quality Management in Nepalese Artificial Intelligence and Data Privacy: Navigating Cyber Laws in the Age of Machine Learning

Dr. Pushkar Shankar Shukla[1], Mr. Satish Marutrao shirsath[2], Gohel Abhijit Jivanbhai[3], Dr. Koteswararao. P[4], Dr Amit Kumar[5], Dr. Amol B. Kasture[6]

[1]LLB, LLM, PhD, MATS University, Raipur. E-mail: pushkarss@rediffmail.com, ORCID Id - 0009-0005-7863-4235
[2]Assistant Professor, Pravara Rural Engineering College Loni, Savitribai Phule Pune University, Pune. E-mail: satish.shirsath@pravara.in
[3]System administrator and computer programmer, School of Engineering and Technology, Dr. Subhash University, Junagadh- 362001, Gujarat, India. E-mail: gohelabhijit3@gmail.com, ORCID: 0009-0000-3230-3434
[4]Associate Professor, Department of Physics, Ace Engineering college, Ankushapur (V), Ghatkesar (Mandal), Ranga Reddy (Dt), Telangana, PIN Code -501301. E-mail: koteswarphd@gmail.com
[5]Assitant Professor, Army Institute of Law, Mohali. E-mail- bhardwaj22195@gmail.com, ORCID: 0009-0005-7738-0579
[6]Associate Professor, SOE -Ajeenkya DY Patil University, Pune. ORCID: https://orcid.org/0000-0002-1200-4514,
E-mail: amol.kasture@adypu.edu.in, amolia2004@gmail.com

ABSTRACT
Artificial intelligence (AI) and machine learning requires massive amounts of personal and sensitive information, resulting in important challenges in protecting privacy and cyber-legal governance. This review explores how the relationship between AI, data privacy and regulatory frameworks has developed, particularly within the context of the main privacy risks, individual rights, regulatory bodies and emerging governance issues. Issues of particular concern are the excessive collection of data, algorithmic profiling, surveillance, re-identification of the collected data, training-data leakage, automated decisions, and data processing across borders. It reviews key regulatory strategies, such as the General Data Protection Regulation (GDPR), the European Union (EU) Artificial Intelligence Act (AI Act) and the developing national privacy laws, while noting the fragmentation of regulation, accountability challenges and enforcement issues. Some of the more important tools for mitigating emerging risks are the methods that preserve privacy, such as federated learning, differential privacy, encryption, explainable AI, and algorithmic auditing. Key features of adaptive cyber laws for effective AI Governance include incorporating technological protections, ethical oversight, organizational accountability, and international coordination, along with ensuring a balance between technological innovation and core privacy rights.

Keywords: Artificial intelligence, Cyber law, Data privacy, Machine learning, Privacy-preserving AI

Introduction

Artificial Intelligence (AI) and Machine Learning (ML) have become a key part of the modern digital transformation and are impacting the way that information is generated, processed, interpreted and used in both the public and private sectors. Advances in data-intensive technologies have allowed companies to identify complex patterns in big and diverse data sets that can be used for automation, prediction, personalization and decision-making on a scale that would have been impossible a few years ago. But at the same time, this transformation has exacerbated the concerns around the gathering and exploitation of personal data. The fusion of the Big Data and AI has challenged the principles of the law, as traditional legal concepts were created before the widespread advent of automated, large-scale, and inferential data processing (Mania, 2022). So privacy protection has become more than merely an information-security issue; it's a fundamental issue of technology, law, governance and individual rights.

In the era of Artificial Intelligence (AI), data is a critical component in the building and execution of AI systems. Personal identifiable information, behavioral data, financial data, biometric data, location data, and online activity are among the sensitive data elements that can be used directly or indirectly for algorithmic training and decisionmaking. This dependency generates conflicts between the need to access broad sets of data and existing privacy values like privacy by design, purpose limitation, transparency and minimization of data. Current laws and regulations might not be able to keep up with the volume, speed, and complexity of data processing by AI, especially when data are linked together to produce new insights about people (Mania, 2023). In general, from a technical and philosophical point of view, the protection of privacy with ML is more complicated than ensuring that no one will have access to identifiable records (Asgarinia, 2024).

The whole lifecycle of AI is surrounded by privacy issues. Data can be gathered without adequate meaningful consent, subsequently used for other goals than those communicated, transferred to other organizations, or entered into models whose behavior after the transfer is hard to follow. Algorithmic profiling is the ability to classify people based on predictions regarding their preference, risk, behaviour or socio-economic status, and facial recognition and other biometric technologies can enable the ability to persistently identify and monitor individuals. This swift evolution of neural networks and sophisticated artificial intelligence techniques consequently presents an ongoing challenge between technological advancement, the production of information, ethical obligation, and privacy safeguarding (Fabiano, 2025). AI has the potential to change the paradigm of data privacy by not only changing the quantity of information that is available regarding the individual, but also the ability to infer, connect and use that information. (Lami et al., 2024)

The developments have implications of fundamental rights. Privacy is not simply about hiding or keeping safe, but also about a person's right to control and to select information, their autonomy, their dignity, and informational self-determination. Such control can be undermined by the use of AI monitoring, profiling, and automated decision-making, especially when an individual is unaware of how their data will be used to inform important algorithmic outcomes. This emerging power of AI therefore necessitates a context for privacy beyond organizational compliance and cybersecurity and in the context of human rights (Adu Wiafe, 2026). The issue of accountability becomes salient when the responsibility for the negative consequence is shared among data providers, model creators, technology vendors, deploying organizations, and automated systems.

AI's connection with data privacy, however, is a complicated one. AI is new threats to privacy, but it can also strengthen the cybersecurity and data-protection landscape. Intelligent security systems can help to identify anomalies, detect threats, prevent fraudulent activity, and ensure that people are not allowed to enter the premises too fast and that their behavior isn't suspicious. Therefore, AI in cybersecurity architectures provides an opportunity to increase the level of protection of the organization from valuable information (Abdur-Rashid, 2024). The effectiveness of data protection can be further analyzed by increasingly advanced analytical and causal modelling techniques which may enable a more structured evaluation of interventions in privacy by organisations and policy makers. AI and privacy should not, therefore, be considered as potential threats to privacy only, but as an opportunity to increase the potential for privacy governance in the context of new technologies.

The regulation of AI systems with cross-border applications and digital infrastructures becomes more complex. Information can be collected in one jurisdiction, stored in another, retrieved through systems created in another jurisdiction, and decision made about individuals across jurisdictions.Information can be collected in one jurisdiction, stored in another, processed by systems constructed in another jurisdiction, and processed across jurisdictions for decision making about persons. Such situations create problems concerning the traditional borders and have posed a challenge for regulation. Advanced technologies also meet cybersecurity, surveillance, state control and national security goals, resulting in complex issues of proportionality between collective security and individual privacy (Montasari, 2024). Meanwhile, the growing data science and intelligent technologies environment expands the technological area in which privacy law operates.

Cyber laws and data protection regulations have to therefore, evolve in tandem with the growing intricacy of AI systems. While these principles are important to understand in regards to consent, transparency, lawful processing, accountability, access, and data security, their applicability to the constantly evolving ML systems is still under debate. Algorithmic opacity and transparency, reuse of data, cross-border data processing, automated decisions and generative artificial intelligence, and accountability all point to a need for increased harmonization between technological protection and legal governance. To identify whether existing cyber legislation offers adequate protection of privacy and whether it is not overly stifling socially and economically beneficial innovation, it is essential that these issues be thoroughly examined.

This review thus critically examines the dynamic relationship between AI, data privacy and cyber law, with particular attention to the new risks, regulatory measures, legal obligations, and privacy protection strategies. The review is guided by three objectives:

To examine major data privacy risks arising from artificial intelligence and machine learning applications across digital environments

To critically evaluate existing cyber laws and regulatory frameworks governing AI-driven collection and processing of personal data

To identify regulatory gaps and privacy-preserving strategies for strengthening accountable, rights-respecting, and legally compliant AI governance

2. Artificial Intelligence and the Evolving Data Privacy Landscape

2.1 Evolution of AI and Machine Learning Technologies

AI is no longer just a computational machine based on rules; it is now an advanced machine learning system that can recognize patterns, make predictions, and adjust to complex datasets. This shift has been hastened in scientific and commercial applications by a number of recent advances in computer hardware, data, neural networks, and algorithm design. In the era of modern AI, it is now more associated with data science and automated analytical processes that can perform tasks normally performed by a human in the loop (Reddy et

al., 2026). This new technological phase has also created new requirements for the emergence of responsible, sustainable and risk-aware Artificial Intelligence (AI) (Haidar, 2024).

2.2 Personal and Sensitive Data in AI Systems

Personal and sensitive information is often the data foundation for many AI systems, such as for training, personalization, authentication, prediction, and decision-making. This can encompass demographic data, financial information, biometric data, health data, patterns of behavior, communications, and location information. With the growing interdependency of AI applications with digital communication systems and Internet of Things infrastructures, the amount and variety of information being gathered is also increasing (Ullah et al, 2024). Privacy protection therefore needs to be realized through protection measures throughout the data collection, processing, model development, deployment and monitoring processes, not just through security measures targeted to specific processes (Boadi, 2025).

2.3 Big Data, Profiling, and Automated Decision-Making

The combination of AI and big data has greatly increased the ability to classify, predict and automate decision making with respect to individuals. Algorithms can bring together data from a variety of sources to create a detailed profile, which can affect recommendations, eligibility, security clearance and other important outcomes. These features enable disruptive innovation and organizational efficiency, but they also raise issues of transparency, fairness, data accuracy and meaningful individual control (Akabagy, 2024). When automated decisions have significant consequences for people, it becomes more and more critical to have responsible AI frameworks in place to mitigate risks (Haidar, 2024).

2.4 Generative AI, Large Language Models, and Personal Data

The use of generative AI and LLM has raised privacy concerns as they are often trained on very large, diverse datasets. During training, information may be received that includes public data as well as data whose origin and access to it by other people, including those trained, is not easy to trace. The generated outputs may also include components that reproduce, infer or combine information in ways that make traditional methods of data governance challenging. As the technologies evolve, so do the emerging issues around consent, accountability, transparency, and regulatory responsibility that call for legal frameworks to adapt to the changing AI capabilities and the jurisprudential issues that arise. (Virk, 2026)

2.5 AI Applications in Data-Intensive Industries

AI applications have become seamlessly integrated into various sectors, such as healthcare, finance, cybersecurity, education, commerce, transportation, communication, and public administration, where significant amounts of personal data are processed often. In the field of cybersecurity, machine learning can be used to recognize unusual behavior, detect threats, bolster authentication mechanisms, and enhance the ability to counter changing attacks (Young, 2025). In other industries, similar capabilities for prediction and automation are data driven. But a wider rollout raises privacy concerns when sensitive information is exchanged or processed across interdependent systems, highlighting the need for embedding privacy aspects explicitly in AI governance and day-to-day operations (Boadi, 2025).

2.6 Transformation of Traditional Concepts of Privacy

AI is not just shifting the paradigm of privacy from one focused on access control to one focused on inference and prediction, on autonomy and algorithmic power, but it is doing so by doing both. Some personal data can be shared, and AI systems can learn other attributes by correlating and analyzing behaviour. As a result, it is becoming more difficult to continue to separate identifiable and non-identifiable information. The legal implications of algorithmic systems therefore need to be understood from a new angle when it comes to the transformation of individual rights and institutional duties (Virk, 2026). To meet the growing demands for privacy protection, multiple layers of security are necessary to defend privacy threats in interdependent technological and organizational contexts (Boadi, 2025) (Figure 1).

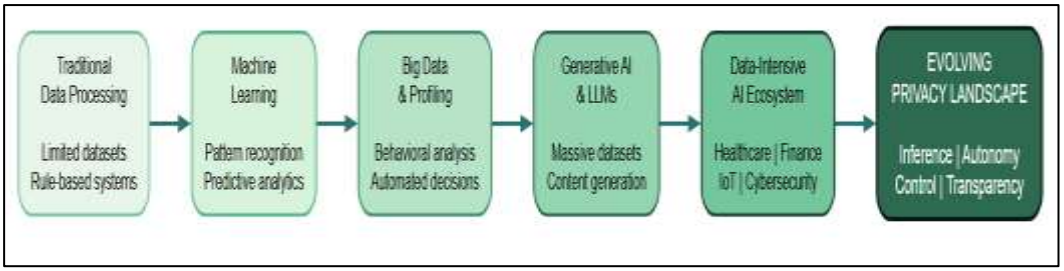

Figure 1. Evolution of Artificial Intelligence and the Changing Data Privacy Landscape

3. Data Privacy Risks in AI and Machine Learning Systems

3.1 Excessive Data Collection, Consent, and Purpose Limitation

AI systems can frequently rely on large datasets, which can lead organizations to gather more data than is immediately required for a specific application. Such practice may compromise data minimization, informed consent and purpose limitation in the context of reusing data for model building or other forms of analysis that are off-target. With AI-driven environments for Internet of Things applications expanding and the data itself continuously gathered and often invisible to the user, it can be hard to keep the data meaningful and relevant to the user's awareness (Chimbga, 2025). Coping with responsible computing, it is necessary to have a clear purpose for the use of processing and a proportional and proportional collection of data at all stages of the AI life cycle (Ouanhlee, 2026).

3.2 Algorithmic Profiling, Behavioral Tracking, and Surveillance

Machine learning can help organizations and public authorities to generate detailed profiles continuously based on behavioral, transactional, biometric and contextual data. Such profiling can be used to provide personalized services and risk assessment, but can also enable continued tracking and surveillance, sometimes with little transparency. In the field of law enforcement, for example, AI-powered monitoring systems and automated evaluations can have an impact on the right to privacy and freedom of movement of both individuals and communities (Merler, 2026). The same profiling in commercial domains can have an impact on risk classification and decision-making, causing ethical issues of fairness, autonomy and discriminatory consequences (Shafik, 2026).

3.3 Re-identification and De-anonymization of Personal Data

Historically, anonymization has been employed to minimize risk of privacy breaches by removing direct identifiers from datasets. AI analytic features, however, can tie together various characteristics and external data sources that, when compiled, can re-connect seemingly anonymous data and individuals. A vulnerable situation arises when the IoT devices are connected to each other, as they are constantly creating behavioral, spatial, and contextual information that can be combined to reveal identity (Jaafar & Pierre, 2023). As computational analysis improves, this means that assumptions that removing explicit identifiers is good enough protection will need to be strengthened in all stages of data storage, sharing, and processing, introducing the need for more effective methods for protecting privacy (Ouanhlee, 2026).

3.4 Training-Data Leakage, Memorization, and Model-Based Privacy Attacks

Even if the datasets used for training machine learning models are no longer directly available, they can still induce privacy vulnerabilities. Complex models may carry knowledge of the learned examples around with them and, with intelligent queries, sensitive attributes or records may be deduced. These vulnerabilities extend privacy beyond traditional database security, as sensitive data can be indirectly included in model parameters or outputs. This, of course, mandates privacy protection during model development, from training and validation to deployment as well as post-deployment monitoring (Ouanhlee, 2026). Such risks can be especially significant in regulated industries, where models are handling highly sensitive data (Shafik, 2026).

3.5 Data Breaches and Unauthorized Access to AI Systems

Cyberattacks are drawn to the attractive opportunities presented by AI infrastructures, as they can include valuable training data, sensitive operational data, model parameters, and user-generated information. Unauthorized entry may lead to confidentiality issues, and allow for manipulation of models or downstream processes. The rise of AI within a network of digital identity and IoT devices further proliferates attack surfaces, making secure authentication, access control and privacy preserving architectures even more critical (Jaafar & Pierre, 2023). The convergence of AI and cyber operations, combined with evolving and complex threat landscapes, poses heightened security risks in these areas (Kumar, 2025).

3.6 Cross-Border Data Processing and Third-Party Data Sharing

AI services are often delivered through multi-cloud architectures and multiple external technology vendors, data brokers, and developers in various jurisdictions. Personal data can thus be transferred from one jurisdiction to another one with varying information privacy laws, regulations and standards. These arrangements exacerbate accountability issues through a proliferation of responsibility for collection, processing, storage, and subsequent disclosure. There is also an additional layer of uncertainty when handling data across countries due to differences between emerging AI governance frameworks (Kumar, 2025). There is a need for robust governance arrangements to support access to third parties, data movements and organisational accountability in interconnected AI + IoT environments (Table 1) (Chimbga, 2025).

Table 1. Major Data Privacy Risks Associated With AI Systems

Privacy risk	AI-related	Main concern	References

	mechanism		
Excessive collection	Large-scale model training	Consent and purpose creep	(Chimbga, 2025)
Profiling	Behavioral prediction	Surveillance and discrimination	(Merler, 2026)
Re-identification	Dataset linkage	Loss of anonymity	(Jaafar & Pierre, 2023)
Training leakage	Model memorization	Sensitive-data exposure	(Ouanhlee, 2026)
Data breaches	AI infrastructure attacks	Unauthorized disclosure	(Kumar, 2025)
Cross-border processing	Distributed AI services	Jurisdictional uncertainty	(Chimbga, 2025)

4. Cyber Laws and Regulatory Frameworks Governing AI and Data Privacy

Cyber laws and data protection laws have dramatically changed to adapt to the fast pace of digitization, moving from rules that mainly tackle with computer misuse, electronically conducted transactions, and cybersecurity towards rules that tackle with personal information, automated processing and algorithmic accountability. The advent of AI has only compounded this shift, as data-driven and increasingly self-governing systems pose issues that traditional laws were not intended to solve, and require frameworks that can keep up with innovation while protecting individual rights (Pokhariyal et al., 2026). In Europe, the General Data Protection Regulation (GDPR) contains principles of lawfulness, fairness and transparency; the limitation of use for the purposes for which the data is collected; minimization of data; security and accountability.In Europe, the General Data Protection Regulation (GDPR) has direct implications for the principles applied to AI systems processing personal data, including those of lawfulness, fairness and transparency; limitation of use for the purposes for which the data is collected; minimization of data; security; and accountability. These safeguards are further reinforced by the EU Artificial Intelligence Act, which takes a risk-based approach to regulation, with the level of legal obligations depending on the level of risk and the potential impact of the AI application (Al-Haija et al., 2025). The U.S. regulatory landscape is significantly more fractured, with agency-specific regulations at the federal level, state privacy laws, regulatory guidelines, and new AI governance efforts. Such a setup yields a complicated compliance landscape, especially within the financial services sector where AI innovation needs to sync with privacy, security, data engineering, and regulatory demands (Paleti, 2025). India has also enhanced its stance on digital privacy with the speed of digitization raising concerns about personal-data processing, cybersecurity, data transfers across borders, and data localisation. Consequently, privacy and localization have emerged as key components of India's evolving regulatory framework and overall digital-governance policy (Vidya, 2025). There are, however, significant disparities across different countries with regards to regulatory definitions, enforcement strategies, localization obligations, and strategies for accountability for AI. The challenges are especially troublesome when AI functions in a distributed network across the globe or when it relies on multiple jurisdictions to access information (Mohaghegh Montazeri 2026). This is even more important for the development of effective global AI governance as well as responsible technological development, particularly with regards to greater regulatory coordination, interoperable standards and alignment of principles towards cybersecurity and data protection (Table 2) (Figure 2) (Pokhariyal et al., 2026).

Table 2. Major Regulatory Frameworks Relevant to AI and Data Privacy

Jurisdiction	Regulatory approach	Primary focus	Key challenge	References
European Union	GDPR	Personal-data rights	AI application complexity	(Al-Haija et al., 2025)
European Union	EU AI Act	Risk-based AI governance	Implementation and compliance	(Pokhariyal et al., 2026)
United States	Sectoral/state model	Sector-specific privacy	Regulatory fragmentation	(Paleti, 2025)
India	Data protection framework	Privacy and data governance	Cross-border processing	(Vidya, 2025)
International	Diverse frameworks	AI governance	Lack of harmonization	(Pokhariyal et al., 2026)

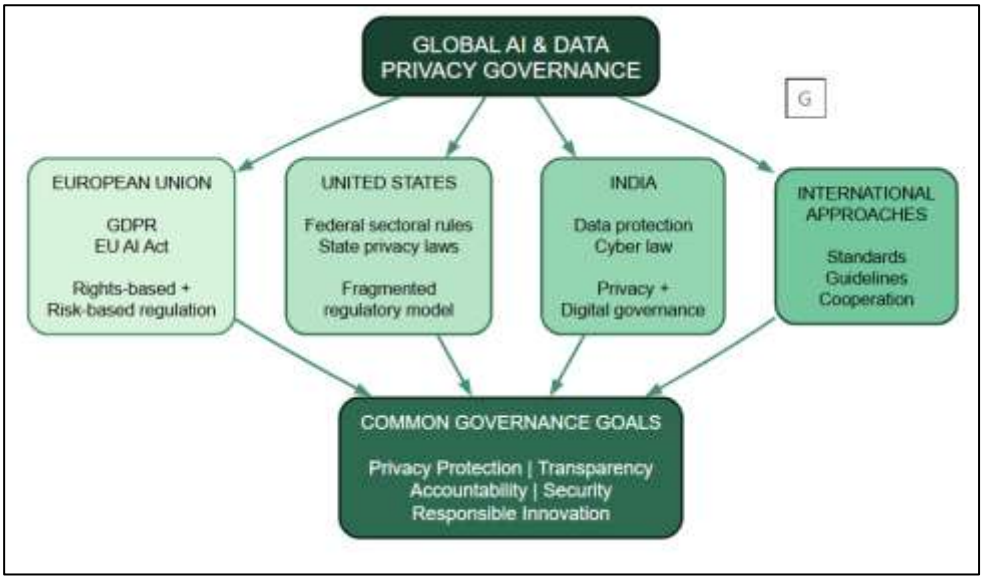

Figure 2. Comparative Landscape of AI and Data Privacy Regulation

5. Privacy Rights and Legal Obligations in AI-Based Data Processing

As AI becomes more deeply embedded in the processing of personal data, the significance of privacy rights and clear legal responsibilities has grown, across the entire lifespan of AI. Organizations must have valid reasons for processing, and ensure transparency and informed consent by explaining the data collection, analysis, and usage processes in algorithmic systems, especially considering the growing focus on AI governance and individual rights protection (Marwala, 2026). These requirements are closely related to purpose limitation and data minimization, which state that the information to be collected should be for specific purposes and only for what is needed to meet those purposes. In fact, the impact of unnecessary exposure of sensitive data while preserving the analytical value of the data has drawn attention, notably in the field of healthcare where data is abundant (Pareshkumar, 2025). There should also be meaningful ways for people to access their personal information, to correct inaccurate data, and to get or transfer their data, where that is legally allowed, to increase control in increasingly automated digital environments (Buckley, 2025). The right to erasure also complicates things as deleting data from traditional databases could not negatively impact the models that have already been trained on these data. The task of machine unlearning thus is an emerging technical and legal challenge that demands techniques capable of decreasing or eliminating the impact of specific training data by not retraining the entire model (Saxena, 2026). Another concern is the destructive influence of automated decision making when there is little or no transparent reason or means by which individuals can challenge the results of algorithms. The right to explanation and principles of transparency, therefore, aim to contribute to the interpretability and contestability of consequential automated decisions, in the broader context of a developing cyber-law jurisprudence (Ranjitsingh, 2025). At the same time, accountability needs to be broadened throughout the AI value chain.There is a need to hold the entire AI value chain accountable at the same time. The system designer should include adequate privacy and security protections and the data controller should be responsible for identifying lawful processing purposes and taking measures for proper governance. Processors and technology suppliers will also have to take appropriate security measures and meet the processing requirements (Razavi et al., 2026). As AI becomes intertwined with other networked technologies and enters the organizational cyber-risk landscape, the responsibilities grow in significance. For privacy governance to be effective, there must be coordinated and integrated legal, technical, and organizational accountability and safeguards for the protection of individual rights to enable responsible AI innovation (Figure 3) (Table 3).

Table 3. Privacy Rights and Legal Obligations in AI-Based Data Processing

Privacy right/principle	Application to AI	Legal/organizational obligation	References
Lawfulness and transparency	Personal-data processing	Disclose purpose and lawful basis	(Marwala, 2026)
Informed consent	AI training and profiling	Obtain meaningful consent where required	(Buckley, 2025)
Data minimization	Model development	Limit unnecessary data collection	(Pareshkumar, 2025)
Access and correction	Stored personal data	Enable review and rectification	(Buckley, 2025)

Right to erasure	Trained AI models	Support deletion and machine unlearning	(Saxena, 2026)
Right to explanation	Automated decisions	Improve transparency and contestability	(Ranjitsingh, 2025)
Accountability	AI lifecycle	Define developer, controller, and processor duties	(Razavi et al., 2026)

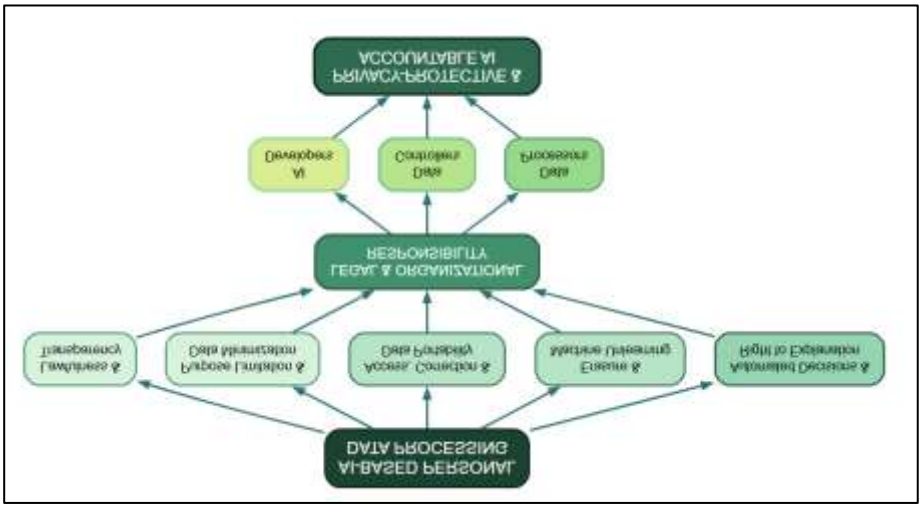

Figure 3. Privacy Rights and Legal Responsibilities Across the AI Data-Processing Lifecycle

6. Ethical, Legal, and Accountability Challenges of AI

As AI technology becomes more autonomous and sophisticated, it raises a whole new set of ethical, legal and accountability issues beyond traditional data protection issues. The opacity of algorithms is especially problematic because highly sophisticated machine-learning algorithms can be "black boxes," which makes it hard to understand how certain outcomes are being created for users, regulators, and affected people. It can also hinder transparency and the capabilities of ethical governance if AI is utilized in domains with serious consequences, such as healthcare (Singh et al., 2025). The challenge of algorithmic bias is also evident as models developed from incomplete, historically skewed, or unrepresentative data may reinforce or perpetuate inequalities, and concerns about fairness and discriminatory results extend beyond industrial/organizational contexts. When bad things happen as a result of developer interactions with data providers, deploying organizations and autonomous systems, it is harder to hold the other party accountable. Lack of accountability and responsibility can thus be avoided by having a clear allocation of responsibility and accountability so as to prevent technological complexity to create an accountability gap. The consequences of automated risk assessments and decisions can be significant for individuals, especially in sectors that are transforming due to AI (Kelaidi, 2025). Connected digital environments produce information continuously which can be collected, merged, and monetised by a variety of parties, which raises other concerns regarding data ownership and informational autonomy. As IoT ecosystems continue to grow, the need to discuss issues of data propertization, control, access, and the scope and limits of personal rights to data created through digital technologies has come back into the spotlight (Lawrence-Ogbeide, 2025). Ethical limits are also being pushed with the integration of AI-powered surveillance and biometric systems, which allow for constant identification, tracking, and predictive analysis of behavior and actions (Karwowski et al., 2025), thereby further diminishing anonymity and individual autonomy in technologically dominated settings (Soofastaei, 2026). When intelligent systems are integrated into transportation or other public infrastructures where there is a large deployment of sensor networks that facilitate real-time data gathering and automatic reacting, these concerns grow even more important (Ouaissa et al., 2026). There is, therefore, a need for human oversight to ensure respect for a fundamental right when decisions are automated and have an impact on privacy, equality, safety or access to essential opportunities. Effective governance of AI should remain grounded in meaningful human intervention and provide opportunities to challenge decisions that have consequences, while also ensuring efficiency and automation does not undermine dignity, autonomy, fairness, and other fundamental rights (Figure 4) (Table 4).

Table 4. Ethical, Legal, and Accountability Challenges Associated With AI

AI challenge	Principal concern	Governance requirement	References
Algorithmic opacity	Unclear decision processes	Explainability and transparency	(Singh et al., 2025)

Algorithmic bias	Unfair or discriminatory outcomes	Bias assessment and fairness controls	(Karwowski et al., 2025)
Accountability	Unclear responsibility for harm	Defined liability mechanisms	(Kelaidi, 2025)
Data ownership	Reduced individual control	Informational autonomy safeguards	(Lawrence-Ogbeide, 2025)
AI surveillance	Privacy and autonomy intrusion	Proportionality and ethical limits	(Soofastaei, 2026)
Biometric monitoring	Persistent identification	Strong privacy safeguards	(Ouaissa et al., 2026)
Limited human oversight	Unchecked automated decisions	Meaningful human intervention	(Singh et al., 2025)

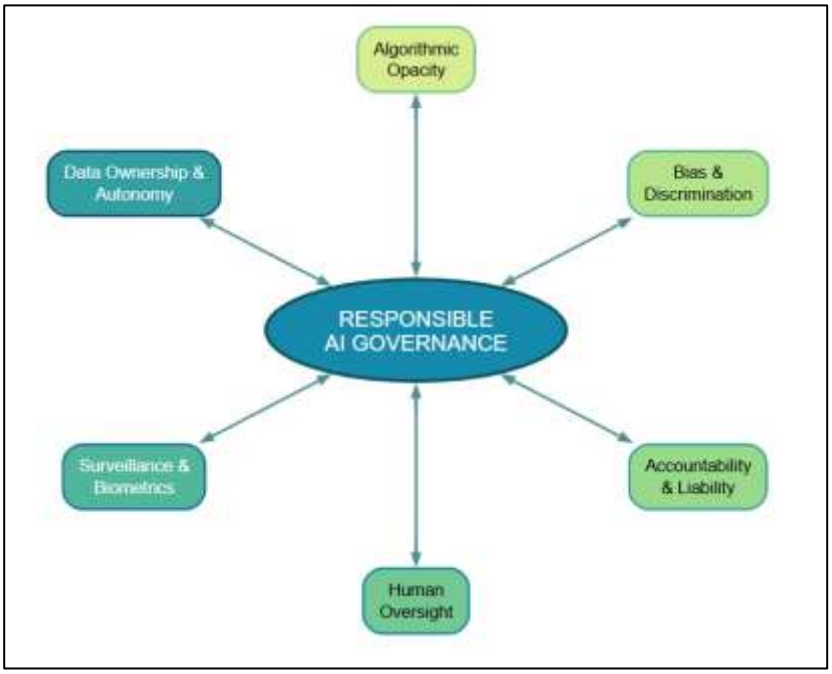

Figure 4. Interaction of Ethical, Legal, and Accountability Challenges in AI

7. Gaps and Limitations in Existing Cyber Laws

The current state of cyber legislation is inadequate to harmonize the regulatory landscape across jurisdictions and result in regulatory fragmentation, as definitions, compliance obligations, risk classification, and enforcement standards differ. The AI-related legal obligations are also not homogenous across jurisdictions, which makes it challenging for organisations to deploy across legal jurisdictions (Artzt et al., 2024). Another hurdle is the rate of innovation in AI technologies, with legal frameworks lagging behind in certain sectors such as autonomous systems, edge computing, and smart engineering applications (Jayaram, 2026). The advent of generative AI and foundation models brings fresh legal challenges due to their extensive training data, multipurpose applications and ability to produce new content that challenges traditional legal principles of consent, transparency, intellectual property and personal data usage (Lomurno, 2024). The accountability is also divided between the actors in the AI value chain, including data provider, the developer, the deployer, the platform operator, and the end user, and where they may have an influence without knowing exactly who is accountable for what. This limits the effectiveness of liability arrangements where the decision-making process is complex and spread out, causing harm (Sekwena, 2025). The enforcement challenge is exacerbated by jurisdictions, cloud infrastructure, distributed processing, and cross-border transfers, particularly in regulated areas like banking, finance, cybersecurity, and other regulated industries (Joyisa, 2025). New privacy-enhancing solutions, like federated learning, could limit the exposure of sensitive data from a central place, but they can't replace the requirement for cross-jurisdictional harmonization of laws and regulations (Sah et al., 2026). AI processes can be executed in the cloud or at the edge, creating additional layers of regulation as data might be processed on a number of different devices, places and legal jurisdictions at once (Khari et al., 2026). Moreover, ethical principles are not enough if they are not backed up by enforceable rule, monitoring and clear accountability systems (Shafik, 2024). The limitations outlined above emphasize the need for stronger harmonization of international regulation by ensuring interoperability of standards, a common understanding of risks, coordinated enforcement and transparent mechanisms for assigning accountability for incidents

across borders all of which must be able to evolve to keep pace with the pace of AI's development. (Table 5) (Figure 5).

Table 5. Key Gaps in Existing Cyber Laws for AI

Regulatory gap	AI-related challenge	Required response	References
Fragmentation	Conflicting national rules	Regulatory interoperability	(Artzt et al., 2024)
Technology lag	Rapid AI evolution	Adaptive legislation	(Jayaram, 2026)
Generative AI	Uncertain data provenance	AI-specific safeguards	(Lomurno, 2024)
Accountability	Multiple AI actors	Clear liability allocation	(Sekwena, 2025)
Cross-border governance	Distributed processing	Coordinated enforcement	(Joyisa, 2025)
Edge AI	Decentralized processing	Distributed governance	(Khari et al., 2026)

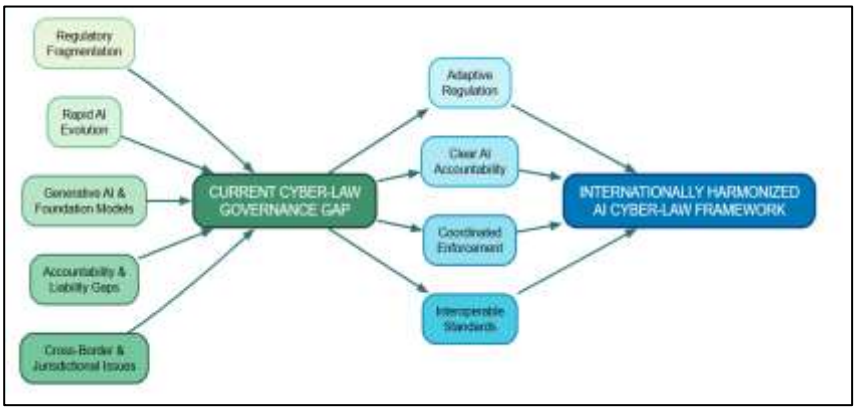

Figure 5. Regulatory Gaps and Pathway Toward Harmonized AI Cyber Law

8. Privacy-Preserving AI and Future Directions for Cyber Law

To ensure privacy-preserving AI, technical measures, ethical data stewardship, and flexible legal frameworks need to be in place throughout the AI lifecycle. Using privacy by design would ensure that privacy principles of data minimization, purpose limitation, access controls and accountability are built into the system from its inception instead of tacked-on. Federated learning is one possibility that allows for decentralized model training without the frequent transfer of personal data to central repositories, but with the need for governance of the devices participating and updates to the models. Differential privacy can additionally minimize disclosure danger by adding controlled statistical noise, and encryption, homomorphic techniques, and secure multiparty computation can secure information in storage, transmission, and collaborative processing. However, technical protection is not enough to address concerns of opaque or consequential algorithmic decisions. Explainable AI, independent algorithmic auditing, privacy and algorithmic impact assessment, are therefore key to assessing transparency, discrimination, security vulnerabilities and potential impacts on fundamental rights both prior to, and in the context of, deployment. At the same time, cyber law needs to be more adaptive, as a fixed and uniform regulatory strategy may quickly fall behind the changing times as generative AI, foundation models, autonomous systems and decentralized technologies develop. It is especially vital to also create interoperable principles for cross-border data processing, accountability, risk assessment and regulatory enforcement through cooperation between international partners. Going forward, it is important to promote privacy enhancing technologies and set clear compliance standards and oversight. Organizations should have extensive AI governance frameworks, documentation, security measures, and regular risk assessments, while researchers should focus on machine unlearning, explaining AI, safeguarding privacy during computation, and developing tools to assess new risks arising from AI algorithms. These measures can collectively contribute to an ecosystem in which technological innovation evolves, alongside enforceable privacy rights, accountability of institutions and respect of individual rights.

9. Conclusion

The collection, analysis and application of personal data has been revolutionized by the advent of AI and machine learning, which presents significant opportunities and a growing level of privacy threats. The following issues are highlighted and represent new challenges for the traditional privacy protection: excessive data collection, algorithmic profiling, surveillance, re-identification, training-data leakage and automated

decision-making, and cross-border processing. Although the GDPR and the EU AI Act provide robust protections, there are barriers to effectiveness arising from regulatory fragmentation, jurisdictional differences, technological complexities and lack of accountability. The concerns are compounded by generative AI and foundation models which are attacking core consent, transparency, purpose limitation, erasure, and personal control over data concepts. Good governance is more than just the right regulations. Technical and organizational measures like privacy by design, federated learning, differential privacy, and secure computation, as well as explainable AI and algorithmic auditing, and impact assessments, can reinforce each other. Future cyber-law should emphasize responsive, risk-based, interoperable law – flexible and responsive to new technologies, but not to preclude beneficial innovations. Proper delegation of responsibilities by the developers, deployers, controllers and processors is also crucial. Ethical guidelines and international cooperation, alongside legal frameworks and technical measures, are essential to ensure that the development of sustainable AI governance does not impact privacy, autonomy, transparency, and fundamental rights.

References

1. Abdur-Rashid, A. N. (2024). Advancing Business Data Privacy Through Artificial Intelligence in Cybersecurity: A Quantitative Analysis of Mobile Technology Enhancements (Doctoral dissertation, National University).
2. Adu Wiafe, A. (2026). The Impact Of Artificial Intelligence On The Right To Privacy: A Human Rights Perspective. The Impact Of Artificial Intelligence On The Right To Privacy: A Human Rights Perspective (January 01, 2026).
3. Akabagy, E. B. (2024). A Bibliometric Review on Exploring the Role of Artificial Intelligence in Disruptive Innovation.
4. Al-Haija, Q. A., Maleh, Y., & Odeh, A. (Eds.). (2025). Intelligent and Secure Solutions for Digital Transformation. CRC Press.
5. Artzt, M., Belitz, O., Hembt, S., & Lölfing, N. (Eds.). (2024). International handbook of AI law: a guide to understanding and resolving the legal challenges of artificial intelligence. Kluwer Law International BV.
6. Asgarinia, H. (2024). Privacy and Machine Learning-Based Artificial Intelligence: Philosophical, Legal, and Technical Investigations.
7. Boadi, P. (2025). Prioritizing Privacy in Artificial Intelligence: A Practitioner-Grounded, Layered Framework.
8. Buckley, G. (2025). Privacy at the intersection of technology, business and regulation: A case study of the GDPR (Doctoral dissertation, UCL (University College London)).
9. Chimbga, B. (2025). Towards the Artificial Intelligence of Things (AIoT): A review of the ethical and societal implications at the convergence of AI and IoT technologies in South Africa (Doctoral dissertation, University of Pretoria).
10. Fabiano, N. (2025). Artificial Intelligence, Neural Networks and Privacy: Striking a Balance between Innovation, Knowledge, and Ethics in the Digital Age. goWare.
11. Haidar, A. (2024). Responsible Artificial Intelligence: designing frameworks for ethical, sustainable, and risk-aware practices (Doctoral dissertation, Université Paris-Saclay).
12. Jaafar, F., & Pierre, S. (Eds.). (2023). Blockchain and Artificial Intelligence-based Solution to Enhance the Privacy in Digital Identity and IoT. CRC Press.
13. JAYARAM, M. (2026). ARTIFICIAL INTELLIGENCE AND APPLICATIONS IN CORE ENGINEERING. PHI Learning Pvt. Ltd..
14. Joyisa, T. (2025). Artificial Intelligence for Cybersecurity: Governance Insights From Cybersecurity Experts in the Banking Industry in South Africa (Doctoral dissertation, University of the Witwatersrand, Johannesburg (South Africa)).
15. Karwowski, W., Duffy, V. G., & Salvendy, G. (Eds.). (2025). Advances in Artificial Intelligence Applications in Industrial and Systems Engineering. John Wiley & Sons.
16. Kelaidi, V. (2025). The reshaping of the Greek insurance sector through artificial intelligence technologies.
17. Khari, M., Gupta, P., & Singh, C. P. (Eds.). (2026). Edge Artificial Intelligence: Transforming Computing from Cloud to Edge. CRC Press.
18. Kumar, N. (2025). A Critical Analysis of the Existing Legal Frameworks Governing Artificial Intelligence in Cyber Warfare. Bahra University.
19. Lami, B., Mohd. Hussein, S., Rajamanickam, R., & Emmanuel, G. K. (2024). The role of artificial intelligence (AI) in shaping data privacy. International Journal of Law and Management.
20. Lawrence-Ogbeide, E. (2025). Defining data protection boundaries in an IoT-connected world: revisiting data propertization.
21. Lomurno, E. (2024). Adversarial and generative deep learning for data privacy in human-centered artificial intelligence.
22. Mania, B. (2022). Big Data and Artificial Intelligence: An examination of the existing legal framework

from a privacy perspective.
23. Mania, B. (2023). Big Data and Artificial Intelligence–An examination of the existing legal framework from a data protection perspective. University of Pécs (Hungary).
24. Marwala, T. (2026). The Governance of Artificial Intelligence. Morgan Kaufmann.
25. Merler, M. (2026). Artificial intelligence in law enforcement: a critical analysis of the EU AI Act's framework for protecting public values and fundamental rights.
26. Mohaghegh Montazeri, L. (2026). Artificial Intelligence of Everything (AIoE) in energy sectors: cybersecurity, data protection, and data localization.
27. Montasari, R. (2024). National security in the Artificial Intelligence era: Challenges and implications of advanced technologies (Doctoral dissertation, Cardiff Metropolitan University).
28. Ouaissa, M., Ouaissa, M., Cherrafi, A., Aoun, N. B., & Kar, R. (Eds.). (2026). Artificial intelligence and fuzzy logic for next-generation intelligent transportation systems. CRC Press.
29. Ouanhlee, T. (2026). Modern Computer Science: Foundations, Artificial Intelligence, Emerging Technologies, Responsible Computing, and the Future of Computing. Thanakit Ouanhlee.
30. Paleti, S. (2025). Smart finance: Artificial intelligence, regulatory compliance, and data engineering in the transformation of global banking. Deep Science Publishing.
31. Pareshkumar, M. A. (2025). An Effective Approach to Mitigate Security Challenges Through Privacy Preservation for Machine Learning Techniques to Build Robust Healthcare Data (Doctoral dissertation, Gujarat Technological University).
32. Pokhariyal, P., Patel, A., Nautiyal, N. S., & Mishra, A. K. (Eds.). (2026). Emerging Technology and the Law: Bridging the Gap Between Innovation and Regulation. Taylor & Francis.
33. Ranjitsingh, L. M. (2025). The Evolution of Cyber Law: A Critical Analysis of Jurisprudence, Regulation, and Digital Rights. Crown Publishing.
34. Razavi, H., Franco, M. F., Ouaissa, M., Ouaissa, M., & Srivastava, G. (Eds.). (2026). AI-driven cyber risk management. CRC Press.
35. Reddy, D., Kumar, L., Gangane, V. W., & Kumar, M. Y. S. (2026). Artificial Intelligence and Data Science. BR Publications.
36. Sah, S., Sulaiman, R. B., & Tyagi, A. D. (Eds.). (2026). Federated Learning in Finance: Unlocking Privacy-preserving and Cyber Resilience Using AI. CRC Press.
37. Saxena, A. (2026). Artificial Intelligence and Machine Learning. BR Publications.
38. Sekwena, T. (2025). Exploring the Factors Influencing Artificial Intelligence (AI) Governance in South Africa (Master's thesis, University of the Witwatersrand, Johannesburg (South Africa)).
39. Shafik, W. (2024). Artificial intelligence and machine learning with cyber ethics for the future world. In Future communication systems using artificial intelligence, internet of things and data science (pp. 110-130). CRC Press.
40. Shafik, W. (2026). Ethical Artificial Intelligence in the Insurance Industry: Balancing Efficiency, Fairness, and Risk. CRC Press.
41. Singh, B., Kaunert, C., Balusamy, B., & Dhanaraj, R. K. (Eds.). (2025). Computational intelligence in healthcare law: AI for ethical governance and regulatory challenges. CRC Press.
42. Soofastaei, A. (2026). LIFE 4.0: Human Life in the Age of Artificial Intelligence. CRC Press.
43. Ullah, I., Khan, I. U., Ouaissa, M., Ouaissa, M., & El Hajjami, S. (Eds.). (2024). Future communication systems using artificial intelligence, internet of things and data science. CRC Press.
44. Vidya, M. N. (2025). Data Protection in the Era of Digitization: with Special Reference to Data Privacy and Data Localization in India (Doctoral dissertation, Alliance University (India)).
45. Virk, S. (Ed.). (2026). Artificial Intelligence and the Law: Global Perspectives, Regulatory Challenges, and Emerging Jurisprudence. Taylor & Francis.
46. Young, R. G. (2025). Artificial Intelligence and Machine Learning in Cybersecurity: A Comprehensive Guide to Improving Cybersecurity Protocol. CRC Press.