I J C R M
International Journal of Contemporary Research In Multidisciplinary

Review Article

Artificial Intelligence and The Law of Data Protection: An Analytical Study of Emerging Global Norms

Deepak Kumar[1*], Dr. Amit Verma[2]
[1] Research Scholar, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
[2] Associate Professor, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India

Corresponding Author: Deepak Kumar*

DOI: https://doi.org/10.5281/zenodo.16879755

Abstract

The accelerated proliferation of artificial intelligence (AI) technologies has ushered in significant advancements across multiple sectors, yet it simultaneously presents multifaceted legal, ethical, and regulatory challenges—particularly in the realm of personal data protection. This study undertakes a comprehensive analytical examination of the evolving global legal frameworks at the intersection of AI and data protection regimes. It investigates the operational dependency of AI systems on extensive data collection and processing, which frequently conflicts with established norms of individual privacy and data sovereignty.

The research centers on key legislative instruments such as the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and Brazil's Lei Geral de Proteção de Dados (LGPD), each offering distinct normative approaches grounded in accountability, transparency, and informed consent. Employing a comparative legal methodology, the paper critically assesses the effectiveness of these frameworks in mitigating algorithmic bias, ensuring fair automated decision-making, and managing transnational data flows.

Furthermore, this study explores the ethical dimensions of AI deployment, focusing on the principles of algorithmic transparency, the right to explanation, and the procedural rigor surrounding informed consent. It also evaluates the role of international institutions and multilateral agreements in fostering harmonized global data protection standards. Through the lens of contemporary case studies and judicial decisions, the research identifies persistent regulatory gaps resulting from the rapid pace of technological innovation outstripping legislative adaptability.

The paper ultimately advocates for a cohesive, human-centric, and forward-looking legal architecture that ensures AI development remains congruent with core data protection values. Emphasis is placed on the necessity of robust governance mechanisms and technological accountability to safeguard fundamental rights in the digital age.

Manuscript Information

- **ISSN No:** 2583-7397
- **Received:** 22-06-2025
- **Accepted:** 20-07-2025
- **Published:** 14-08-2025
- **IJCRM:**4(4); 2025: 510-517

- **Plagiarism Checked:** Yes
- **Peer Review Process:** Yes

How to Cite this Article

Kumar D, Verma A. Artificial Intelligence and The Law of Data Protection: An Analytical Study of Emerging Global Norms. Int J Contemp Res Multidiscip. 2025;4(4):510-517.

Access this Article Online

www.multiarticlesjournal.com

KEYWORDS: Artificial Intelligence, Data Protection Laws, GDPR, Algorithmic Transparency, Global AI Regulation.

INTRODUCTION

The race to develop artificial intelligence ("AI") has begun. Countries are heavily backing efforts to be the world leader in this technology. This nascent development promises to create a smarter, autonomous world. However, it is not without its concerns. It is not uncommon to hear people fear an inevitable uprising of machines. More realistic, at least for now, concerns regarding this technology are 'Shakespearean' in nature: Can machines think? Some scholars, organizations, and governments are concerned that with AI will come unprecedented power and control over individuals who do not opt in to its usage. Perhaps most prevalent are concerns regarding consumer personal data privacy and protection. One of the enabling technologies behind the development of smart AI is algorithm-driven machine learning, which requires vast amounts of personal and private data. This in turn, leads to use and misuse concerns, calling into question regulatory and legal approaches and limits.

The development of AI requires vast troves of private and personal data, along with advanced and expensive algorithms and infrastructures. Until recently, this has not been a major concern for some countries. The U.S.A., for instance, took a hands-off approach to regulating this technology. However, increasing concerns regarding privacy violations and data protection, combined with a desire to gain the upper hand in the race to develop AI, resulted in a growing framework of regulation (Humerick, 2018). Nations worldwide have adopted varying degrees of personal data protection, but the E.U. has established itself as the leader on this front. Having achieved the impossible by getting tech giants to comply in large measure with its privacy protections and resulting fines, the E.U. is again seeking to push the agenda globally by implementing the most comprehensive regulatory scheme yet on consumer personal data privacy and protection: the General Data Protection Regulation ("GDPR").

The GDPR has been hailed for its aggressive approach to protecting personal data privacy. Articles 5, 9, 12, and 22 of the new GDPR impose requirements on the Big Tech firms and other actors in the AI marketplace that cannot be easily reconciled with their development (and deployment) of smart AI. The GDPR's provisions imposing accountability and liability on the 'controller' of data (those that determine the 'what' and 'why' of the processing) are well-recognized. While this term captures the firms and agencies that currently create AI, it is important to note that, through processes like training and stealth deletion, AI must be able to independently collect and regenerate their own datasets.

1. Historical Context of Data Protection

The idea of data protection is not one that has arisen in a vacuum, but rather has been shaped and formed by pragmatic considerations that have developed over time. It is within that larger framework that such laws and proposed new laws are better understood, as well as the intentions of those laws. This discussion describes the history of data protection across the world. Discussion is first framed in the concepts of data stewardship, balancing harms and benefits, and transparency and redress. Placing the topic of data protection within the historical context of how privacy concerns have evolved and been addressed can help in understanding the intent of various laws that are either proposed or in place. Three primary concepts have guided this evolution, namely, data stewardship, balancing harms and benefits, and transparency and redress. Ensuring that these concepts and the objectives that they are based on are met is the determinative factor in seeing that existing laws do not fall short of their intention, and that any proposed new laws do not go too far in the consideration of the application of advanced technologies. The historical context of data protection takes a wider view of this topic than is commonly done, and with it brings in various perspectives that may have been overlooked before. That broader perspective has been necessary in order to bring a better understanding of each of the ways that this issue is being confronted more recently (F III Palmieri, 2019). This broader perspective also fits within a greater plan to round out this topic by considering the same issues from multiple angles, or through multiple lenses.

2. The Rise of Artificial Intelligence

Having heralded whistleblowing as the triumph of the free press, it remains to be seen whether in two years' time the same press will be applauding another tsunami of data apples from Apple. What is already clear is that this first serious calculation of the ethical risks presented by AI has the potential to change the balance of power in both the data economy and the online world. AI raises ethical questions that are much more intermittent than the simple question of fairness in AI decision making or the quantitative quest for representativeness in data. One area where this is relevant is in the democratic debate around the political economy of data much more broadly, fishing for the digital equivalents of the industries of yesteryear. Another area is in the self-reflection on the disciplines of computer science (including AI) around the framing and ambitions of these disciplines (Koos, 2018). That debate was last thought dormant in 1995 when many saw it as an example of epistemic progress that an imposition of this type on the sciences had been avoided. In its absence, AI has enjoyed a free hand to propel itself around the world in all manner of appropriate ways, for both good (its suppers relied risks to life, liberty and felicity) and evil (both holistically and globally). But it is difficult to know whether this was the result of laissez faire or contingency. Certainly, in numerous instances too easily forgot before the modern era of Netflix the festering of the online world has been shown to fuel the trolls and great egrets of Davidson's cyber utopia (D'Aloia, 2019). It is now suggested that the data gathered by cars, watches, phones and public screens to mention only a few will be mined by sector-enhancing industries in a bid for that ultimate digital prize foretold by the intelligence economy. Given that the demands of mining the huge and diverse other sources of publicly gathered and, with the proper permission, judiciously annotated data are thought to far exceed present capabilities or expectations of future machine-based productivity advances,

nahard reflection on the uses of passive or surveillant data duty calls.

3. Data Protection Regulations Worldwide

The World web is a global landscape as well as an information domain that shapeshifts around the business, social condition and governance of cyber data. From the days of the dotcom bubble, through the birth of search engines, social media platforms, and data analytics, the uncharted territory raised concern and awareness of the data assets. Cyber data and its jobs are no longer techno-legal wonders, but recognized goods with Algorithm in the role of gateway to interfaces and data assets. A slew of data protection rules follow, with the General Data Protection Regulation (GDPR) widely regarded as the ne plus ultra of data protection and the benchmark for new frameworks globally, some of which provide a further toughness than rid GDPR. A data protection regime may be loosely analyzed based on the nature of regulatory frameworks and the projection of control in the digital space. (F III Palmieri, 2019). There's a track whose reach goes far beyond home brand – the data sovereignty iteration. This is a stickier iteration of re-territorialization where data generated, collected or processed in the territory is locked in the territory, or where the governance, handling or processing of such data is within the regulatory grasp of the jurisdiction. In addition to custody regulations typically seen in banking and financial services, stricter laws may apply to the collection, usage or processing of data with governmental concern of national security, law and order, or manifest domestic interests, or even with reference to behavioral or predictive analytics posing risks on social million. Portability and interoperability of data, particularly in the data economy is also drawing concern in the lab on raw or processed inputs and a host of business, legal and ethical questions. This is notwithstanding the difficulty algorithmic teachings need on good behavior, or duty of good faith in Indonesia extension of a beachhead on a 'forced' sharing of machine learning model and trade secrets (not just inputs, parameters or output over officially managed application interfaces). This is legally a corollary of property data, but poses more complexities than durable goods, and there's fear of 'dumper' service ensnaring entities on unwieldy choices on equal access and promotion (which typically may be new but not insulation, like fiber port or e-SIM) instead of the methodical enhancements of elastic query debates now on-going on application data confidentiality. For cross-border regulation of data governance, aside from procedural and linguistic affinities, cultural proximity also brings like-mindedness on mood blinds and alarms, carefully docile resolutions or declarations that are nameless laws in soft power design.

4. AI's Impact on Data Privacy

In the last five years, there have been major developments with artificial intelligence impacting data privacy and protection. The following sections analyze these developments, with particular emphasis on the EU regulation on AI, the EU Data Governance Act, the EU Data Act, and national initiatives in the US. The sections also recall the regulatory background provided by the GDPR as well as the current claims and relevant litigation developments against AI-based online search systems. Then, they analyze the recent regulatory developments in AI and data protection and governance. The sections conclude with examinations of a possible better alignment of AI with the GDPR and proposals for a stricter governance of AI-trained AI systems.

While AI is everywhere and has many applications, it is often seen as a black box and its use raises many questions. While it is understandable that AI should be more regulated than other technologies, it is also true that AI is not a uniform technology. AI is trained on data, so it can either be directed to do something in a fairly predictable manner or present unpredictable outcomes depending on the approached. This means more regulation on the regulation and control elements should be adopted depending on the risks at stake. This was already highlighted with regards to privacy by design and by default in design, with it being more difficult to ensure adherence with stricter requirements such as data retention and the right to erasure with regard to AI activities (Humerick, 2018). In addition, one important element is that the access of more data must also be fostered by regulatory or economic incentives given that competition between AI systems is in their outputs. Hence, the likelihood of regulatory fragmentation is increased as jurisdictions adopt different or additional rules. Therefore, it is important to ensure alignment between regulations focusing on AI, data and privacy. So far very little attention has been paid to governance arrangements to ensure this alignment. Additionally, smarter litigation is needed given that AI systems are used to either be directed to discriminate between data subjects or simply given to other users due to a lack of evidence of non-compliance.

5. Data Collection Techniques

The majority of data collection techniques used by Artificial Intelligence/Awareness/Data Protection other than Information Data sub-regimes are indicative media collection and analysis/decoding techniques. Some of these media are affected by EU Information Data experts and legislation, but in general, Data Protection legislation has less influence on these media and data processing operations. The other technique, Social Media Activity Collection, is used in these sub-regimes, but there are more sub-techniques used in this media, such as observing Public Posts of others and Shadow Activity. These are sometimes related to Social Networks media, but the comments and descriptions are distinctive. Another significant and more sophisticated method is Feedback Processing, which indicates the rapid development of future AI potential and its awareness data.

Both computer analysis and Data Protection capability of AI need further clarification of data protection techniques. AI decision content and observation capability are too abstract, even for lawyers and computer specialists. This results in mistrust of self-learning computer analysis that can be invisible and without documentation, and shadow processing outside of

the monitoring or supervising authority. The broadcast model of the European Data Protection Supervisor is an indicative attempt to monitor and intervene.

As computer decision rules are public and understandable, monitoring these regulations and decisions is not sufficient for Data Protection monitoring. The idea of AI rules being blind and non-controllable rapidly rose, as the later self-learning frame was evaluated to be impenetrable. As AI was not understood, it was not trusted. Abstract processing and treatment rapidly raised concern, which was intensified by hidden governmental and investor involvement of big enterprise capacity. Hidden data analysis loopholes and the complex and automated script operation of these analyses led to a boom of awareness defence and control data, and techniques. New computational analysis scrutinising ex- and op-post knowledge became OECD methods and civic movements (Humerick, 2018).

6. Data Processing and Algorithmic Bias

Artificial intelligence (AI) and machine learning (ML) systems are increasingly used in public policy, commerce, and people's everyday lives. AI and ML are pervasive, powerful, and prone to errors and biases. Affected individuals may experience incorrect or biased outcomes of AI or ML systems (van Bekkum & Zuiderveen Borgesius, 2022). AI and ML systems in the public sector, finance, employment, education, insurance, and on social media platforms can lead to unfairness. AI and ML systems can discriminate against people based on race or gender, which may violate the law.

At least in the EU and the US, anti-discrimination laws exist to prevent unfair treatment of individuals based on sensitive characteristics, also called characteristics of protected status. In Europe, this is done by laws like the Race Directive, the Employment Directive, and national laws. In the US, important federal anti-discrimination laws prohibit discrimination based on race, gender, religion, national origin, age, or disability. These laws usually prohibit discrimination directly or indirectly by characteristics such as race or gender, as well as by algorithms learned from such characteristics. Most of these laws are based on the notion of fairness, which denotes an absence of unfair treatment based on characteristics of protected status.

However, algorithmic discrimination can be a law enforcement problem. AI or ML models can exhibit or cause discriminatory behavior in several ways. First, the algorithmic system can use sensitive data such as characteristics of protected status, which is strictly prohibited by antidiscrimination laws. Second, prohibited sensitive characteristics can be learned by an algorithm. Third, it is possible that the AI or ML model generates a discriminatory outcome, such as allocation of resources or services, which is prohibited by the law.

7. Global Norms in Data Protection

Under the slogans "The Age of AI Has Arrived", "The war of AI technology has begun", and so on, artificial intelligence (AI) is increasingly consequential for our well-being. AI promises faster, cheaper, and smarter solutions for humanity's basic and existential problems. Put negatively, AI threatens to disrupt our environment and threaten our existence (Humerick, 2018). The race for the AI crown is fierce and worldwide, and many sectors are producing various AI technologies. National governments invest heavily in AI development because AI leadership promises economic growth, a competitive edge, and international recognition and prestige. Recently, China has rapidly traversed from laggard to a world leader in a few years, raising national security concerns among European and American nations.

With its market size bigger than credit card and social network markets combined, AI can be used for personalized marketing, infra-red and facial biometric technology, real-time translation, etc. However, AI is not without its dark side. The Agency for Fundamental Rights of the European Union warns that AI can also be used to drive state-sponsored censorship, mass surveillance, social credit systems, and automated law enforcement. AI algorithms demand training data, which can be collected from web scraping and violations of the General Data Protection Regulation, raising serious concerns about individuals' personal data. If not designed safely and ethically, AI machines can bias against, discriminate, censor, block, or divert individuals alike and thereby threaten human rights.

At the same time, AI-machine technology is introduced to the public. Cyberbullying, fake news generation, text-presentation on knowing too well on victims, autonomous droning, entrapment, etc. abuse AI-mas can imply serious and sometimes existential dangers to its targets. The real-world deployment of AI technologies raised awareness of the concerns of using these technologies, leading the public, academia, and regulators to propose effective and persuasive measures to mitigate the harm.

8. Ethical Considerations in AI and Data Protection

Despite the benefits of AI in different domains, various ethical issues affect its social and economic deployment. On a theoretical level, a few desired types of outcomes for "ethical" AI technologies are already known: sustainability, equity, accountability, fairness, robustness, privacy, and transparency. There is a debate on which of these goals — often introduced by contrasting categories, e.g., procedural and fair decision-making — should be prioritized in public policy leading the feedback systems that bring together AI technologies, public information services, and human beings. Nonetheless, these ethical values could limit AI use depending on the handling of property data of citizens, and non-ethical postures could not be neutral to the recognition of all the desired social outcomes (Korobenko et al., 2024).

The difficulty in foreseeing inequitable or biased outcomes arises from the complexity of the data and algorithms on which the software systems are based. This significant unresolved issue of fairness is often linked to the notion of equity in the database. Historical prejudices encoded in the training data deliver inequitable or biased outcomes, especially in self-learning AI systems with search and deep learning (Humerick, 2018). Controversies on biased outcomes and ineffectiveness in

algorithm regulation often center on whether biased training data or a biased learning process of the software are to blame. As a legal issue, corporations need to be clear on whether they and their AI systems are liable for biased outcomes or if they can be secured in the absence of wrongdoing. If courts accept liability of flawed historical data, the economic growth potential of these datasets would be lost. On the other hand, if lived experience data is used for training, claims could be dismissed on the grounds of its legality. In either case, ethical AI development continues to remain a challenging endeavor.

Robustness constantly returns as a more non-tangible concern. It surfaced early in AI development in preventing subtle user manipulation of criminal justice systems. In general, the need for safety against attack surfaced as a legal concern. Existing AI systems may be too inequitable and biased or too intrusive and intrusive. Robustness in AI development may be as important as the discrimination issue in AI regulation. Ethics emphasize the need to guarantee the safety of AI technologies. Nonetheless, it brings complex legal issues. Safety requires AI systems to be observable and comprehensible for verification. This raises problems on balancing the protection of AI system property, creators, and users.

9. Challenges in Enforcement

Concerns regarding AI and contact with the data it is trained on are manifold: They range from concerns about provably safe machine learning (ML) and AI, through issues of fairness and bias, to concerns about models capturing sensitive personal data, reproducing and amplifying stereotypes, and infringing data protection rights. These challenges are exacerbated by training large scalable models and ML systems that deploy them in real-world applications. Enforcement against such infractions is difficult, and scholars are questioning the adequacy of existing conceptual frameworks of accountability in this space (Humerick, 2018).

A dual recommendation for a legal protection approach which aims at societal design challenges and strengthening existing legal norms at the context of society-altering AI and ML systems and inadequate or multi-dimensional paradigm matters: pseudo-systems containing knowledge and output data. This is addressed by ways of concept-testing the fiability and legitimatedness of the 2023 EU AI Act, and the General Data Protection Regulation (GDPR).

The goal is develop a spectrum legitimate or (arc – though arguably non-universal) tests to avert abuses of the additions and abuses of applying uncertain AI and ML cogency. Three groups containing the following matters and positions of law or AI Society: i. Exploitation discrimination, consequences; ii. Concentration abuse, issuer concentration, knowledge discrimination-persons/society-indicium; iii. Empowerment domain cumulus and thus qualified as regulated monopoly. This environment call for urgently regulation at technology not merely industry or estate level adopting a socially sound long sord policy. Four categories to be developed aggregates AI or big-data.

10. Jurisdictional Issues

Today the issues of jurisdiction and sovereignty regarding artificial intelligence are currently unresolved. They remain far away from reaching any global consensus. Given the cross-border flow of data and the unbounded nature of emerging economic actors, switching to a new regulatory framework will be favoured by a relatively small set of countries which possess the necessary domestic or bilateral tools. They are likely to engage in a variation of the cooperate-race-vs.-cooperativeness approach, adopting theoretically clever but practically vague definitions of “law on data protection” or “data protection law”, which will then be deemed protection-friendly. Countries that cannot or will not change their legal culture to favour the new set of rules are bound to have a huge and detrimental impact on the effectiveness of protections.

Simply filling any gaps in the current understanding of what ‘data protection’ means or would mean under such re-calibrated regulations on AI would needlessly prolong uncertainty, as carded actors are unlikely to lose their clout or retain it effectively in the coming situation. The latter means that sand-box and other ‘live test’ regulations will be favoured, blissfully ignoring the fact that if with artificial intelligence largely unlimited, undemocratic powers were before then, probabilities are they won’t be immediately down to reasonable levels this time. It is also highly likely that uncommitted states will be pressured to tone down their protection-friendly definitions to those in the present instruments in exchange for economic support to transition to the new regime. An illustrative example could be a country that co-formulated regulations but has since opted for a largely undemocratic but economically easy to enforce regime because of its geographic closeness to Europe.

The lack of substantive deviation from existing frameworks might point at stability, but like past accelerative shifts in regimes, the space for abuse could widen significantly during this period. Accordingly, unless the quantum leap is executed in an even-handed manner, it is likely that the current widening has established a new margin between the fit-for-use actors and its unfit ones. One outcome of this divergence could be bifurcation spilling out east vs. west and north vs. south narratives, where each side will argue grounds about which is the fittest legal jurisdiction.

11. Case Studies of AI and Data Protection

More than 20 billion devices worldwide are connected to the Internet and play a role in data transmission (Humerick, 2018). A device often measures or detects certain measurable parameters within a defined period of time, such as how many steps a user takes during a day, whether the user can fall asleep, and how many hours of sleep the user can get. The measured parameter is then quantized into multiple states and transmitted to the cloud by an Internet-of-Things (IoT) system. Through data fusion algorithms, the measured parameters of the IoT system can be integrated to assess one state or a higher state. Hence, a legal dispute commonly arises when an individual's device does not measure parameters when such parameters should normally have been measured and revealed. Specific

case studies are introduced on the basis of detecting the missing data.

As the cloud-computing industry allows the cloud to gain a competitive advantage over the user in the analysis of device data, a device data discrepancy is often found, such as wrongly determining the lower states. For transboundary monitoring cases, the user often has an information advantage over the cloud. The case studies demonstrate how to prove these stands. In contrast, the law can only verify the fact of a device that is not measuring or has detected no parameters but in a subjective manner. Thus, it cannot clarify the circumstance where the cloud-us user further colludes to destroy workloads in order to rise above the proof standard.

Therefore, the measures are proposed from three aspects. From a global and holistic viewpoint, first, the situation of illegal rules and weak institutions, especially in developing countries, should be carefully noticed. Secondly, content-related activities to some certain extent are significant as rapidly emerging national norms. At this stage, a collaboration of voluntary self-regulations can be regarded as the most promising approach since the government intervention on this issue can slow down the speed of AI development and bring the possibility of opportunistic exploitation by the incumbent players. Lastly, the existing frameworks or institutions should be applied based on current substantive market competition. The superior regulatory or legally binding institutions should be considered first, otherwise, as holding sway norms emerge, it may be too late to consider such frameworks.

12. Future Directions in Data Protection Law

Data, in many different forms, has recently become ubiquitous. Businesses increasingly seek to obtain, store, and analyze this data in order to learn about their customers, patients, and members, while fraudsters, hackers, and even governments are motivated to know everything they can about everyone for malicious business practices, identity theft, and politically motivated repression. Wielding so much power over people, businesses, governments, and critical infrastructure, data may well be the keyword of the 21st century. Ironically, however, as data has grown more potent, it has also become more vulnerable, as new levels of exposure and analysis, in both legal and illegal contexts, have developed. The rapid growth in data and its acquisition, use, and loss has led to widespread concern, debate, and study. The 1970s and 1980s were decades of great growth for computer technology, data acquisition, and analysis. There was no better time for engaging in debates primarily about who owned the data, who had access to it, and whether business models exploiting that data could be developed. As a result, the 1990s were decades of great business growth, with escaping personal data gathering, analysis, and sharing becoming forever harder, leading to citizens becoming more suspecting of their governments and corporations. Governments globally tried to respond to citizens' demands for data protection, regulation, and transparency. Often, however, the data-related scandals revealed in depth the struggle between what is owned, how it is used, and how it is legislated, and thus how to find legitimate avenues for data's increasing power to be harnessed to serve further data-based growth. The need for law, regulation, and governmental oppression has been debated. Just as in earlier decades this played out in the contexts of data in relation to knowledge, societal structures, and economic models, so in contemporary discussions and analyses is interest shifting from data owned and obtained to what users and owners may do with that data. The result is a burgeoning literature on privacy, data hoarding, emulation, regulation, and discrimination concerning citizens and behaviour, with these issues undergoing analysis alongside, or often being subordinate to, fears or hopes of new, powerful paradigms of knowledge, structuring, and economy ushered in or reconfigured by these new technologies.

13. Public Perception and Awareness

Public Perception and Awareness of artificial intelligence (AI) is essential and can yield insights into underlying attitudes around data protection and privacy laws. Overall, survey participants stated that they were familiar with the term Artificial Intelligence and techniques, uses, and jargon related to it. Those who were aware of the term AI also had a positive perception of it, between Neutral to Agree. The mainstream media was one of the most frequent information sources about AI, followed by personal experiences with smart technology (Latham & Goltz, 2019). The general attitude was that AI creates an overall net positive. However, some AI techniques, mainly involving sensitive data, were seen less favorably. Prior to answering the survey, respondents stated that they did not have much awareness of data protection and privacy. However, respondents were aware of the general concepts and had low exposure to the largescale data protection and privacy law. Those who were familiar with and followed the GDPR closely were confident that their data was more protected because of it.

Familiarity with the term GDPR does lead to favorable perceptions about existing data protection laws. It was noted that Europeans tend to have a much more favorable opinion of regulations governing the privacy and protection of personal data. However, the effects of regulations, such as the GDPR on AI, machine learning (ML), or predictive analytics (Humerick, 2018) were unclear. Most responses rate statements regarding the negative effect of the GDPR on AI efforts as Neutral, with an overall high level of uncertainty. There was even a discrepancy between Follow-up (o) and Follow-up (z) between European and non-European respondents, where Europeans tended to rate these statements slightly agree as compared to Neutral by non-Europeans. Overall, respondents appeared to be uncertain about the effect of data protection laws on AI and bias efforts. Nonetheless, respondents were somewhat aware of the possibility of bias being introduced at various points in a data analysis process.

14. Technological Innovations and Legal Adaptation

Introduction to Technological Innovations and Legal Adaptation

Artificial intelligence (AI) has the potential to improve cybersecurity significantly. AI-driven technologies will play a crucial role in detecting and preventing attacks in cyberspace, protecting personal information contained in data-processing systems, and addressing a broad spectrum of cyber threats. AI-based technologies will improve cybersecurity greatly, enabling it to cope with emerging threats like deepfakes or automated cyber-attacks against critical infrastructures. AI will thus facilitate the task of fighting malicious actors such as hackers and uncooperative states (Humerick, 2018).

On the other hand, a new watershed moment of concern accompanies this technological evolution. If misused, AI could augur a catastrophic decline of universally enjoyed rights and freedoms, leading to a new form of dictatorial control over populations. Even legitimate security uses of AI in cyberspace can negatively impact the civil society fabric, human rights ecosystems, and freedom-based systems of governance. AI in practical cyber-security activities poses threats to privacy and data protection, the presumption of innocence, and other prima facie incompatible rights and interests.

Lawfulness of AI in Cybersecurity

This contribution examines how existing legal standards regarding the use of AI in cybersecurity will evolve in the future. The impact of AI-enhanced cyber measures on people's lives remains today an open research question. The prospect is of AI technologies ruling the cyberspace fight between defenders and attackers, with unknown implications for the legal attribution of responsibility for damage, the harms inflicted on daily human life, the ultimate goals pursued by states and private actors, and much more. Technological was as shocking to civil society as today's AI is, and the clash with human beings' fundamental rights and freedoms triggered major differentiations of legal standards across jurisdictions in the 20th century.

Notably, compliance with the law does not grant automatic legitimacy. It rather obliges, in light of the aforementioned "universal guarantees of humanity," to respect, honor, and protect such rights and freedoms. Jurisdictions vary greatly in civil society's vulnerability toward abuse by public or private actors. The meat industry's unnoticed suffocation in hyper-connected spaces, agricultural production rendering human eating unnecessary, and the world's rich becoming the world's rulers are extreme anecdotes of the homogenization of the latest technologies spanning cyberspace and their far-reaching workplaces, but whistleblower exposé led to the survival of a fairer risk-sharing system among the parties involved in cyberspace decision-making.

15. CONCLUSION

The data protection rights of most of the advanced countries in the world, China and the US being the exceptions, were retained. But in addition to these taken-for-granted rights, for the first time, the EU introduced a comprehensive and modernized law of data protection applicable to both public and private cyber entities of the world engaging in either the collection, processing, storage or sharing of personal data of individuals in the EU or the provision of services to persons in the EU (Humerick, 2018). The GPDR, thus, faced with the irrepressible rise of AI and its attendant dangers to data protection, became a robust and growing edifice on which a new and admirable regulatory law structure emerged.

The challenge of AI is global and massive, but it entails massive investment, talent and support by governments. Possible dangers are multiplying, especially with the rapid growth of generative AI with its accompanying social and technological technologies. States are trying to intervene and the nation-state line remains but the soil for the growth of global norms has probably been prepared which will evolve rapidly. There may arise clashing claims about actual results when countries with conflicting codes of conduct seek to stall the growth of rival AI. For humanitarian reasons, there must be new global norms that offer flexibility and abide by cultural competition. An analysis of the preceding material suggests the capability under different cultural imperatives and celebrations to spearhead the process of growth and popularization of norms requires more research and exploration.

REFERENCES:

1. Humerick M. Taking AI personally: how the E.U. must learn to balance the interests of personal data privacy & artificial intelligence [Internet]. Santa Clara High Technol Law J. 2018;34:393. Available from: https://digitalcommons.law.scu.edu/chtlj/vol34/iss4/3/
2. Palmieri NF III. Data protection in an increasingly globalized world [Internet]. Indiana Law J. 2019;94(1):297–.Available from: https://www.repository.law.indiana.edu/ilj/vol94/iss1/7/
3. Koos S. Artificial intelligence – science fiction and legal reality [Internet]. Malays J Syariah Law. 2018;6(3):23–29. Available from: https://mjsl.usim.edu.my/index.php/journal/article/view/275
4. D'Aloia A. Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale [Internet]. BioLaw J – Rivista di BioDiritto. 2019;1:3–31. Available from: http://amsacta.unibo.it/6509/
5. Mészáros J, Minari J, Huys I. The future regulation of artificial intelligence systems in healthcare services and medical research in the European Union [Internet]. Front Genet. 2022;13:927721. Available from: https://www.frontiersin.org/articles/10.3389/fgene.2022.927721/full
6. Birrell E, Rodolitz J, Ding A, Lee J, McReynolds E, Hutson J, et al. SoK: technical implementation and human impact of Internet privacy regulations [Internet]. arXiv. 2023;arXiv:2301.08611. Available from: https://arxiv.org/abs/2301.08611
7. Samarin N, Kothari S, Siyed Z, Björkman O, Yuan R, Wijesekera P, et al. Lessons in VCR repair: compliance of Android app developers with the California Consumer Privacy Act (CCPA) [Internet]. Proc ACM Interact Mob

Wearable Ubiquitous Technol. 2023;7(4):179. Available from: https://dl.acm.org/doi/10.1145/3631414
8. Rodrigues Nascimento Vieira V. Lei Geral de Proteção de Dados: uma análise da tutela dos dados pessoais em casos de transferência internacional [Internet]. Brasília (BR): Universidade de Brasília; 2019. Available from: https://bdm.unb.br/handle/10483/24513
9. van Bekkum M, Zuiderveen Borgesius F. Using sensitive data to prevent discrimination by artificial intelligence: does the GDPR need a new exception? [Internet]. Comput Law Secur Rev. 2023;48:105770. Available from: https://www.sciencedirect.com/science/article/pii/S0267364922001913
10. Korobenko D, Nikiforova A, Sharma R. Towards a privacy and security-aware framework for ethical AI: guiding the development and assessment of AI systems [Internet]. Digital Business. 2024;4:100136. Available from: https://www.sciencedirect.com/science/article/pii/S2666956124000051
11. Radanliev P, Santos O, Brandon-Jones A, Joinson A. Ethics and responsible AI deployment [Internet]. Front Artif Intell. 2024;7:1377011. Available from: https://pubmed.ncbi.nlm.nih.gov/38601110/

About the Corresponding Author

Deepak Kumar is a Research Scholar at Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India. His academic pursuits focus on advancing knowledge through rigorous research and scholarly engagement. With a commitment to academic excellence, he actively contributes to his field of study, aiming to address contemporary issues with innovative perspectives.