International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838, Print ISSN: 2664-682X
Received: 14-01-2024, Accepted: 29-01-2024, Published: 13-02-2024
Volume 6, Issue 1, 2024, Page No. 78-82

The impact of emerging technologies on cyber law

Pankaj Dhankhar[1], Shivangi Sinha[2*]
[1] Department of Law, Bharati Vidhyapeeth University, Pune, Maharashtra, India
[2] Assistant Professor, Department of Law, Bharati Vidhyapeeth University, Pune, Maharashtra, India

Abstract
Arising advancements, specifically Man-made reasoning (artificial intelligence), Web of Things (IoT) and Blockchain, have fundamentally changed numerous social aspects, including business, correspondence and administration. In any case, their quick spread likewise presents complex difficulties to the legitimate structure directing the internet. This exploration paper inspects the complex effect of these advances on digital regulation, looking at their effect on protection, security, licensed innovation privileges, and ward. It gives a far reaching survey of existing writing and contextual investigations, digging into the developing crossing point of innovation and regulation, and giving an outline of the advancement of digital regulation in the computerized age.

Keywords: Cyber law, artificial intelligence, internet of things, blockchain

Introduction

Prologue to New Advancements: Blockchain, the Internet of Things, and artificial intelligence.

Artificial intelligence: It is the process of computer-based simulation of human intelligence processes. These cycles incorporate getting the hang of, thinking, critical thinking, discernment and navigation. Technologies for artificial intelligence can be found in a wide range of applications, including expert systems, machine learning, natural language processing, computer vision, and robotics.

Web of Things (IoT): The Web of Things alludes to an organization of interconnected gadgets implanted with sensors, programming and different innovations that empower them to gather and trade information over the Web. IoT gadgets can incorporate regular gadgets like brilliant home gadgets, wearable wellness trackers, modern machines, clinical gadgets and ecological sensors.

The Blockchain: Blockchain is a technology for a distributed ledger that makes it possible to securely, transparently, and immutably record transactions on a computer network. Occasions kept in the blockchain are gathered into blocks and connected together in a sequential and cryptographic chain, shaping a carefully designed and irrefutable record.

Significance of Digital Regulation in Managing Advanced Exercises

Security of Privileges and Protection: Cyber Law provides individuals with a legal framework; freedoms and protection in the advanced world. It safeguards individual information against unapproved access, use and abuse by characterizing security strategies, protection approaches and assent systems.

Avoidance of Digital Wrongdoing: Cybercrime, which includes hacking, phishing, identity theft, cyberbullying, and cyber fraud, is the subject of cyber law. It characterizes wrongdoings and punishments for criminal behavior on the Web, deflects noxious entertainers and improves network safety measures.

The thesis provides an overview of how new technologies will affect cyber law. New technologies like artificial intelligence, the Internet of Things, blockchain, and biotechnology will fundamentally alter new cyber rights and laws. difficulties, open doors and moral contemplations that require imaginative administrative arrangements, interdisciplinary participation and worldwide collaboration to guarantee successful administration, security of freedoms and advancement of capable development in the computerized age.

The improvement of digital regulation

A verifiable viewpoint on the improvement of digital regulation

1960-1970: The introduction of PC organizations

The creation of computer networks in the 1960s and 1970s, as well as the early 1919s, marked the beginning of cyber law. indeed, even years, as ARPANET (High level Exploration Undertakings Organization).

The Present Day: The Development of Cyber Law

The 21st century has seen digital regulation grow to cover a great many legitimate issues, including information regulation, information insurance, computerized regulation, digital regulation

Outline of fundamental legitimate standards in the internet

Jurisdictional standards figure out which regulations and guidelines apply to Web movement, considering variables like the area of servers, clients and the effect of that action.

Protected innovation privileges: licensed innovation standards oversee the security of imaginative works and developments in the internet.

Expression freedom: The standards of opportunity of articulation ensure people and the freedom to communicate, share information, and voice opinions online.

New technological difficulties within the existing legal framework * Concerns regarding privacy: New advancements frequently include broad information assortment, handling and sharing, raising worries about the number of people; security privileges and information insurance.

Dangers to safety: New attack vectors and vulnerabilities are created by the interconnected nature of emerging technologies like IoT devices and AI-based systems.

Implications for privacy * Problems with data protection and AI-based surveillance * Mass surveillance: Data can be gathered and analyzed by AI-based surveillance systems from a variety of sources, including social media, closed-circuit television (CCTV) equipment, and closed-circuit cameras. broad communications and online stages

Absence of straightforwardness: It is challenging to comprehend how AI algorithms used in surveillance systems process data, make decisions, or identify individuals because they frequently function as black boxes.

Dangers to safety: Observing frameworks that utilization man-made consciousness calculations to process and investigate information are powerless against information breaks, digital assaults and unapproved access.

IoT device privacy concerns; data collection and storage: IoT devices continuously collect data from sensors, cameras, and interactions with users.

Security Weaknesses: IoT gadgets frequently need solid safety efforts, making them powerless against hacking, malware and unapproved access.

Absence of encryption: Unauthorized parties are able to intercept and eavesdrop on sensitive data because many Internet of Things devices transmit data over unencrypted channels.

The privacy-enhancing potential of blockchain technology * Immutable data storage: Blockchain gives unchanging and blunder free information stockpiling where information can't be changed retroactively without the assent of organization members.

Decentralized design: Blockchain runs on an organization of decentralized hubs, so there is no requirement for a focal power or go-between to approve exchanges interminably.

The Threat Landscape in the Age of Artificial Intelligence * Security Issues * Cyberattacks Powered by AI: Cybercriminals are employing automated cyber attack algorithms as AI technology advances.

Security and Information Assurance Dangers: Artificial intelligence advances frequently depend on a lot of information to prepare and work on prescient models, raising worries about protection dangers and information breaks.

Machine Learning for Competition: AI includes controlling simulated intelligence frameworks by making unpretentious and designated changes to enter information or calculations that cause the simulated intelligence models to create bogus or destructive outcomes.

Weaknesses and dangers in IoT security

Lacking Confirmation and Approval: Numerous IoT gadgets need hearty confirmation instruments, depending on default passwords or powerless verification conventions.

Weaknesses in Outsider Parts: IoT biological systems frequently depend on outsider parts, libraries, and programming advancement packs (SDKs) that might contain security weaknesses or secondary passages.

Unreliable Organization Conventions and Connection points: IoT gadgets might utilize uncertain organization conventions and correspondence interfaces, like HTTP, Telnet, or FTP, which need encryption, validation, and respectability check systems.

The vulnerability of the blockchain to cyberattacks and its security in a proof-of-work (PoW) blockchain, a 51% assault happens when a solitary substance or gathering controls over half of the organization's hashing power.

Sybil Assault: To gain control of a significant portion of a blockchain network, a Sybil attack involves creating multiple fake identities or nodes.

Issues pertaining to intellectual property; Implications for copyright laws; Authorship and Ownership: The subject of origin and responsibility for produced content is complicated and frequently relies upon the imaginative commitments and human contribution in the substance creation process.

Creativity and Originality: Intellectual property regulation safeguards unique works of initiation that display an insignificant degree of innovativeness and creativity.

Subordinate Works and Extraordinary Use: Simulated intelligence created content might be viewed as subsidiary works or extraordinary utilization of existing protected materials, contingent upon the degree of change, transformation, or recombination of prior works.

IoT and the insurance of licensed innovation freedoms Implanted Programming and Firmware: Numerous IoT gadgets depend on installed programming or firmware to work, which might contain exclusive calculations, code, and proprietary advantages.

Licenses for IoT Developments: IoT advancements frequently include imaginative equipment, sensors, correspondence conventions, and information handling calculations that might be qualified for patent insurance.

Protecting IP Rights: Implementing protected innovation privileges in the IoT biological system requires carefulness, perseverance, and proactive measures to screen, distinguish, and hinder IP encroachment, duplicating, and unapproved utilization of exclusive advancements. Utilizing lawful cures, authorization activities, and IP implementation systems, for example, orders to shut everything down, directives, and suit, can assist with safeguarding IP

privileges and protect the worth of licensed innovation resources in the IoT commercial center
Blockchain's effect on advanced freedoms the executives and licensed innovation

Brilliant Agreements for Permitting and Sovereignties: Shrewd agreements, self-executing arrangements coded on blockchain stages like Ethereum, empower computerized, straightforward, and enforceable permitting and sovereignty installments for advanced content.

Distribution of content decentralized: Peer-to-peer content distribution bypasses centralized intermediaries and channels of distribution thanks to blockchain-powered platforms and decentralized file storage networks.

Cross-border data flows and conflicts between jurisdictions * Jurisdictional Complexity * Data Sovereignty and Localization Requirements: Numerous nations have executed information sway regulations and limitation prerequisites that order the capacity, handling, and move of information inside public lines.

Extraterritorial Use of Regulations: Jurisdictional struggles emerge when laws of one nation try to control the direct of people, associations, or stages working in another nation's purview.

Administrative difficulties in overseeing decentralized advances
Jurisdictional Equivocalness: Decentralized innovations work across public lines, making it challenging to figure out which ward's regulations and guidelines apply.

Conformity to Regulation: Decentralized advancements might present provokes for administrative consistence because of the absence of mediators answerable for carrying out and upholding administrative prerequisites.

International Treaties and Agreements: * Legal frameworks for resolving jurisdictional disputes in cyberspace Global deals and arrangements give a system to participation among countries in tending to jurisdictional questions, cybercrimes, and transnational legitimate issues.

Principles of Jurisdiction: Jurisdictional standards decide the legitimate power of courts and states to manage and arbitrate debates emerging from advanced exercises led inside their regional lines or influencing their residents.

Risk-Based Regulation: An Examination of Current Approaches to Emerging Technologies and Regulatory Responses Numerous administrative systems embrace a gamble based way to deal with survey and deal with the expected dangers and advantages related with arising innovations.

Area Explicit Guideline: Industry-specific considerations, market dynamics, and regulatory priorities all play a role in the wide range of regulatory approaches to emerging technologies that exist across various domains and sectors of the economy.

Need for versatile and innovation impartial administrative structures
Fast Mechanical Development: Innovation is developing at an exceptional speed, presenting new advancements, interruptions, and difficulties across different areas.

Advancement of Development: Innovation impartial administrative systems cultivate development by keeping away from prescriptive guidelines that favor explicit advances or plans of action over others.
Significance of worldwide participation in tending to worldwide digital regulation difficulties

Cross-Line Nature of Digital Dangers: Digital dangers, like cybercrime, digital secret activities, and digital psychological oppression, rise above public boundaries and purviews, making them hard to address through one-sided or disengaged measures.

Limit Building and Specialized Help: Numerous nations, especially agricultural countries, miss the mark on specialized aptitude, institutional limit, and assets to really battle digital dangers and authorize digital regulations.

Relevant Provisions
Under Indian laws, the crimes that are related to social media are governed under the Information Technology Act, 2000 and the Indian Penal Code, 1860, the relevant provisions dealing with such crimes are:

- Section 499 of IPC deals with defamation It refers to the act of making false statements or spreading misleading information about an individual or an entity through various online platforms. These statements can harm a person's reputation, causing damage to their personal or professional standing. Most common forms of defamation on social media include false accusations, misleading posts, or the sharing of damaging content with the intent to tarnish someone's character.
- Section 354D of IPC deals with 'stalking'. Stalking was added to the IPC by the Criminal Amendment Act, of 2013, after the Delhi gang rape case of 2012. The definition under this Section takes into consideration both types of stalking whether Physical or Cyber.
- Section 507 of the IPC deals with the crime of "criminal intimidation through anonymous communications." This provision specifies that if the stalker tries to conceal his identity and that the victim continues to remain unaware of the source from which he generates it is considered to be an offence.
- Section 67B under the Information Technology Act, 2000 inserted by the Amendment Act of 2008. This section focuses on the crimes in which the stalker attacks children who are under the age of 18 and uploads content that is related to children involved in intimate activities to intimidate the children. 4 https://www.freelaw.in/legalarticles/Social-Media-Laws-and-its-Implications
- Section 66E of the Information Technology Act, 2000 and Section 354C under the Indian Penal Code address "voyeurism" It can be defined as the act of intentionally capturing, publishing, or transmitting images of the private area of an individual without their consent which leads to violation of the privacy of that person.

- Section 292 of the IPC and Section 67 of the Information Technology Act, 2000 describes and deals with the term 'obscenity'. Obscenity involves the act of sharing inappropriate/vulgar content with the victim via social media networks, e-mails, text messages, etc.

Case laws

1. Shreya Singhal v. UOI

In the instant case, the validity of Section 66A of the IT Act was challenged before the Supreme Court.

Facts: Two women were arrested under Section 66A of the IT Act after they posted allegedly offensive and objectionable comments on Facebook concerning the complete shutdown of Mumbai after the demise of a political leader. Section 66A of the IT Act provides punishment if any person using a computer resource or communication, such information which is offensive, false, or causes annoyance, inconvenience, danger, insult, hatred, injury, or ill will.

The women, in response to the arrest, filed a petition challenging the constitutionality of Section 66A of the IT Act on the ground that it is violative of the freedom of speech and expression.

Decision: The Supreme Court based its decision on three concepts namely: discussion, advocacy, and incitement. It observed that mere discussion or even advocacy of a cause, no matter how unpopular, is at the heart of the freedom of speech and expression. It was found that Section 66A was capable of restricting all forms of communication and it contained no distinction between mere advocacy or discussion on a particular cause which is offensive to some and incitement by such words leading to a causal connection to public disorder, security, health, and so on.

2. Shamsher Singh Verma v. State of Haryana

In this case, the accused preferred an appeal before the Supreme Court after the High Court rejected the application of the accused to exhibit the Compact Disc filed in defence and to get it proved from the Forensic Science Laboratory.

Decision the Supreme Court held that a Compact Disc is also a document. It further observed that it is not necessary to obtain admission or denial concerning a document under Section 294 (1) of CrPC personally from the accused, the complainant, or the witness.

3. Shankar v. State Rep

Facts: The petitioner approached the Court under Section 482, CrPC to quash the charge sheet filed against him. The petitioner secured unauthorized access to the protected system of the Legal Advisor of Directorate of Vigilance and Anti-Corruption (DVAC) and was charged under Sections 66, 70, and 72 of the IT Act.

Decision: The Court observed that the charge sheet filed against the petitioner cannot be quashed with respect to the law concerning non-granting of sanction of prosecution under Section 72 of the IT Act.

Illustrations learned and suggestions for future administrative undertakings

Need for Clear Administrative Systems: Lawful cases have featured the significance of clear and cognizant administrative systems to address arising difficulties and alleviate gambles related with new advances

Security of Purchaser Freedoms and Protection: Legitimate cases including IoT and information security infringement highlight the significance of safeguarding shopper privileges, protection, and information security in associated gadgets and computerized administrations.

Future Bearings

Expected mechanical patterns and their lawful implications

Artificial intelligence (computer based intelligence):

Data Security and Privacy: The rising utilization of artificial intelligence calculations for information examination and dynamic raises worries about information protection, security, and assent. To guarantee accountability and fairness in AI systems, legal frameworks must address algorithmic transparency, data protection, and user rights. *

Liability and Accountability: As artificial intelligence innovations become more independent and refined, questions emerge about responsibility and responsibility for computer based intelligence related mishaps, blunders, and damages. Lawful structures might have to advance to characterize obligation principles, lay out legitimate liability, and assign risk among partners in computer based intelligence improvement, arrangement, and use.

Internet of Things (IoT)

Information Security and Protection: Concerns about data security, privacy breaches, and unauthorized access to sensitive information are raised by the proliferation of IoT devices.

Administrative Consistence and Guidelines: Interoperability standards, compliance mechanisms, and regulatory harmonization are all necessary for IoT ecosystems, which include a variety of technologies, protocols, and stakeholders. In order to guarantee the interoperability, dependability, and safety of IoT products and services, legal frameworks ought to establish industry standards, certification programs, and regulatory oversight.

Blockchain and Appropriated Record Innovation (DLT)

Administrative Consistence and Oversight: The decentralized and cross-line nature of blockchain innovation presents difficulties for administrative oversight, consistence requirement, and lawful purview.

Legal Validity and Smart Contracts: There are concerns regarding the legality, enforceability, and conformity of self-executing agreements, smart contracts, and decentralized autonomous organizations (DAOs). To accommodate blockchain-based transactions, legal frameworks must recognize smart contracts as legally binding instruments, establish rules for contract formation, interpretation, and dispute resolution, and adapt conventional legal concepts.

Proposals for policymakers, legitimate experts, and technologists

Advance Authoritative Dexterity: Cultivate official structures that are coordinated and adaptable enough to

adjust to quick mechanical progressions and developing digital dangers.

Advance Moral Legitimate Practice: Maintain moral guidelines, proficient trustworthiness, and regard for common liberties in legitimate practice, especially with regards to arising advances where lawful and moral contemplations meet.

Insert Security by Plan: Adopt the principles of security by design, privacy by design, and ethical design to incorporate security and privacy considerations into the initial design, development, and deployment of technologies. This will help to reduce the risks associated with cybersecurity and safeguard user privacy.
A focus on working together across disciplines to solve problems related to cyber law * Recognizing Complex

Legal and Technical Issues: Digital regulation difficulties frequently include complex lawful and specialized issues that require aptitude from different disciplines. Interdisciplinary joint effort empowers legitimate specialists, technologists, and topic experts to team up, trade information, and influence their mastery to break down, decipher, and address lawful and specialized parts of digital regulation difficulties all the more thoroughly.
Strategy Advancement and Administrative Structures: Creating viable approaches and administrative structures to address digital regulation difficulties requires interdisciplinary info and coordinated effort among policymakers, lawful specialists, industry partners, and scholarly analysts.

Conclusions

Innovative Headways Shape Lawful Scene: Blockchain, the Internet of Things (IoT), and artificial intelligence (AI) are just a few of the emerging technologies discussed in the research paper. These advances present novel lawful difficulties, valuable open doors, and intricacies that request creative administrative reactions and interdisciplinary cooperation.
Difficulties and Amazing open doors in Digital Regulation: The paper features the multi-layered moves presented by arising advancements to existing lawful structures, including protection concerns, security chances, jurisdictional ambiguities, and administrative holes. Be that as it may, it additionally accentuates the open doors introduced by these advances for upgrading computerized freedoms, working on administrative consistence, and cultivating development in the computerized economy.
Need for Versatile Legitimate Systems: A vital important point from the examination is the requirement for versatile and innovation nonpartisan legitimate systems that can stay up with fast mechanical headways and address developing digital regulation difficulties really. Policymakers, legitimate experts, and technologists should work cooperatively to foster nimble administrative methodologies that balance advancement, security, protection, and responsibility in the computerized age.
Significance of Worldwide Collaboration: The paper highlights the significance of worldwide participation in tending to worldwide digital regulation difficulties, advancing lawful harmonization, and encouraging cross-line coordinated effort among countries, associations, and partners. In the interconnected world of cyberspace, international cooperation strengthens global cybersecurity governance, enhances legal interoperability, and enables collective responses to cyber threats.
A Call to Action for Participants: All in all, the exploration paper gives a source of inspiration for policymakers, legitimate experts, technologists, and different partners to adjust to the developing scene of innovation and regulation, cultivate interdisciplinary cooperation, and advance capable advancement in the internet. By cooperating across disciplines, areas, and boundaries, partners can assemble stronger, comprehensive, and economical lawful structures that safeguard advanced privileges and advance the benefit of all in the computerized age.
The research paper emphasizes the significance of proactive measures, collaborative approaches, and ethical considerations in navigating the complex intersection of technology and law in the digital era. Additionally, it emphasizes the transformative potential of emerging technologies in shaping the future of cyber law.

Reference

1. https://www.techerati.com/features-hub/eight-cybersecurity-trends-to-navigate-in-2024
2. https://www.ibm.com/topics/blockchain
3. https://www.investopedia.com/terms/a/artificial-intelligence-ai.asp#:~:text=Artificial%20intelligence%20(AI)%20refers%20to,industries%20from%20finance%20to%20healthcare**.**
4. https://www.balbix.com/insights/addressing-iot-security-challenges/
5. www.forage.com
6. https://enhelion.com/blogs/2021/03/01/landmark-cyber-law-cases-in-india/
7. https://www.thelawwaywithlawyers.com/advancement-in-cyber-law-and-cyber-security-in-india/
8. https://www.brillopedia.net/post/emerging-trends-in-cyber-law-and-cyber-security-issues-and-challenges-in-the-digital-era