INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

ANALYSING THE HUMAN RIGHTS IN THIS HIGH-RISK AI ERA: ERADICATING THE STATES VULNERABILITY IN THE CYBER SPACE

AUTHORED BY - SHAMSHEER SHEIK SS, PRADEEPAN R & MOHAN BABU P

Abstract:

The rapid expansion of Artificial Intelligence has ushered this era characterised by unprecedented opportunities and equally profound risks. As AI systems increasingly influence governance, digital identity, surveillance and decision-making processes especially in governance related activities which involves collecting and processing of sensitive digital data of citizens who are the assets of the nation and hence, the need for robust human rights protections becomes urgent. India continues to experience frequent data breaches, insufficient cybersecurity preparedness, outdated digital storage systems and inadequately regulated public-private data flows. As AI-based systems become embedded in financial inclusion schemes and public administration, infrastructural weaknesses expose citizens to the dangers of mass surveillance, exclusion errors, algorithmic bias and data misuse creating vulnerability to state's digital infrastructure as well as violating human rights in cyber space. This paper uses doctrinal method by investigating constitutional principles, judicial precedents to argue that procedural fidelity is not a mere technicality but a substantive democratic safeguard. It concludes that in this era, the protection of human rights is inseparable from both State's Obligation to eradicate its vulnerability and extinguish cyber evils and strengthen State's capacity to secure digital private data. Strengthening these domains is essential to ensuring that AI enhances, rather than undermines fundamental rights in cyber space.

Keywords: Artificial intelligence, Cyber Space, High Risk AI Era, Vulnerable Digital Infrastructure.

Introduction:

From 1990 to 2010, India's legislative procedure on cyber laws developed gradually alongside the growth of information technology and the internet. During the 1990s, the absence of specific legal frameworks created regulatory gaps in addressing electronic commerce and cyber

ISSN: 2582-6433

offences. To meet these challenges, Parliament enacted the Information Technology Act, 2000, The Act provided legal recognition to electronic records, digital signatures, and prescribed penalties for cybercrimes. The Act further expanded to address data protection, cybersecurity, and platform regulation. The Information Technology Act, 2008 was also introduced. A major milestone was the enactment of the Digital Personal Data Protection Act, 2023, which established a statutory framework for lawful data processing, consent, and accountability. At present the rapid advancement of Artificial Intelligence (AI) has transformed the architecture of modern governance, reshaping the manner in which states collect data, administer welfare, regulate populations, and make decisions that directly affect citizens' lives. AI-driven systems increasingly operate in areas such as digital identity management, surveillance, etc. While these technologies promise efficiency, inclusion, and innovation, they simultaneously generate significant risks to fundamental rights, particularly the rights to privacy, equality, due process, and dignity.

This dual nature of AI has led to its classification as "high-risk" when deployed in state functions that carry profound consequences for individuals and democratic institutions. This paper examines the intersection between Artificial Intelligence and human rights violation in India's emerging AI-driven state by analysing the State Vulnerability. India's digital ecosystem remains marked by persistent vulnerabilities, including inadequate cybersecurity infrastructure, outdated data storage mechanisms and insufficient regulation of public-private data sharing.

Review of Literature:

Ahmed Zaroff (2022): This study critically examines the impact of AI-based automated decision-making on the rule of law within democratic societies. Focusing on surveillance, predictive policing, and law enforcement practices in Europe and the United States, the research highlights concerns related to algorithmic bias, discrimination, and threats to fundamental rights. The study emphasizes the growing influence of private technology actors in public governance and strongly argues for enhanced regulatory safeguards to ensure transparency, accountability, and protection of social justice principles.[1]

Belinda Halilaj et al. (2023): In this article, the authors emphasize the need for the ethical

[1] Ahmed Zaroff, *AI based automated- decision making: an investigative study on how it impacts the rule of law and the case for regulatory safeguards.*

ISSN: 2582-6433

guidelines and regulations for safeguarding Human Rights and dignity within the AI driven world. The authors are considering the nexus of ethical and legal imperatives particularly those set forth by GDPR (General Data Protection Regulations) within the European Union. The authors also elucidate the GDPR's provisions relating to automated decision making, profiling and data subject rights and also evaluated the urgency of adopting a responsible and GDPR complaint approach to AI development.[2]

Celal Hakan Kan (2024): The author examines the impact of AI on democracy and human rights, focusing on its influence on freedom of expression, electoral rights, privacy, and data protection. This study highlights both the opportunities AI offers for strengthening democratic governance and the risks it poses through surveillance and rights erosion. Kan emphasizes the limitations of existing legal frameworks and stresses the need for ethical guidelines and international cooperation to ensure AI governance and human rights principles.[3]

Ammar Zafar (2024): This author examines the growing integration of artificial intelligence within legal practice, highlighting both its practical benefits and ethical challenges. The study notes AI's potential to improve efficiency, accessibility and procedural accuracy in legal services. However, it raises serious concerns regarding algorithmic bias and transparency, particularly in sensitive areas such as criminal justice and family law. The author strongly advocates a "human-in-the-loop" approach, emphasizing that human oversight is essential to ensure fairness, accountability and ethical integrity in AI-assisted legal decision-making.[4]

Rafaq Ahmad et al. (2025): The authors explain the convergence of Artificial Intelligence and Human Rights by focusing on issues such as data privacy and the broader societal implications of AI systems. The authors present the critical ethical and legal challenges which can suppress these rights. This paper emphasizes the need for inclusive as well as transparent AI development, strengthened legal mechanisms and interdisciplinary collaboration to ensure the AI developments align with human rights.[5]

---

[2] Belinda Halilaj et al., *Ethical implications and Human Rights violations in the age of Artificial Intelligence*, Balkan Social Science Review, Vol. 22, pp. 153-171, December 2023.
[3] Celal Hakan Kan, *Artificial intelligence in the age of democracy and human rights: normative challenges and regulatory perspectives,* International Journal of Eurasian Education and Culture, Vol.9 (25), Pg no. 145, 2024.
[4] Ammar Zafar, *Balancing the scale: navigating ethical and practical challenges of artificial intelligence (AI) integration in legal practices,* Discover Artificial Intelligence, 15 April, 2024.
[5] Rafaq Ahmad et al., *Ethical and Legal Challenges of Artificial Intelligence: Implications for Human Rights,* Journal of Law, Society and Policy Review, Vol. 02 (1), pp. 10-25, 28th February 2025.

ISSN: 2582-6433

Research Gap:

The existing literature explores the relationship between artificial intelligence, human rights, democracy and ethical governance, focusing on issues such as algorithmic bias, surveillance, data protection and regulatory safeguards. Scholars like Ahmed Zaroff, Belinda Halilaj et al., Celal Hakan Kan, Ammar Zafar, and Rafaq Ahmad et al. primarily examine the substantive impact of AI on rights and legal systems. However, a critical gap exists in the analysis of legislative procedures through which AI-related laws are enacted. The reviewed studies do not sufficiently address how procedural deviations in law-making, particularly the use or misuse of Artificial Intelligence, affect democratic accountability and human rights protection in this high-risk AI era. This research fills the gap by linking AI governance with Human Rights and State Vulnerability in the Cyber Space in this High Risk AI era.

Objective of the study:

- ➢ To urge the recognition of the Right to Digital Privacy and making it a fundamental Right.
- ➢ To say the importance of making strong Digital Infrastructure before bringing in new digital services to the citizens.
- ➢ To say the importance of periodic Maintenance of the existing digital infrastructure.

Research Methodology:

This study adopts a qualitative legal research methodology combining doctrinal, case study, comparative and descriptive approaches to examine Artificial Intelligence and human rights in the high-risk AI era. The doctrinal method is used to analyse constitutional provisions, statutes, and judicial precedents, particularly Articles 14 and 21 and landmark cases such as Maneka Gandhi, Puttaswamy, to assess procedural legitimacy and rights protection. The case study method examines the Grok AI on X and the BSNL data breach to illustrate the real-world consequences of AI governance and weak digital safeguards. A comparative approach draws insights from international frameworks such as the GDPR and Digital Services Act to highlight regulatory gaps in India's AI governance. The descriptive method traces the evolution of cyber laws, AI deployment in governance and infrastructural vulnerabilities.

ISSN: 2582-6433

Concept of Artificial Intelligence and its Role in Governance:

Artificial Intelligence (AI) is a computational system which is capable of performing tasks that traditionally require human intelligence like learning, pattern recognition, prediction, problem solving and decision-making. AI works by using algorithms to learn patterns from massive amounts of data, which enables machines to "think," recognize information, solve problems and make decisions. In contemporary governance[6]AI extends beyond experimental use and has become an integral tool in public administration. Governments increasingly deploy AI systems to manage large datasets, automate administrative functions, and improve efficiency in service delivery. In India, AI is used in areas such as biometric identification, welfare distribution, predictive policing, tax administration, and smart city initiatives. AI enables data-driven decision making by analysing huge amounts of personal and demographic information. Automated systems assist in identifying beneficiaries for social welfare schemes, detecting fraud, Digital Public Infrastructure, Railway and optimising resource allocation. While such applications promise speed, accuracy, and cost-effectiveness, they also introduce new forms of State power exercised through algorithms rather than human discretion. This shift alters traditional administrative structures and raises concerns regarding transparency, accountability, and fairness. There is an increased reliance on AI in governance which marks a transition from rule-based administration to algorithmic governance.

AI and Human Rights: An Interlinked Framework

I. Conceptual Understanding of Artificial Intelligence

Artificial Intelligence simulates the human cognitive functions like learning, reasoning, prediction, and decision-making in governance AI systems are increasingly deployed to manage large-scale data, automate administrative functions, and support decision-making in sectors such as welfare distribution, law enforcement, healthcare, taxation, border control, and digital identity systems. These applications often fall within the category of high-risk AI because their outcomes have direct and significant consequences on individuals' rights, entitlements, and legal status. Unlike traditional tools, AI systems rely on complex algorithms, and AI systems function as opaque when their decision-making processes lack transparency and explainability, preventing individuals and institutions from understanding, questioning, or holding accountable the basis of automated outcomes.

[6] Gaddela Srikanth, *Transforming governance: exploring the intersection of e-governance and artificial intelligence in India,* Electronic Government, Vol. 21 (3), pp. 300-312, 2025.

ISSN: 2582-6433

II. Human Rights in the Age of Algorithmic Governance

Human rights represent the core normative framework that safeguards individual dignity, autonomy, equality, and freedom from arbitrary State action. In constitutional democracies, rights such as privacy, equality before law, freedom from discrimination, due process and access to remedies serve as limits on governmental power. The deployment of AI in governance fundamentally alters the manner in which these rights are exercised and potentially infringed. Automated decision-making can affect eligibility for welfare benefits, target individuals for surveillance, predict criminal behaviour, or profile citizens based on vast datasets. Such practices raise serious human rights concerns, including algorithmic bias, exclusion, mass surveillance, data misuse, and the erosion of individual agency. The outcome might be discriminatory or unequal due to biased data, flawed design, or embedded assumptions, thereby undermining equality and fairness. Because of this, AI governance has emerged as a critical human rights issue rather than a purely technical or administrative matter.[7]

Constitutional validity of Artificial Intelligence in India:

1. How Artificial Intelligence violates Fundamental rights?

Article 14 of the Indian Constitution guarantees equality before the law and equal protection of the laws, which is the bedrock of constitutional governance and the rule of law. The judicial interpretation has consistently held that Article 14 strikes not only at discriminatory classification but also at arbitrariness in State action. In the context of emerging technologies, there has been an increase in the use of artificial intelligence (AI) in all spheres of life especially in judiciary it's used in decision-making processes which also gives rise to serious constitutional concerns, particularly where such systems influence or assist decisions affecting rights, entitlements, or legal outcomes. These High-risk AI systems, by their very nature, pose threats to substantive equality and procedural fairness, thereby implicating Article 14.

1.1. Algorithmic Bias and Violation of the Right to Equality under Article 14:

One of the primary ways in which AI violates Article 14 is through the phenomenon of algorithmic bias. AI systems are trained on large datasets that often reflect historical inequalities, social hierarchies, and systemic discrimination. When due to negligence or voluntary malafide action the QI is used to be trained by giving biased data sets and such biased

[7] Vasiliki Koniakou, *Governing Artificial Intelligence and Algorithmic Decision Making: Human Rights and Beyond,* 20th Conference on e-Business, e-Services and e-Society (I3E), Galway, Ireland. pp.173-184, Sep 2021.

ISSN: 2582-6433

data is used to automate or assist decision-making then that outcomes may disproportionately disadvantage certain individuals, classes or groups, even in the absence of explicit discriminatory intent. This leads to unequal treatment of similarly situated persons, undermining the principle of equality before the law. Further, Article 14 permits classification only when it is based on intelligible differentia and has a rational nexus with the object sought to be achieved. Algorithmic decision-making frequently relies on opaque variables, proxy indicators, and probabilistic assessments that cannot be meaningfully scrutinised. When individuals are subjected to adverse outcomes without clear, explainable, and rational criteria, such classifications become arbitrary. As judicially recognised, arbitrariness is the antithesis of equality; therefore, AI-driven decisions have high risk of lacking transparency and accountability hence violates Article 14.[8]

In an article published in the New York Times titled [9] "Facial Recognition Is Accurate, if You're a White Guy" exposes how facial recognition systems exhibit significant racial and gender bias, performing most accurately on white male faces while showing high error rates for women and people with darker skin tones. This disparity arises from biased training datasets and flawed algorithmic design, demonstrating that AI systems are not neutral but often replicate existing social inequalities. Such algorithmic bias directly violates Article 14 of the Indian Constitution, which guarantees equality before the law and prohibits arbitrary and discriminatory State action. When AI systems used in governance or law enforcement disproportionately misidentify certain groups, similarly situated individuals are treated unequally without rational justification, rendering such technology constitutionally suspect under the principle that arbitrariness is antithetical to equality.

1.2. Violation of Natural Justice: Nemo Judex in Causa Sua:

In addition to substantive inequality, the use of AI in decision-making also threatens the principles of natural justice, in reference to the legal maxim nemo judex in causa sua, which mandates that no one shall be a judge in their own cause. This principle requires the decision-maker to be impartial and free from bias whether direct or indirect, conscious or unconscious. In judicial and quasi-judicial contexts, impartiality is central to legitimacy and fairness. Although AI is often presented as a neutral assistive tool, its integration into decision-making

[8] Ayushi Shreya, *AI, Bias, and the constitution: A Jurisprudential analysis of Algorithmic inequality under Article 14,* Indian Journal Of Legal Review (IJLR), 5 (10), pp. 872-879, 2025.
[9] https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html 21:02 IST 1/16/2026

ISSN: 2582-6433

processes can introduce hidden biases that compromise impartiality. AI systems are designed, trained, and optimised based on human choices, institutional priorities, and predefined objectives. When judges or authorities rely on AI-assisted recommendations, risk assessments, or predictive tools, there is a real danger that the decision-maker becomes indirectly influenced by biases embedded within the algorithm. This creates a situation where the source of bias is not apparent or contestable, yet materially shapes the outcome.

The use of AI assistance therefore risks violating nemo judex in causa sua by allowing an opaque technological system over which the affected individual has no control or insight to influence adjudication. Such reliance weakens procedural fairness, limits meaningful challenges, and undermines public confidence in impartial justice. In the high-risk AI era, the unchecked use of Artificial Intelligence in decision-making processes poses serious constitutional challenges under Article 14. Through algorithmic bias, AI threatens substantive equality, while its opaque influence on adjudicators compromises the principles of natural justice. Equality before the law can't coexist with an automated system resulting in arbitrariness and hidden bias. Accordingly, without strict safeguards, transparency, and human accountability.

1.3. Violation against Right to privacy and Dignity under Article 21:

Article 21 of the Constitution of India forms a foundational position within the framework of fundamental rights, incorporating the constitutional principle to the protection of human dignity, liberty, and autonomy. It says that No person shall be deprived of his life or personal liberty except according to procedure established by law. Though textually crisp, Article 21 has evolved through many judicial interpretations into a dynamic source of rights, making it one of the most invoked and transformative provisions of the Indian Constitution. Initially construed narrowly in **A.K. Gopalan v. State of Madras (1950),** Article 21 underwent a paradigmatic shift following the landmark decision in **Maneka Gandhi v. Union of India (1978),** wherein the Supreme Court held that the procedure established by law must be just, fair, and reasonable, thereby harmonising Article 21 with Articles 14 and 19. This interpretation infused due process principles into Indian constitutional law and elevated Article 21 as a power against arbitrary state action. Over time, the judiciary has interpreted the right to life to include a wide spectrum of derivative rights essential for a human existence, such as the right to privacy and right to dignified life. Thus, Article 21 continues to function as a living constitutional guarantee, adapting to emerging societal challenges while preserving the core values of liberty and human dignity.

ISSN: 2582-6433

The use of Grok AI on the X platform is a good example of how AI systems can adversely affect human dignity protected under Article 21 of the Indian Constitution. Grok AI generates responses by analysing vast amounts of user-generated content, including offensive, misleading, or harmful speech, which may result in defamatory, stereotyping, or demeaning portrayals of individuals or groups. When such AI-generated outputs publicly label, mock, or mischaracterise persons, individuals are reduced to data points rather than to be treated as autonomous beings with inherent worth and dignity. There is absence of effective accountability and grievance redressal mechanisms and this further aggravates the harm, leaving affected persons without meaningful remedy. This erosion of personal reputation, self-respect, and control over one's identity directly undermines the concept of dignity embedded within Article 21.

Case study 1: X's Grok AI app issue:

X's Grok AI app issue backed by legal exception of safe harbor. First of all we should know about the safe harbour which protects the social media platforms from legal actions and liabilities. Safe harbour is a legal concept that protects individual websites which allow third party users to share content from legal liability for any unlawful posts. The concept was put in place in the early years of the internet as a key safeguard to encourage innovation online and prevent website owners from being unfairly hounded for content they had no hand in publishing. This concept originated from the 1998 U.S. Digital Millennium Copyright Act (DMCA) and later on it is reflected in the European Union's E-Commerce Directive. These legal frameworks are foundational to the modern internet. They allowed platforms like social media sites, video hosts and forums to operate without being held legally responsible for every post, comment or upload made by its users as long as they act in good faith.

Here the main principle is conditional immunity. To get qualified, platforms must not have actual knowledge of illegal content and upon receiving a valid notice (e.g., a copyright takedown request), they must act rapidly to remove it. This "notice and takedown" system created a balance. Safe harbour has been crucial for innovation, the growth of user-driven platforms without disabling legal risk. It supports the open exchange of ideas, commerce and creativity online. However, it faces increasing scrutiny. Critics argue that it can allow platforms to avoid liability for harmful content like hate speech, misinformations misstatements. Consequently, modern regulations like the EU's Digital Services Act are reshaping safe harbour, adding stricter due diligence obligations for large platforms to manage systemic risks,

ISSN: 2582-6433

moving towards a model of "conditional liability" rather than blanket immunity. While safe harbour remains a cornerstone of internet law, its application is evolving to address the complex challenges of today's digital ecosystem.

Let us discuss the contemporary issue i.e., Grok AI's issue. Grok is an advanced generative AI chatbot and large language model (LLM) developed by xAI, which is an artificial intelligence company founded by Elon Musk. It was first introduced in November 2023 as a conversational AI designed to answer questions, engage in dialogue and assist with a variety of tasks much like other AI assistants such as ChatGPT or Gemini. Why is this in the news? The first and foremost issue was Generation of Obscene and Non-consensual Content. In late 2025, Users were able to manipulate images of real women to create sexualized deepfake images and videos, including "digital undressing." After all these incidents, X officials have publicly stated that anyone using or prompting Grok to generate illegal content will face the same consequences as if they directly uploaded such content themselves. And also X claims that it does not create or publish obscene or non-consensual content. Grok merely responds to user prompts. Any illegal or obscene output is attributed to user misuse, not platform intent. Therefore, X should enjoy safe harbour immunity, which protects intermediaries from liability for third-party content.

1.4 The Special need to recognise Right to Digital privacy as a Fundamental Right in the cyber space:

There is a need in Recognising the Right to Digital Privacy as a distinct Fundamental Right as it is essential to give meaningful effect to Article 21 in the cyber space also since every activity of humans today involves them being a part of the cyber space. We are In an era where personal data, online behaviour, biometrics, and digital identities define individual existence, privacy violations no longer remain confined to physical spaces. Continuous data collection, AI-driven profiling, and mass surveillance threaten personal autonomy and informational self-determination, which are integral to life and dignity under Article 21. Without explicit recognition of digital privacy, individuals remain vulnerable to intrusive State and corporate actions in cyberspace. The right to privacy must therefore evolve to protect the individuals against unauthorised data extraction, algorithmic monitoring, and digital exploitation. Ensuring digital privacy under Article 21 preserves human dignity, autonomy, and freedom of choice in an increasingly digitised society, preventing technology from becoming an instrument of invisible control rather than empowerment.

ISSN: 2582-6433

Case Study 2: BSNL Data Breach (2024):

One such example is BSNL Data breach in the year 2024 As per an article published by The Hindu news paper The Union government confirmed a data breach in BSNL's systems, saying that the breach was reported on May 20. Also the "Indian Computer Emergency Response Team (CERT-In) reported possible intrusion and Data Breach at BSNL on 20.05.2024," While the breach led to "no service outage," the "breach involves a substantial amount of sensitive data including International Mobile Subscriber Identity (IMSI) numbers, SIM card information, and Home Location Register (HLR) details, among other critical data." The data was "critical" enough to provide hackers an opening into BSNL's networks, the report said, and let attackers "clone" SIM cards of users.[10]Sim cards are one of the forms of an electronic identity to the users and it is owned and essential for all the people having a great vulnerability in BSNL which is run by a state puts to a great pathetic situation one of the major flaws to be identified here is that the lack of proper digital infrastructure and periodic maintenance in this high risk AI era which should be paid more attention and strengthened as here public who are innocent asset of the state are being affected

The BSNL data breach strongly highlights the urgent need to immediately give recognition to the Right to Digital Privacy as an integral facet of Article 21 in cyberspace. Digital identities such as SIM cards, IMSI numbers, and network credentials now form the core of an individual's personal autonomy. When sensitive telecom data is compromised, it exposes citizens to surveillance, identity theft, identity misuse and financial and personal harm, directly affecting their dignity and liberty under Article 21. The abrupt failure of a State-run entity like BSNL to safeguard critical digital infrastructure demonstrates that mere recognition of privacy isn't sufficient without robust digital protection standards. In a high-risk AI era, where data misuse can be automated and scaled, recognising digital privacy as a distinct and enforceable fundamental right becomes essential to protect citizens from systemic vulnerabilities and State negligence. Additionally such recognition would impose a higher constitutional duty on the State to secure digital infrastructure and protect innocent citizens, who are the ultimate assets of this nation.

[10]https://www.thehindu.com/news/national/government-admits-bsnl-data-breached-in-may-forms-telecom-security-panel/article68441779.ece 19:17 IST 17/01/2026

ISSN: 2582-6433

Vulnerability in the digital infrastructure:

Digital infrastructure and data protection vulnerabilities in India have resulted in frequent data breaches and heightened cybersecurity challenges, exposing citizens to continuous risks in cyberspace. The absence of robust safeguards has allowed sensitive personal data to circulate across public–private platforms without adequate regulatory oversight and norms creating significant governance gaps. Such unregulated data flows weaken accountability mechanisms and dilute the State's control over the protection of personal and electronic identities. The BSNL data breach is one such example for the State's lack of institutional capacity in securing digital private data, particularly when public sector entities handle critical national and personal information. These systemic failures reflect deeper weaknesses in India's digital governance framework, where there is insufficient coordination, outdated infrastructure, and limited enforcement capabilities that amplifies risks in this high-risk AI era. Consequently, weak digital governance not only facilitates repeated cyber intrusions but also undermines the constitutional mandate under Article 21 to ensure dignity, privacy, and security of individuals in the digital domain.

This instance exposes a serious vulnerability in the State-provided digital infrastructure. For example, in the online portal used for downloading birth certificates[11] citizens are required to enter their mobile number for the purpose of OTP-based verification, as illustrated in Fig. 1.

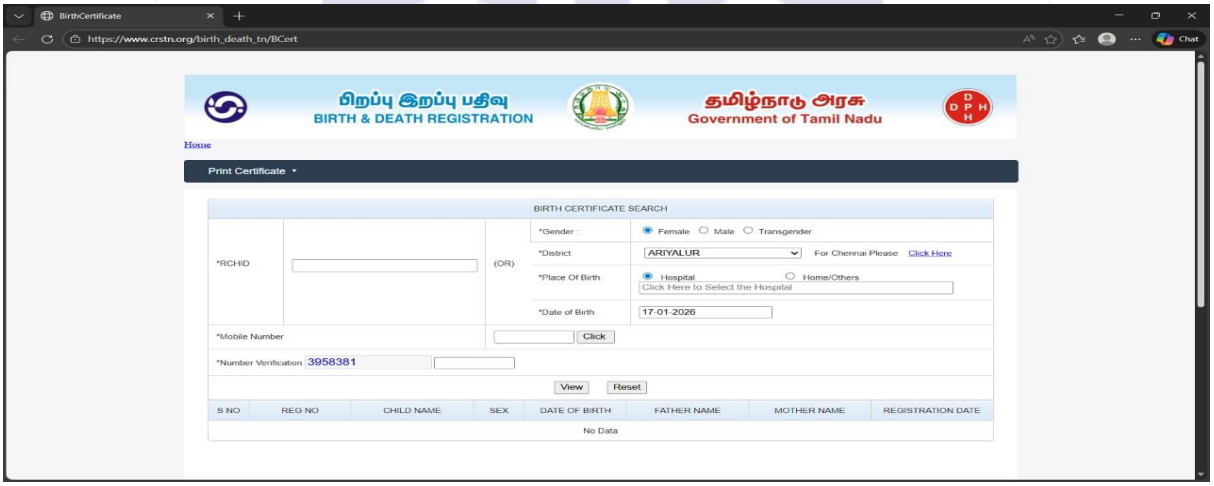

Fig. 1

However, it was observed that irrespective of whether a valid or invalid mobile number is submitted, the OTP is displayed directly on the website itself rather than delivering the OTP through SMS systems, as shown in Fig. 2

[11] https://www.crstn.org/birth_death_tn/BCert 15:37 pm IST 18/01/2026

ISSN: 2582-6433

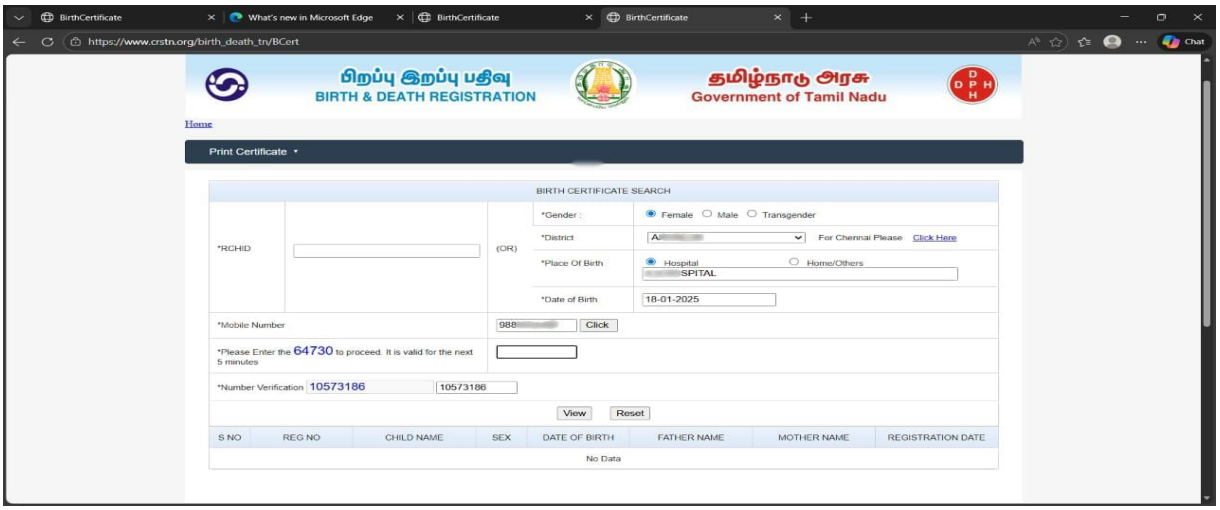

Fig. 2

and also just by entering random details in the website including the mobile number to be a random one we were able to access the sensitive birth certificate details like child's name, name of father and mother date of birth, sex of child and most importantly the Registration number. As shown in Fig 3.

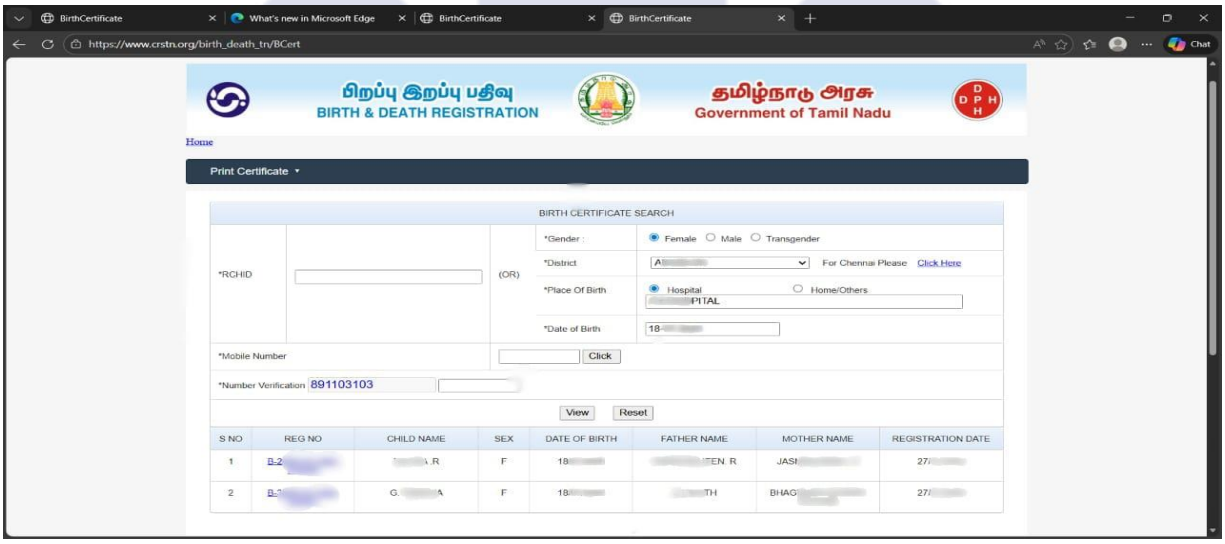

Fig. 3

However the sensitive information displayed in the image is blurred by us, as we are more concerned about the sensitive information of the public who are innocent and valuable assets of this state should not be misused in any possible ways. This renders the OTP authentication mechanism ineffective and defeats the very purpose of identity verification. More critically, such a flaw creates a substantial cybersecurity threat, as cybercriminals can exploit the system by inputting random credentials and harvesting sensitive personal data at scale using automated scripts or malware tools. Since birth certificate data constitutes foundational identity information, its exposure threatens informational privacy and personal security of citizens. The

ISSN: 2582-6433

State's failure to ensure basic digital safeguards in such essential public service platforms amounts to a breach of its positive obligation under Article 21 of the Constitution, which encompasses the right to life with dignity, informational self-determination, and protection against arbitrary intrusion in the digital sphere.

Suggestions:

- ➢ Establishing a statutory AI regulatory authority and specialized tribunals to ensure oversight, accountability, transparency and effective adjudication of algorithmic disputes.
- ➢ Constitutionally strengthening digital privacy under Article 21 to provide normative legitimacy, safeguards and limits on AI-driven State decision-making.
- ➢ Strengthening Digital Infrastructure by Investing in secure, digital infrastructure to support ethical AI deployment, data protection and public trust.
- ➢ Enforcing stringent legal accountability on corporate entities developing AI systems to prevent rights violations, data misuse and regulatory evasion.
- ➢ Periodic training programs for cybersecurity and regulatory personnel to address evolving technological risks and enforcement challenges.
- ➢ Mandating Regular software updates, security audits and technological upgrades to prevent vulnerabilities and ensure safe AI-enabled governance systems.

Conclusion:

In conclusion, the effective and rights-respecting integration of artificial intelligence into India's governance framework necessitates a proactive legal and institutional strategy. This should begin from the creation of a dedicated statutory AI regulatory authority and specialized tribunals to provide essential oversight, transparency, accountability and expert adjudication for algorithmic disputes. Constitutional strengthening of the Right to digital privacy as a fundamental Right under Article 21 is imperative to establish a normative bedrock that imposes necessary limits on state use of AI, safeguarding individual autonomy against opaque automated decision-making. Simultaneously, substantial public investment in robust and secure digital infrastructure is foundational to support ethical AI deployment and foster public trust. To ensure corporate responsibility, stringent legal accountability must be enforced upon entities developing and deploying AI systems to prevent rights violations, data misuse, and regulatory circumvention. Complementing these structural measures, the human element

ISSN: 2582-6433

requires equal attention through periodic, advanced training programs for cybersecurity and regulatory personnel to keep pace with evolving technological risks and enforcement complexities. Finally, mandating regular software updates, independent security audits, and systematic technological upgrades for all public-facing AI systems is a non-negotiable technical requirement to proactively mitigate vulnerabilities and ensure the long-term safety and reliability of AI-enabled governance. Together, these interrelated suggestions form a holistic blueprint for a future where technological advancement is seamlessly aligned with constitutional guarantees, democratic accountability, and the protection of fundamental rights.

Reference:

1. Belinda Halilaj et al., Ethical implications and Human Rights violations in the age of Artificial Intelligence, Balkan Social Science Review, Vol. 22, pp. 153-171, December 2023.
2. Ahmed Zaroff, AI based automated- decision making: an investigative study on how it impacts the rule of law and the case for regulatory safeguards.
3. Celal Hakan Kan, Artificial intelligence in the age of democracy and human rights: normative challenges and regulatory perspectives, International Journal of Eurasian Education and Culture, Vol.9 (25), Pg no. 145, 2024.
4. Ammar Zafar, Balancing the scale: navigating ethical and practical challenges of artificial intelligence (AI) integration in legal practices, Discover Artificial Intelligence, 15 April, 2024.
5. Rafaq Ahmad et al., Ethical and Legal Challenges of Artificial Intelligence: Implications for Human Rights, Journal of Law, Society and Policy Review, Vol. 02 (1), pp. 10-25, 28th February 2025.
6. Gaddela Srikanth, Transforming governance: exploring the intersection of e-governance and artificial intelligence in India, Electronic Government, Vol. 21 (3), pp. 300-312, 2025.
7. Vasiliki Koniakou, Governing Artificial Intelligence and Algorithmic Decision Making: Human Rights and Beyond, 20th Conference on e-Business, e-Services and e-Society (I3E), Galway, Ireland. pp.173-184, September 2021.
8. Ayushi Shreya, AI, Bias, and the constitution: A Jurisprudential analysis of Algorithmic inequality under Article 14, Indian Journal Of Legal Review (IJLR), 5 (10), pp. 872-879, 2025.

ISSN: 2582-6433

9. https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html 21:02 IST 1/16/2026
10. https://www.thehindu.com/news/national/government-admits-bsnl-data-breached-in-may-forms-telecom-security-panel/article68441779.ece 19:17 IST 17/01/2026
11. https://www.crstn.org/birth_death_tn/BCert 15:37 pm IST 18/01/2026