VOLUME 4 | ISSUE 3

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

ARTIFICIAL INTELLIGENCE AND DATA LOCALIZATION – AN URGENT NEED OF CONTEMPORARY LAW IN INDIA: STUDY

- Vipul Jain[1] & Dr. Sushanta Shadangi[2]

❖ Abstract

The rise of artificial intelligence (AI) raises questions about responsibility, particularly in criminal contexts due to AI's autonomy and human-like actions. This article examines legal doctrines to understand liability for AI behaviour. Proposed solutions include recognizing the rights of AI owners or creating liability for AI entities, but neither fully resolves the issue. The owner's duty of care could be the best solution, holding owners accountable for AI actions. However, criminal liability for AI remains challenging.

Data localization laws restrict the free flow of information across borders, impacting knowledge management. This affects data science, which thrives on access to data. To ensure data science can flourish while protecting personal rights, regulators should adopt processes that avoid unnecessary restrictions. Regulating data flow can benefit data research and personal rights protection.

❖ Introduction

Artificial Intelligence (AI) is a field of computer science aiming to create intelligent machines that can think and behave like humans. John McCarthy, a pioneer in AI, defined it as the science and engineering of making intelligent computers. AI involves developing algorithms that enable computers to learn and perform intelligent tasks with minimal human intervention. This technology finds applications in various domains such as robotics, e-commerce, diagnostics, gaming, mathematics, military planning, and transportation. AI

[1] LLM (Corporate and Commercial Law), ICFAI University, Dehradun, Uttarakhand, India

[2] Chief Mentor, LLM (Corporate and Commercial Law), ICFAI University, Dehradun, Uttarakhand, India

©2024 International Journal of Advanced Legal Research

researchers study how humans think, learn, make decisions, and solve problems to create intelligent software and systems.

Data localization refers to laws requiring data about a country's citizens or residents to be collected, processed, and stored within that country's borders, often following the enactment of local privacy or data protection laws. This concept is rooted in data sovereignty, which asserts control over certain types of data through applied rules. For instance, data about citizens may need to comply with a country's personal or financial laws, necessitating its storage within the country's borders. In some cases, data must be removed from foreign systems before it can be transferred to the country's systems. This ensures that data is handled according to local regulations and protects the privacy and rights of citizens.

❖ Research Methodology

The research methodology employed in this paper includes primary and secondary legal sources and a doctrinal methodology. This study aims to analyse the impact of Artificial Intelligence (AI) on the future of work and the HRM function. With AI becoming increasingly prominent in businesses, there are concerns about its potential to cause mass unemployment and reshape job roles. To understand how AI will transform jobs, a qualitative research approach using secondary data was chosen due to the difficulty of conducting a study involving a large number of participants. The study focused on four main objectives: identifying new job structures in the AI era, understanding the impact on work organization and environment, determining the skills necessary for success in an AI-driven culture, and assessing the impact of AI on HR management. An exploratory study was conducted to comprehend the context of AI-related changes in the workplace, leading to the development of these objectives. Subsequently, a descriptive study was carried out to analyse these objectives in depth and provide recommendations and conclusions. Secondary data from authentic studies, research papers, and articles by consulting firms, organizations, and HR leaders were analysed qualitatively to develop frameworks for understanding the objectives, with conclusions drawn from these frameworks and recommendations provided by the studied materials.

❖ UNDERSTANDING ARTIFICIAL INTELLIGENCE

©2024 International Journal of Advanced Legal Research

➢ WHAT IS ARTIFICIAL INTELLIGENCE?

Artificial Intelligence (AI) is a field of computer science aiming to create intelligent machines. It encompasses understanding human thinking processes and replicating them in computer systems. Alan Turing's Turing Test, proposed in 1950, is a benchmark for machine intelligence, suggesting a machine can be considered intelligent if it can mimic human conversation effectively. Roger C. Schank identified five qualities essential for intelligence: communication, internal learning, external information, goal-driven conduct, and creativity. John McCarthy, the father of AI, defined it as the science and engineering of creating intelligent machines. The Dartmouth Conference in 1956, attended by McCarthy, further refined AI's definition, emphasizing its focus on building intelligent computer programs. Marvin Minsky's later interpretation saw AI as the study of enabling machines to perform tasks requiring human-like intelligence. AI research covers diverse areas such as robotics, e-commerce, gaming, etc., with the United States leading in AI development. Despite challenges in defining intelligence, AI continues to advance, aiming to create machines capable of human-like cognition and behaviour.

➢ ARTIFICIAL INTELLIGENCE AND CREATIVITY

The concept of artificial creativity has been pondered for over 170 years, alongside artificial intelligence. Ada Lovelace, an English mathematician in 1843, suggested that even a computer, as sophisticated as it may be, lacks true human-like intelligence unless it can generate original ideas. Lovelace's idea led to the formalization of the Lovelace Test in 2001, which challenges AI to produce results beyond what its creators have explicitly programmed. No AI has yet passed this test. Despite this, AI has achieved tasks considered creative and original, which would typically be associated with human intelligence. Some examples include composing music, creating artwork, generating innovative designs, and even writing literature. These achievements demonstrate AI's ability to produce outputs that exhibit creativity and originality, albeit within the constraints of its programmed algorithms and data inputs.

➢ DIFFERENT FORMS OF ARTIFICIAL INTELLIGENCE

Various forms of Artificial Intelligence (AI) pose challenges regarding criminal liability. Bots, such as those on the Darknet, demonstrate unpredictability. For instance, the Random

©2024 International Journal of Advanced Legal Research

Darknet Shopper made unauthorized purchases, and Microsoft's Tay exhibited offensive behaviour despite its creators' good intentions. Drones and autonomous cars, equipped with AI, raise safety concerns due to accidents and potential criminal use. High-frequency trading AI systems can cause market disruptions, as seen in the 2010 stock market crash. Regulations like the EU's MAR and MAD address such issues. Algorithmic trading can also be manipulated for market control, as seen in the Timber Hill case. Military applications of AI, including autonomous weapon systems, raise ethical and legal questions. Some have called for a ban on such systems to prevent an AI arms race. AI in healthcare, while promising, faces legal challenges, such as determining liability for AI errors in medical diagnoses. These examples highlight the complex legal and ethical implications of AI in various domains.

❖ UNDERSTANDING DATA LOCALIZATION

Data localization laws require that data about citizens or residents of a country be collected, processed, and stored within the country's borders, ensuring compliance with local privacy and data protection laws. India's Data Localization Act governs such measures, mandating data be stored domestically. India has enacted various sector-specific policies regarding data storage, including those for commerce, telecommunications, and health. These policies aim to enhance cybersecurity, privacy, national security, and innovation while preventing foreign surveillance. Recommendations for data governance vary between general and sector-specific needs. The General Agreement on Trade in Services (GATS) is crucial in understanding the implications of these policies on international trade, particularly in bilateral negotiations with the US and EU. These measures have significant implications for individual privacy, businesses, and international relations, shaping the future of digital trade agreements and data sovereignty.

➢ IMPORTANCE OF DATA LOCALIZATION

Data localization is crucial for safeguarding the personal and financial information of a country's citizens from foreign surveillance and ensuring access for local authorities. Recent incidents like WhatsApp-linked lynchings and Facebook's data sharing with Cambridge Analytica have highlighted the need for such measures globally. Local data storage aids law enforcement in investigations, preventing delays caused by mutual legal assistance treaties (MLAT). Despite the benefits, managing multiple data centers locally requires significant

©2024 International Journal of Advanced Legal Research

infrastructure investment and may increase costs for global companies. India's Data Protection Act and other regulations aim to protect privacy and enhance security. While global tech companies may oppose data localization, it benefits India's economy by encouraging local data management and attracting investment. Machine learning, artificial intelligence, and the Internet of Things can derive immense value from localized data, benefiting both public safety and economic growth.

- **WHAT ARE THE OBJECTIVES OF LOCALIZATION OF DATA?**

The objectives of data localization are multifaceted. Firstly, it aims to foster innovation and develop local ecosystems, as highlighted by the Srikrishna committee, recognizing AI as a key driver of economic growth. This aligns with global trends seen in China and the Americas. Secondly, data localization seeks to enhance national security by protecting citizens' data from foreign surveillance and ensuring accessibility for law enforcement. Currently, accessing Indian citizens' data stored in the US is slow and cumbersome due to mutual legal assistance treaties (MLAT), while submarine cables make data transmission vulnerable to interception. Regionalization can mitigate these risks and safeguard citizens' privacy. Overall, data localization serves to promote economic growth, protect national security, and enhance privacy rights for citizens.

- **What are the potential spill-overs and risks of a localization mandate?**

The potential spill-overs and risks of a localization mandate include:

a) Customs and policy: Localization can impact India's trade relations with its partners.

b) Security risks: Storing data in multiple locations increases the risk of unauthorized access. Thus, infrastructure development needs to prioritize security measures.

c) Financial impact: Restrictions on cross-border data flow can increase compliance costs and hinder access to foreign service providers. These costs may be passed on to consumers, affecting the economy. Compliance challenges include high data creation costs and India's challenging weather. Additionally, startups may face integration restrictions from other countries, limiting their international exposure.

- **SOVEREIGN CONTROL OF DATA**

©2024 International Journal of Advanced Legal Research

In discussions surrounding data management systems, various terms like regional data, live data, national data, and evidence are commonly used to address the need for states to control data within their borders. While these terms are often used interchangeably, it's important to understand their nuances. Data localization and residency requirements refer to policies mandating local storage and processing of data. Regional data encompasses laws restricting data movement internationally and regulating its local storage. These laws may include requirements for local data storage, content production, or conditions on cross-border data transfers, effectively acting as data localization mandates.

- **Data Nationalism, Data Protectionism, Data Sovereignty and Data Colonialism**

Data nationalism refers to laws governing the management of local data, while data exceptionalism argues that data is non-regional and challenges territorial jurisdiction. However, proponents of "private knowledge" assert geographical limits on data. Data sovereignty ensures national law applies to data, even if it is outside the country. Some argue for storing data within the country for sovereignty reasons. Data colonialism refers to modern Western digital companies' practices, akin to historical cultural colonization, which influences income and behaviour through knowledge control.

- **IMPACTS OF DATA LOCALIZATION**

Data localization aims to enhance information security, protect public information from foreign government access, facilitate data access for national regulators, and create local job opportunities. However, there's limited evidence that localizing data achieves these goals. Data security relies more on infrastructure investment and maintenance than on physical data location. For instance, data fragmentation in cloud storage enhances security by dispersing data across multiple systems. Additionally, local data mandates may reduce investment in security measures. Restrictions on cross-border data flow can increase risks of money laundering and terrorist financing, as seen in mobile money services hindered by regulations. Moreover, increased costs or lower service quality due to localization mandates may lead companies to leave, negating any positive impacts on job creation.

- **DATA PROTECTION ACROSS THE WORLD**

Over the past decade, regional data regulations have expanded globally. Russia has the strictest laws on data flows with severe penalties. The European Union's General Data

©2024 International Journal of Advanced Legal Research

Protection Regulation (GDPR) restricts data streaming to countries with strong data protection. China mandates important information to be stored locally and requires security assessments for cross-border data transfers. The United States has the CLOUD Act for data sharing with certain countries.

- **SECURITY RISKS DUE TO DATA LOCALIZATION**

Data localization itself does not guarantee security; data controllers must ensure strict protection of authorized data. India's repeated breaches of Aadhaar citizen data highlight this. Storing data locally is not inherently secure until effective data protection laws are enacted and proven. The Supreme Court's ruling in the Puttaswamy case established privacy as a fundamental right and emphasized the need for legal safeguards against government surveillance. Adequate legal protection is essential to enable legitimate law enforcement access to data.

- **ECONOMIC AND POLITICAL HARMS**

Policy mandating data localization could harm the Indian economy in several ways. Requiring Indian companies to store data locally may hinder their international expansion and burden them with maintaining various legal and technological standards across countries. Additionally, localizing only a fraction of the personal information held by Indian companies could still have significant economic consequences. The Indian outsourcing industry relies on the ability to store and process data in India for foreign clients, which could be jeopardized by local regulatory requirements. Furthermore, if India mandates local data storage for foreign companies operating in India, other countries may follow suit, leading to conflicts and business challenges for Indian companies.

- **NECESSITY OF A STRONG REGULATOR**

A strong regulatory authority is necessary for effective data protection and management. Strong data protection laws and regulations enforced by a regulatory authority will provide better protection for users and businesses compared to relying solely on local data storage mandates. The regulatory-powered Data Protection Authority (DPA) can incentivize companies to comply with data laws while ensuring privacy protection, accountability for both public and private sectors, and enforcement of rights on behalf of all Indians.

©2024 International Journal of Advanced Legal Research

➢ THE ROLE OF GOVERNMENT IN DATA PRIVACY PROTECTION

The government plays a significant role in protecting data privacy, not just private companies. There's a debate about how much personal data governments should collect, store, and process, and what laws should protect citizens' privacy. While governments collect personal information to improve public services and security, concerns arise over data protection, especially in countries lacking cybersecurity measures. The debate over freedom versus security remains relevant, with issues of state surveillance and individual privacy at the forefront. Despite various data protection laws, inconsistencies exist globally, posing challenges in data collection. Questions arise about the extent of data collection by governments and private companies, along with legal and ethical restrictions to prevent over-collection and misuse. Moreover, data ownership is a complex issue as governments, organizations, and even games collect personal data. The digital age introduces new challenges in data retention policies, with issues of lost, damaged, or misused information. Property rights concerning data are divided into privacy, intellectual property, and confidentiality laws, each aiming to protect data from unauthorized access and use.

❖ LIABILITY ISSUES UNDER ARTIFICIAL INTELLIGENCE

➢ CRIMINAL LIABILITY

Computer-based intelligence is now an integral part of modern life, raising concerns about potential risks. Isaac Asimov's three laws of robotics, formulated in 1942, have been widely discussed, with a fourth law later added. However, some consider these laws outdated. In 2015, over 1000 AI scientists, including Stephen Hawking and Elon Musk, warned about the dangers of AI warfare and autonomous weapons. Gabriel Hallevy questions which laws or ethics should govern AI and who should decide. He notes that fear of AI stems from its lack of legal accountability, unlike corporations. However, concerns have eased as companies are now subject to criminal and corporate laws.

- **AI: - ACTUS REUS & MENS REA**

Criminal liability in AI revolves around actus reus and mens rea. Actus reus involves identifying the actors involved in AI decision-making, such as users, administrators, manufacturers, software developers, and outsiders. Users and administrators control AI

©2024 International Journal of Advanced Legal Research

behaviour directly or remotely, while manufacturers are responsible for AI hardware, software, and development. Software developers, although third parties, also play a role. Outsiders, like hackers or malware, can influence AI behaviour. However, criminal responsibility ultimately rests with humans behind AI actions, depending on their ability to influence AI behaviour. Users and administrators are responsible for AI use, especially when they control or influence its actions. Manufacturers are responsible for AI design and programming, but issues arise when AI behaves unexpectedly. The owner's liability is yet to be fully determined but will likely be significant. Ultimately, accountability depends on how much control individuals have over AI behaviour.

- **CRIMES AND CRIMINAL ACTS**

In criminal law, there must be a human agent to be held accountable for the actions of artificial intelligence (AI), as only individuals can commit crimes. Actus reus, the guilty act, forms the external elements of an offense, focusing on the action rather than the defendant's mental state. Actus reus elements typically involve conduct, circumstances, and consequences. The conduct component includes both acts and omissions likely to have caused the offense. However, for an act to be considered a criminal offense, it usually requires human control. Criminal law traditionally focuses on positive acts, where the defendant has control over the action resulting in an anticipated outcome. Yet, AI introduces a challenge as it operates with increased autonomy, reducing human control. While AI's actions may constitute positive acts in a legal sense, humans may not actively participate or be involved when the AI commits the act. However, there are exceptions where positive action may not be required.

- **OMISSIONS IN GENERAL**

The actus reus requirement encompasses omissions, where the defendant fails to act despite having a duty to do so, constituting a legal omission. For instance, a tired driver who falls asleep at the wheel, causing harm, could be held liable either for driving while fatigued or for failing to stop the vehicle when feeling tired. Similarly, in the case of crimes committed by AI, human liability for omissions is crucial for prosecution. This duty to act can arise in two main scenarios:

©2024 International Journal of Advanced Legal Research

1. Duty based on specific obligation: This duty arises from a role or contractual obligation, legally binding or customary, imposing a responsibility on the defendant to act.
2. Duty based on a special relationship to the harm: Duties stemming from awareness of a real risk of harm, requiring the defendant to act to avoid it. Even an unintended act can create a duty to prevent harm when the risk is foreseeable.

However, prosecution for omissions should only occur when the defendant could have acted but failed to do so, according to the principle of lex non cogit and impossibilia. For AI, this means that only humans likely to influence the AI's core decisions can be held criminally liable when AI causes harm. Therefore, the responsibility for criminal liability in cases involving AI falls primarily on those who can impact the AI's actions.

- **A DUTY TO ACT ASSUMING A PARTICULAR RESPONSIBILITY**

In certain circumstances, individuals may have a legal duty to act when they have a particular responsibility over an AI, such as when they are in a supervisory role. This duty is more specific than a general duty of care, and it arises from common law obligations or contractual agreements. For instance, a supervisor overseeing drones' routes has a duty to intervene if necessary to prevent harm. In a scenario where a supervisor, A, fails to redirect a drone that poses a risk to an airport runway, resulting in a collision, A breaches both his contractual obligation to manage the AI and his duty to intervene. Similarly, individuals like B, who have the ability to control an AI, may be held responsible for failing to intervene when necessary. For example, if B, while using a semi-autonomous vehicle, watches a movie instead of taking control when needed, **he** may be considered liable for any resulting accidents. Therefore, only those in management positions or with explicit responsibilities over the AI can be held accountable for its actions. Other actors, like clients or users, may have a close relationship with the AI but generally do not bear the same level of responsibility.

- **A DUTY TO ACT DUE TO SPECIAL RELATIONSHIP TO THE HARM**

In certain cases, individuals may have a legal duty to act due to their special relationship to the harm caused by an AI, although the requirements for such a duty vary across legal frameworks. This duty arises when the defendant's actions lead to a real risk of harm and when they fail to act unfairly in harsh circumstances. For instance, clients and supervisors of

©2024 International Journal of Advanced Legal Research

AI are obligated to act according to their roles and duties, as specified by contracts or customs. Consider a scenario where a manufacturer, C, fails to address a glitch in AI-operated robotic surgeons, causing harm during surgeries. C's failure to update the program despite being aware of the glitch constitutes a real risk of harm and establishes a duty to act. Similarly, another manufacturer, D, may have a moral obligation to inform customers about the conditions under which their autonomous vehicles are tested, although the lack of an actual risk of harm may limit legal liability. However, as AI becomes more autonomous and unpredictable, the extent of liability for manufacturers becomes less clear, especially when AI begins to learn and behave independently. Therefore, the determination of legal responsibility in such cases remains a complex issue.

- **CAUSATION AND ARTIFICIAL INTELLIGENCE**

Causation in legal terms is the connection between the defendant's actions and the resulting harm, usually determined by the "but for" test. However, this test is broad and may not always establish legal causation. Intervening causes, both intentional and unintentional, can break the chain of causation. With AI, causation becomes more complex. When an AI causes harm, the focus is on the defendant's duty to act and whether their failure to fulfil that duty led to the harm. For example, if a supervisor, F, leaves their position overseeing an AI trading securities, and the AI makes a damaging trade in their absence, F may be held responsible. The foreseeability of the AI's actions and the defendant's duty to control it are crucial. Additionally, if an AI causes harm by its own actions, such as acquiring an illegal item, the defendant's actions may still be seen as the legal cause if they could have prevented it. However, if the defendant acted lawfully, establishing causation becomes challenging, especially in cases involving self-made hazardous situations. In such cases, the defendant's duty to foresee and prevent harm from the AI's actions is crucial for determining causation.

- **THE INNOCENT AGENT DOCTRINE**

The Innocent Agent Doctrine considers how individuals can participate in a crime without being the primary offender. A person can enable an AI to commit a crime through guidance, assistance, or manipulation, making them an accessory. For instance, if someone instructs an AI to carry out a hacker attack on the tax agency, they are using the AI as a tool for the crime. However, if the AI causes harm unexpectedly, determining the individual's liability becomes

©2024 International Journal of Advanced Legal Research

more complex. Currently rare, such cases will likely increase in the future. If the AI autonomously decides to commit the crime, the individual cannot claim innocence. Thus, liability rests on whether the individual had control or oversight over the AI's actions.

- **REQUIREMENT AGAINST/LIABILITY OF ARTIFICIAL INTELLIGENCE**

As AI becomes more prevalent, questions of liability arise, particularly in cases of harm caused by autonomous machines and robots. Traditionally, robots and machines couldn't be held liable as they lack legal personhood. However, with the emergence of highly intelligent, autonomous machines, this notion is being reconsidered. While robots can't be sued like humans, they can still cause significant harm. Thus, the legal relationship between AI and its developer is crucial. Legal principles dictate that damages caused by the unlawful actions of another must be compensated. Therefore, the responsibility for harm caused by AI often falls on its developer or creator.

- **IMPORTANT CASES RELATED TO ARTIFICIAL INTELLIGENCE**

In the Hudson v. Tesla case, Hudson sued Tesla after his Tesla Model S, equipped with Autopilot, collided with other vehicles. He claimed "serious and permanent injuries" and accused Tesla of negligence and breach of warranty. Tesla defended itself, stating that Autopilot does not make the vehicle completely safe and that drivers are responsible for maintaining control at all times. Tesla also pointed out that Autopilot's limitations are clearly stated in the manual. This case highlights the debate over the responsibilities of drivers versus the capabilities of autonomous driving systems.

In the Nilsson v. General Motors case, Oscar Nilsson sued General Motors after being injured in a collision involving a Chevrolet Bolt in Autopilot mode. Nilsson argued that GM failed to operate the self-driving car lawfully, leading to the accident. GM settled the lawsuit for an undisclosed amount, but the incident raised concerns about the safety and legality of autonomous vehicles. Despite this, GM announced plans to release a Level 5 autonomous car without steering wheels or pedals, indicating the company's commitment to self-driving technology despite legal challenges.

- **CIVIL LIABILITY**

©2024 International Journal of Advanced Legal Research

In legal terms, harm is a fundamental element of liability, requiring demonstration for change. Arguments arise regarding the liability of fully autonomous AI systems, suggesting that if they are aware of their actions, they should be held accountable. Granting autonomy to AI implies endowing them with rights and obligations akin to legal persons. Thus, the question arises whether AI should be conferred legal identity if they are to be held liable. Although there are no definitive answers yet, the law is expected to evolve over time. Recent accidents involving autonomous vehicles from companies like Tesla and Uber have brought issues of liability for AI systems and their developers to the forefront. These incidents underscore the need for clear legal frameworks to address liability in the context of AI technology.

- **NEGLIGENCE**

Negligence claims against software vendors typically hinge on three elements: duty of care, breach of that duty, and harm suffered by the plaintiff. Whether software is considered a product or service affects the standard of care owed by developers. Gerstner suggests viewing AI systems as products and holds developers responsible for defects or inadequacies. However, Cole argues that AI should be seen as a service rather than a product, but there's no clear legal stance. Laws related to duty of care include providing accurate information, implementing error-checking mechanisms, and disclosing limitations. If AI is considered a product, it must be sold with a warranty, either express or implied. Implied warranties ensure the product is fit for its intended purpose, and contractual exclusions are often ineffective when AI is incorporated into other goods, like cars. Despite debates over whether AI is a product or service, it's crucial for developers to uphold a duty of care and provide adequate safeguards and disclosures to prevent harm to users.

➢ COMPARATIVE STUDY OF ARTIFICIAL INTELLIGENCE WITH OTHER COUNTRIES

- **UNITED STATES**

The United States has prioritized leadership in artificial intelligence (AI), with significant investments in research and development (R&D) and defense. The government emphasizes an "ethical AI community" and aims to regulate AI without hindering progress. Recommendations include investing in AI, educating the workforce, and aiding workers

©2024 International Journal of Advanced Legal Research

affected by automation. However, there's a lack of comprehensive vision on socially acceptable AI development, and the focus on self-regulation may favor industry goals over broader societal interests. The US also needs clearer strategies for addressing ethical issues and ensuring fair economic impact. The government emphasizes diversity in the AI workforce and inclusivity in AI development. Nevertheless, the reliance on market capitalism as the underlying framework is a critique across all reports. The OSTP report and other documents stress the importance of economic prosperity, education, and national security, but they tend to fit AI into existing national priorities rather than re-evaluating them. Overall, while recognizing the potential benefits of AI, the US needs a more comprehensive approach that addresses the unique challenges and opportunities of AI for society at large.

- **EUROPEAN UNION**

The European Union (EU) has initiated efforts to establish ethical rules for the development and implementation of artificial intelligence (AI). A group of experts appointed in June 2018 has been working to make these rules practical. The EU aims to increase investments in AI to at least €20 billion per year over the next decade. Compared to the US approach, the EU focuses more on robotics than AI and sees AI as an enabling technology for smart autonomous robots. The EU report addresses concerns about the impact of robotics and AI on the workforce, advocating for workforce training and monitoring tools. It suggests imposing taxes on companies benefiting from automation to counterbalance negative effects on tax revenues and social security. The report calls for the establishment of a European Agency for Robotics and AI to regulate and monitor these technologies, provide advice, and manage a registration system for smart robots. It emphasizes the need for a mix of hard and soft laws to address potential risks and calls for harmonized standards across EU member states. The EU stresses the importance of testing robots in real-world scenarios and calls for uniform criteria for such tests. However, it doesn't specify the basis for these criteria or address the distinction between primary and secondary rules in the legal system.

- **India**

India's legal framework has not yet addressed the legal status of AI machines, although there is recognition of AI's importance and potential. The Ministry of Industry and Commerce established a team in 2017 to explore AI's role in India's development. The team's report

©2024 International Journal of Advanced Legal Research

identifies ten key areas for AI development in India, along with major challenges and recommendations. The report suggests setting up an "Inter-Ministerial National Artificial Intelligence Mission" and establishing data banks, exchanges, and an ombudsman for data-related issues. It also recommends setting standards, developing human resources, and fostering bilateral collaborations for international rule-making.

Regarding intellectual property, copyright law requires a level of creativity for protection, but AI's status as a creator is uncertain. Patent law may evolve due to AI's role in innovation, and the definition of a design owner may become complex with AI involvement. Information protection laws in India require reasonable security practices, but concerns exist about their effectiveness, especially regarding sensitive data. E-contracts are recognized under the IT Act, but issues arise with enforceability against AI and understanding complex software-based terms. Liability and standard of care issues emerge with AI's involvement in actions causing harm. The law is yet to clearly define the responsibility of AI in such cases, which has implications for product liability and innovation adoption rates.

❖ LIABILITY ISSUES UNDER DATA LOCALIZATION

➢ DRAFTED BILL

The Drafted Bill on Data Protection Act outlines provisions for the transfer of personal data outside India. It permits the transfer of sensitive personal information with user consent and approval from data protection authorities. However, certain conditions must be met, including adequate protection of data, adherence to laws, and non-interference with law enforcement. The bill aims to mirror documents abroad but requires them to be kept in India. It follows European data protection standards, ensuring transferred data receives similar protection as under Indian law. Critical personal data can only be processed in India unless the government allows exceptions, ensuring national security. Sensitive information, if misused, can pose risks not only to individuals but also to society and the country. The Privacy Policy Bill, approved by the Union Cabinet in 2019, awaits parliamentary review.

➢ SOVEREIGNTY ISSUE OF DATA

Data residency refers to the practice of storing data in a specific location, often for legal or regulatory reasons, such as tax benefits. It involves ensuring that core activities, including

©2024 International Journal of Advanced Legal Research

data processing, are conducted within the country's borders. Data sovereignty goes beyond residency, emphasizing that data storage must comply with the laws of the country where it's physically located. This is crucial because privacy and security protections for individuals vary by location. Data localization, as seen in India's Personal Data Protection Act and Russia's OPD-Law, mandates that data be stored, processed, and accessed within the country's borders. Critics argue that such laws hinder data utilization and promote digital fragmentation. Understanding these distinctions is vital for businesses to navigate regulatory requirements and ensure compliance with data privacy laws. Key considerations include where data is stored, who owns the data center, backup processes, and the data privacy practices of cloud service providers.

- **DATA LOCALIZATION COMPARATIVE STUDY**

Data localization laws vary across different regions, with countries like Brunei, China, Indonesia, Nigeria, Russia, and Vietnam having some of the strictest regulations. For instance, Russia imposes fines of up to 18 million Russian rubbles for non-compliance with data protection laws. Similarly, China mandates the storage of certain business data within its borders. In the European Union, the GDPR governs data protection and privacy for EU citizens, regulating data transfers within and outside the EEA. Belarus, India, Kazakhstan, Malaysia, and South Korea have implemented various measures, including regulations specific to certain domains and requiring consent for cross-border data transfers. Australia, Canada, New Zealand, Taiwan, Turkey, and Venezuela have industry-specific data localization policies. However, not all countries have such laws, and some companies, particularly in the US, face conflicts with foreign governments over data localization. Setting up data centers locally can face challenges, including legal compliance, increased operating costs, and concerns about government access to data. While local data centers can facilitate business operations and access tax benefits, there are debates over data control and privacy, especially for companies with global operations like Flipkart and Paytm in India.

❖ PROBABLE POSSIBLE SOLUTIONS AND APPROACHES TO DEAL WITH IT'S ISSUES

- **FOR ARTIFICIAL INTELLIGENCE ISSUES**

©2024 International Journal of Advanced Legal Research

The issues surrounding artificial intelligence (AI) and criminal liability are complex, particularly in determining who should be held responsible for AI-related crimes. Various solutions and approaches have been proposed. One approach involves imposing a supervisory duty on AI owners to monitor and control AI actions to prevent harm. This duty, akin to civil law obligations, would create legal accountability. However, the unpredictability of AI behaviour poses challenges to this solution. Another suggestion is to grant legal personality to AI, similar to corporate entities, thus making AI directly liable for its actions. However, this raises questions about how AI can be punished and deterred. Changing fundamental principles of criminal law may be necessary to address AI criminal liability effectively. Despite these challenges, finding a solution is crucial as AI technology advances.

- **DIFFERENT MODELS OF THE CRIMINAL LIABILITY OF ARTIFICIAL INTELLIGENCE ENTITIES**

Criminal liability requires both actus reus (external behaviour) and mens rea (mental state). AI entities can be held liable using three models: perpetration-via-another, natural-probable-consequence, and direct liability. In the first model, AI is an innocent agent, acting on behalf of the programmer or user. The second model applies when AI commits an offense unintentionally during its normal functioning. Programmers or users are liable if they should have known the offense was a probable consequence of their actions. The third model treats AI as a human offender, liable if it meets actus reus and mens rea requirements. These models can be combined: perpetration-via-another for AI acting as an innocent agent, natural-probable-consequence when AI acts beyond intent, and direct liability when AI is the main perpetrator. This coordinated approach ensures all involved parties, whether human or AI, are held accountable under criminal law.

- **FOR DATA LOCALIZATION**

Encryption, particularly end-to-end encryption (E2EE) used in platforms like WhatsApp and Facebook Messenger, poses a challenge to data access. With 1.5 billion mobile users relying on E2EE for messaging, decrypting such data becomes difficult. For India, managing citizens' data both domestically and internationally is crucial, with concerns about foreign governments accessing data. The Srikrishna committee addressed these issues, emphasizing the need to balance data protection with technological advancement. While data localization

©2024 International Journal of Advanced Legal Research

laws are debated, a one-size-fits-all approach may not be suitable, and sensitive data should be treated differently. Cloud-based services offer cost-effective solutions for consumers and startups, aiding in global market access. However, the decision to establish data centers depends on various factors, including economic potential, privacy laws, and security measures. Ultimately, promoting innovation while safeguarding data privacy is essential for India's economic growth and technological development.

- **DATA LOCALIZATION AND DATA ACCESS AND DATA DRIVEN INNOVATION**

The development of data protection laws should consider key privacy and national security issues:

1. Data Access to Law Enforcement Agencies (LEAs): Hosting data locally does not automatically grant LEAs greater access. Access to data should be governed by recognized laws, ensuring the rights of accused individuals and offenders are protected under judicial oversight.
2. Improving Personal Protection: Localizing data may enhance personal protection by limiting access to third parties. However, the effectiveness depends on factors like purpose limitation, user engagement, and internal data management processes.
3. Impact on Economy and Innovation: Data localization can have negative effects on business growth and innovation. Studies suggest a potential decrease in GDP, growth rate, and foreign direct investment. India's digital transformation, including cloud adoption, can significantly boost GDP and support millions of MSMEs.
4. Role of Encryption: End-to-end encryption enhances personal privacy by securing communication. However, it poses challenges for LEAs' data access. Encryption is vital for cybersecurity, and LEAs must develop cryptanalysis capabilities to address these challenges effectively.

Overall, data protection laws should balance the needs of law enforcement with privacy rights, foster economic growth through innovation, and recognize encryption's importance in safeguarding personal data.

- **WHAT SHOULD DATA LOCALIZATION POLICY BE?**

©2024 International Journal of Advanced Legal Research

India's data localization policy should strike a balance between economic growth, innovation, job creation, and national security concerns. Recent directives, including the RBI's mandate for payment service providers to retain data locally, indicate a push towards data sovereignty. However, encryption policies must be carefully managed to ensure cybersecurity while protecting user privacy. Access to law enforcement agencies (LEAs) for encrypted communication is essential, but strict regulation is needed to prevent misuse. Legislators should focus on fostering the growth of cyberspace, acknowledging its potential for the economy. Cross-border data flows are crucial for India's IT/BPO industry, and the country should not impose regional data restrictions. Collaboration with countries like the US under agreements like the CLOUD Act can streamline LEA access to data without compromising legal processes. India should avoid sending negative signals on regional data to maintain its global competitiveness. A decision on data localization should await the recommendations of the Srikrishna Committee, ensuring a balanced approach based on economic needs, innovation, and international standards.

❖ CONCLUSION

➢ FOR ARTIFICIAL INTELLIGENCE

Artificial intelligence (AI) presents legal challenges concerning accountability for AI actions and the allocation of responsibility. The absence of clear legal guidelines raises questions about who should be held responsible for AI-related harm. Supervisory duties on owners, with an obligation to intervene to prevent harm, seem the most viable solution, although unpredictable AI behavior remains a challenge. The increasing use of AI across various sectors emphasizes the need for regulatory frameworks that balance innovation with ethical considerations and human rights. Key issues include determining AI accountability and clarifying the rights and responsibilities of programmers and manufacturers. Legal standards are needed to address AI's impact on society and ensure the protection of rights while fostering innovation. International cooperation through a new international governing body for AI regulation could streamline policymaking and prevent fragmented approaches that may lead to tensions between nations. This proposal aims to establish a comprehensive international regulatory framework for AI, promoting global cooperation to address emerging challenges effectively.

©2024 International Journal of Advanced Legal Research

➢ FOR DATA LOCALIZATION

The introduction of the Personal Data Protection (PDP) Act marks a significant step in India's data protection reform. However, the effectiveness of the new law depends on crucial aspects such as the classification of personal data, exemption conditions, and authorization by the government. Implementation of the PDP Act is pending until it is approved by the Indian Parliament and the President. Data localization initiatives in India have sparked debate within the tech industry, with some Indian companies supporting the move while international players like Google and Amazon oppose it. The government's aim to regulate foreign companies could lead to economic benefits and protect Indian citizens' financial information, as emphasized by digital payment companies like Paytm and PhonePe. While data localization can enhance security and reduce surveillance risks, it may hinder the growth of Indian startups reliant on cloud services. Overall, balancing the benefits and costs of data localization is crucial for India's data security strategy and economic growth.

❖ SUGGESTIONS

➢ FOR ARTIFICIAL INTELLIGENCE

To foster responsible AI adoption, a platform should be created for government agencies to promote AI leadership. Before implementing new technologies, compliance and legal issues must be thoroughly analysed. While caution is needed to reduce risks, innovation should not be hindered. With impending EU legislation and advancing AI, decision-makers will soon gain more control, opening up new opportunities for responsible AI development and market entry in India.

➢ FOR DATA LOCALIZATION

European concerns about terrorist attacks have led to stricter laws regarding the transfer of Passenger Information Records (PNRs). India's data localization laws aim to address similar security concerns and improve privacy. However, criticisms arise over government surveillance exemptions and doubts about the effectiveness of data localization in enhancing security. Despite protests from tech giants like Facebook and Google, data localization is seen as necessary to protect privacy and boost business. Yet, there are fears that it could hinder the

©2024 International Journal of Advanced Legal Research

global growth of Indian startups and established companies like Tata Consulting Services and Wipro.

❖ BIBLIOGRAPHY

WEBSITES VISITED / REFERENCES

1. https://tech.economictimes.indiatimes.com/news/corporate/data-localization-data-access-policy-challenges-for-lawmakers/64371561
2. https://www.lexology.com/library/detail.aspx?g=4c845762-e954-4f47-8809-f5ad0f5d3716
3. https://www.mondaq.com/india/new-technology/914028/regulating-artificial-intelligence
4. https://link.springer.com/chapter/10.1007/978-3-030-32361-5_1
5. https://www.loc.gov/law/help/artificial-intelligence/americas.php
6. https://timesofindia.indiatimes.com/blogs/toi-edit-page/power-over-privacy-new-personal-data-protection-bill-fails-to-really-protect-the-citizens-right-to-privacy/
7. https://www.prsindia.org/theprsblog/relaxation-labour-laws-across-states
8. https://www.prsindia.org/theprsblog/relaxation-labour-laws-across-states
9. https://www.prsindia.org/billtrack/personal-data-protection-bill-2019
10. https://www.insightsforprofessionals.com/en-us/it/storage/data-sovereignty-data-residency-data-localization

ACTS & BILLS

1. Digital Personal Data Protection Act, 2023
2. PersonalDataProtectionBill, India,2018.
3. PersonalData ProtectionBill, India,2019.
4. InformationTechnologyAct,2000.
5. IndianContractAct,1872.
6. IntellectualPropertyRights.
7. GeneralDataProtectionRegulation,EuropeanUnion, 2018.

©2024 International Journal of Advanced Legal Research