

AMOGHVARTA

ISSN : 2583-3189



Cybersecurity and its Role in Protection of IP and Data Privacy in the AI Era

ORIGINAL ARTICLE



Author

Vasudhi Mishra
Research Scholar
Department of Law
Bharti Vishwavidyalaya
Durg, Chhattisgarh, INDIA

Abstract

The rapid advancement of artificial intelligence (AI) and its integration into various sectors has brought forth immense opportunities as well as significant challenges, particularly in the realm of cybersecurity and intellectual property rights (IPR) protection. This paper delves into the intricate interplay between AI, cybersecurity, and IPR, exploring the emerging threats, challenges, and potential solutions. With the rise of AI-generated content and the increasing sophistication of generative AI models, issues related to authorship, ownership, and copyright infringement have come to the forefront. The paper examines the implications of data scraping practices employed by AI developers and the potential infringement of privacy rights and data misappropriation. It also addresses the unique concerns surrounding the protection of data generated by minors and the vulnerability of this demographic in the AI era. The paper further investigates the challenges posed by

the borderless nature of the internet and the difficulties in enforcing IPR across different jurisdictions. It explores the need for harmonization of international IPR laws and the potential of emerging technologies such as blockchain and smart contracts in streamlining rights management and compensation for creators. Additionally, the paper scrutinizes the existing cybersecurity regulations and their limitations in addressing the complexities introduced by AI systems. It draws insights from various international frameworks and initiatives, highlighting the need for a comprehensive AI governance framework that balances innovation, protection, and ethical considerations. By examining these critical issues, the paper aims to contribute to the ongoing discourse on cybersecurity and IPR in the AI era, providing valuable insights and recommendations for policymakers, industry stakeholders, and researchers alike.

Key Words

IPR, AI, Cybersecurity, Copyright, Trademark, Patent

Introduction

The rise of computers and the Internet has significantly increased the importance of intellectual property rights, particularly in e-commerce. However, this reliance on ICTs has led to difficulties in policing intellectual property violations in cyberspace. The challenge lies in protecting intellectual property online and preventing others from using it without permission. Cyberspace's anonymity and ease of access make intellectual property violations more common online than offline. Unauthorized use of trademarks, logos, graphic, audio, or literary works constitutes intellectual property infringement. New forms of infringement, such as deep hyperlinking, framing, meta-tags, spamming, and digital copyright infringement, have evolved.¹

Intellectual property protection is a global issue aimed at safeguarding the creative efforts of authors and recognizing their pioneering spirit. Due to the lack of oversight and legal constraints on the internet, treaties and conventions are necessary to harmonize global intellectual property laws. National laws have played a crucial role in strengthening intellectual property rights.²

The Agreement on “Trade-Related Aspects of Intellectual Property Rights (TRIPS), Convention for the Protection of Literary and Artistic Works (Bern), Hague Agreement for the Deposit of International Designs, Madrid Agreement for the International Registration of Trademarks, and the Patent Cooperation Treaty are internationally recognized treaties that protect intellectual property. The TRIPS Agreement, first created in 1994, requires member states to adhere to the most-favored-nation approach. However, the protection of intellectual property rights has not kept pace with national laws harmonisation and has not established standard protection criteria across different regimes. Articles 10 and 11 of the TRIPS Agreement address computer programs and data compilations, while Article 11 addresses writers’ rights to permit or prohibit commercially renting their intellectual works. Trademark law protects traditional brands, while copyright law provides extensive protection for sound recordings, literary themes, and cinematic works.³

The emergence of Cyber Law and Cyber Crime

The word ‘cyber’ has been around since at least 1984, when science fiction author William Gibson used it for the first time in his work ‘Mecomancer.’⁴ The author used the word to describe the virtual realm of computers. The idea of the internet was disconcerting for the legal profession since it allowed people to view the same website from different locations. The issue of the court’s jurisdiction has to be revisited. ‘Cyberlaw’ emerged to regulate the internet as its use became more widespread. The legal system is always attempting to keep up with the latest technological developments. While the widespread use of new technologies has presented unprecedented possibilities for human flourishing, it has also created fertile ground for all kinds of wrongdoing. Such dishonest behaviour consistently outpaces the mechanisms put in place by the authorities. Every aspect of modern life, from ideation to distribution to retrieval to storage, relies on computers.⁵ The internet has ushered in a new age of communication and is used extensively in both the private and public sectors. As a result, cybercrime will not only endanger the economic world but also undermine other community’s interests. Cybercrime, the commission of any criminal act via the use of a computer, has no universally accepted definition. Similarly, the term ‘cybersecurity’ lacks a universally accepted definition due to the complexity of the topic at hand; however, it can be summed up as follows: ‘It is a body of technologies, processes, and practises which is designed to protect computer, network, programme, and data from unauthorised access, disclosure, modification, damage, and attack.’ It refers to the safety of the building itself and the data contained inside it. Cyber security is defined similarly in the Information Technology Act of 2000: ‘the safeguarding from unauthorised use, access, modification, disclosure, or destruction of information, equipment, computer, computer resources, devices, communication device, and information stored therein.’⁶

Use of Artificial Intelligence in Cyber Crimes

Cybercrime continues to thrive despite efforts to prevent it. Technological advancements have led to the development of instantaneous global communication, self-driving cars, and the internet. Advances in AI, such as facial recognition technology in the criminal justice system, drones, and lethal autonomous weapon systems, can be used in disruptive ways that violate people’s rights and freedoms if not managed with appropriate oversight. Medium and small-scale organizations face challenges in equipping themselves to increase their cybersecurity capabilities due to high prices and limited budgets. Despite the potential for AI and ML to react more effectively to threats, the deployment of various defenses highlights the need for cyberspace authorities to adopt rigorous rules to control cybercrime and improve the administration of justice for victims. Regulation of cybercrimes is crucial in the age of information technology, and cyber legislation must be tightened to deal with cyber terrorism and hackers.⁷

Since COVID-19, the use of AI-based technology has surged globally, leading to increased crimes targeting foreign organizations, health sector businesses, and supply chain personnel. Cybercriminals have found a new tool to carry out illegal activities and launch attacks against Government institutions, private businesses, and people. They have discovered the dangers and disruptive potential of AI and ML in criminal and anarchist

contexts. Currently, 10 organized criminal gangs were hiring skilled hackers to infiltrate attacks and engage in illicit activities worldwide.⁸

Navigating Intellectual Property Rights in Cyber-space: Challenges, Enforcement and Emerging Technologies

Violation of Trademarks in Cyberspace

Section 2(zb) of the Trademark Act, 1999 defines a trademark as a visually presented mark that makes products or services easily identifiable and distinguishable. Its primary purpose is to increase value, maintain brand awareness, and provide a unique selling point. A trademark allows customers, clients, partners, and business owners to communicate, find, and purchase associated goods and services. A domain is an Internet Service Provider (ISP), similar to a street address for a website. It is a series of numbers that can be entered into a computer browser, similar to a phone number. With the internet and letter-number tracking system, accessing websites has become easier, with domains enabling universal access to the web's content.⁹ The Trademark laws aimed to protect and prevent counterfeiting of goods and services. However, trademark holders often acquire domain names that are confusingly close to their trademarks due to ICANN's first-come, first-served system. This can lead to the creation of domain names with trademark information without the owner's authority. Cybersquatting occurs when domain names are identical to genuine trademarks, posing a risk to the trademark holder's reputation. Reverse domain name hijacking occurs when domain holder relinquishes control due to fear of costly litigation. Large corporations and organizations often engage in reverse cybersquatting, while smaller businesses and individuals are victims. Meta tags, originally designed to help search engines classify websites, are now being used to manipulate search engine results and steal the goodwill of legitimate businesses.

Copyright Infringement

Copyright infringements are prosecuted in India under section 63 of the Copyright Act, 1957. The Napster Case is one of the most well-known instances of violations of digital copyright. In this case, the defendants sued the plaintiff for P2P file sharing, and the plaintiff eventually lost the case. Thanks to the software that Napster has made available to its users, those users are now able to exchange songs and other types of media files (such as MP3s) that are saved on their personal computers with other users of Napster. Since the lawsuit was first filed, the music firms have been demanding a payment of one million United States dollars for every copyrighted song downloaded over Napster. In the year 2000, the parties reached an agreement that resulted in the dissolution of Napster Inc. As part of the settlement, Napster agreed to pay the parties involved one-third of any future earnings.¹⁰

Software is likewise protected under copyright legislation.¹¹ The Copyright Act of 1957 defines computer programs, tables, and compilations as 'literary works,' including computer databases. However, the security of business methods remains uncertain. The 21st century, with the internet and the world wide web, has made access to information easier, posing new problems for copyright enforcement online. Intellectual property rights are increasingly important in the fast-paced media, communications, and technology industries. The scale and variety of IPR violations are expanding with network and internet technologies. Resolving copyright concerns is not a viable choice as the internet is essential to modern life. Copyright holders have instituted technological protections like the Electronic Copyright Management System (ECMS) to prevent unauthorized duplication and distribution.¹²

Patent Infringement

Infringing on a patent occurs when someone acts illegally concerning a patented invention without the permission of the patent holder. A licence is the standard form of authorization. While the precise elements of patent infringement vary from country to country, it often requires making commercial use of the protected technology. The patent law protects the original work of the writers and their innovations, which have an impact on computers and are thus subject to cyber law. Penalties for infringing on the patents of others were established by the Patent Act of 1970.¹³ It makes this behaviour illegal and specifies a maximum sentence of two years in prison. Infringement of intellectual property rights confidentiality requirements is likewise punishable under Section 118. Individuals who make an unwarranted patent claim are subject to a fine of one hundred thousand rupees under Section 120 of the Patent Law Act.¹⁴

It is common knowledge that every computer-related invention that has any kind of useful function is patentable. While software innovations are often not protected by patent law, medical equipment such as pacemakers are. Only when computer software significantly advances an art form can it be patented. A patent for the same software may be obtained if it improves the speed and efficiency of the original. A few software patents are as follows:

- Program algorithms.
- Program language translations.
- Menu arrangements.
- OS functions.
- Editing functions and interface features.
- Display presentations.

The Indian Patent Law does not have a clause addressing software protection, unlike the US, where online stock trading, gambling, and e-commerce are protected. The Indian Patent Office does not adhere to any standards regarding software, and a patent may be issued even if the software has a novel or useful purpose. If a patent owner engages in patent abuse, they are breaking the law and potentially misuse the monopoly power. Any patent that has been shown to be abused is null and void. Patent abuse occurs when a patent owner violates antitrust laws or inappropriately broadens the scope of the patent to benefit from it. Until parties can settle their differences, the patent should be rendered unenforceable. If the original owner seeks to profit from the invention through further licensing agreements, it is considered an abuse of the patent.

***Apple V. Samsung*¹⁵**

The patent infringement litigation between Apple and Samsung, which lasted seven years, involved Apple alleging that Samsung replicated its smartphone's features, including zooming in and out, and home screen design. The American legal system successfully settled the lawsuit, which had already been filed in over 50 jurisdictions worldwide. Apple warned Samsung in 2010 about developing software identical to its own, and the following year, it brought it to action. Samsung claimed Apple had stolen its patents, but the jury found in favor of Apple and ordered Samsung to pay almost \$1 billion. After a revised trial jury found both corporations were at fault for the same patent violation, the two sides settled out of court. The Supreme Court ultimately ruled against the petition in 2018, stating that the patent violation involved only a fraction of the device. Samsung was fined over \$540 billion for replicating Apple's features. Conventions like the Berne Convention, OECD Convention on Data Protection, and WIPO Performance and Phonograms pact have established rules to protect intellectual property rights, but current laws are insufficient to combat the exponential growth of cybercrime.¹⁶

Securing Tomorrow's Generative AI via IP Protection

Generative AI (GenAI) has the potential to create material that resembles human thinking through non-human intelligence. Software applications like OpenAI's ChatGPT/GPT-4 and Google's BARD were trained using extensive datasets and powerful computer resources. This has raised concerns about copyright infringement, privacy breaches, and potential instances of libel and defamation. The use of user-provided data, including data created by minors, to train software by firms raises concerns about copyright infringement and the vulnerability of young individuals. The extent to which corporations can claim the Copyright Act's 'fair use' exemption is also being scrutinized. This essay explores the implications of these cases in India, particularly in relation to the Digital Personal Data Protection Act of 2023.¹⁷

Data has become a valuable resource in the 21st century, comparable to oil. AI developers have been accused of unauthorized web scraping, collecting consumers' data without their knowledge. OpenAI is accused of collecting over 300 billion words from the internet, including personal information, to train its software. Courts have acknowledged data as a property in the US, leading to accusations of data misappropriation and theft. Even when sharing information online for public viewing, there is a justifiable expectation of safeguarding the confidentiality and integrity of the data. Therefore, data is considered a property in the US. The Supreme Court, in the case of *KS Puttaswamy v. Union of India*,¹⁸ acknowledged the right to privacy as an aspect of Article 21 of the Constitution. Unauthorized use of our data for AI software training without explicit authorization constitutes a breach of trust and an infringement on our privacy.

Furthermore, the data produced by children and their concerns around privacy are distinct and independent. They are more susceptible to abuse, prejudice, and exploitation. Regrettably, AI lacks adequate mechanisms to protect minors from accessing its online platform. The 'Children's Online Privacy Protection Act' (COPPA) in the US prohibits the monitoring, collection, or use of data from children without obtaining proper authorization from their parents or guardians. Regrettably, India lacks such regulations, relying only on self-reporting as the sole verification means, which proves ineffective.¹⁹

Furthermore, AI software has shown the capability to generate erroneous or imprecise paragraphs when prompted to reference a particular author's work, such as a poem. This erroneous outcome leads to the dissemination of incorrect information to the general public while also impeding the moral rights of writers by distorting their creations. The next part will explain how the courts are now dealing with these problems, guiding the future development of copyright law.²⁰

OpenAI asserts that the data provided for AI training and execution is protected under the fair-use exemption. Public reading or recitation of appropriate passages from a published literary or dramatic work in a digital setting, duplication of a work for research purposes, and other fair uses are all explicitly protected under Section 52 of India's Copyright Act, 1957. Similarly, the US Jurisprudence determines fair usage based on the following four factors:

Firstly, the aim and nature of the use, whether for commercial or educational purposes. In the case of *Campbell v. Acuff Rose Music*,²¹ the Court determined that the level of protection would be enhanced if the work was considered 'transformative,' meaning it exceeded the original production or introduced new elements rather than just being 'expressive.'

Secondly, the extent to which the fraction is utilized relates to the copyrighted work. OpenAI asserts that although the training material is not publicly disclosed, they do make the newly created content accessible based on that material. Consequently, they assert that the program is revolutionary.

Thirdly, the impact of the utilization on the pertinent market or the worth of the product inside the pertinent market. OpenAI asserts that by allowing robots to absorb the dataset without displaying it to people, the authors may avoid losing any possible audience. Nevertheless, the New York Times, among others, is contemplating legal action against OpenAI due to the AI technology significantly reducing the need to visit the publisher's website.

Fourthly, in addition, the decision also entails an examination of the inherent characteristics of the copyrighted work. In the case of *Andy Warhol v. Goldsmith*,²² the court determined that if the secondary work serves the same or very similar function and is utilized for commercial purposes, it becomes more difficult to argue for fair use unless there are strong justifications.

Emerging Technologies and Intellectual Property: Challenges and Opportunities

The integration of AI and Blockchain has significantly impacted intellectual property rights (IPR) landscapes. AI algorithms can generate creative works autonomously, raising questions about authorship and ownership. Blockchain, a decentralized and tamper-resistant ledger technology, offers transparent and secure ways to record and manage IP assets, reducing counterfeiting risk. Smart contracts automate IP transactions, ensuring fair compensation for creators and reducing intermediaries. The challenge lies in determining the extent to which AI systems should be recognized as inventors or creators. The constantly evolving content development environment presents both challenges and opportunities for IPRs. This study aims to investigate the significant difficulties and possible solutions associated with IPR in content development.

Challenges

- i. **The Rise of AI-Generated Content:** It is becoming increasingly difficult to differentiate between authorship and ownership as the level of sophistication of AI continues to increase. This is because AI gives machines the ability to develop material that is increasingly complex and original. It is difficult for legal frameworks to keep up with the rapid improvements in artificial intelligence, which has led to questions over the ownership of work generated by AI and the most efficient ways to protect it.

- ii. **Phantomization and Content Sharing:** Even though digital platforms make it easier to share content, they can sometimes make the problem of copyright infringement much worse. It can be challenging for creators to monitor and prevent the illegal use of their work, which can result in potential financial losses and a decrease in the value of their creations.²³
- iii. **Data Ownership and Privacy Concerns:** There have been new issues raised regarding privacy as a result of the collection and utilisation of personal data in the development of content. A substantial amount of deliberation is required to reach a harmonious equilibrium between the prerogatives of users to protect their privacy and the prerogatives of producers to utilise data for customisation and financial advantage.²⁴
- iv. **Borderless Infringement and Enforcement:** It is difficult to enforce IPRs due to the fact that different jurisdictions have varied legal systems and enforcement standards. This is because the internet is accessible all over the world. This creates opportunities for violations and hinders the ability of producers to protect their work on a worldwide scale. It also creates the possibility of violations.²⁵
- v. **Balancing Innovation and Protection:** When it comes to protecting existing content while also encouraging innovation, it is of the utmost importance to create a happy medium. A lack of suitable safeguards can deter innovators from investing in their original ideas, while too severe IPR systems have the potential to stifle innovation.²⁶

Opportunities

- i. **Collaborative Ownership Models:** The investigation of alternative ownership arrangements for content generated by AI should be carried out. These structures might potentially include authors, developers, and even the AI system itself. This may encourage cooperation and ensure that rights and advantages are distributed equitably.²⁷
- ii. **Leveraging Technology for Rights Management:** The utilisation of blockchain technology, in conjunction with other cutting-edge tools, can be utilised to automate the process of awarding licences, streamline the collection of royalties, and monitor the utilisation of material. The management of rights is simplified, and artists are given more control as a result.²⁸
- iii. **Data Governance Frameworks:** Through the implementation of data governance frameworks that are both explicit and easily understandable, it is possible to effectively handle privacy issues, which in turn enables producers to utilise data responsibly while also protecting user rights.²⁹
- iv. **Harmonization of International IPR Laws:** The effort to standardise IPR legislation on a global scale may result in the establishment of a more equitable competitive environment, the simplification of the enforcement of IPR across international borders, and the protection of creators all over the world.³⁰
- v. **Open Access and Fair Use Flexibilities:** By examining alternate licencing models such as open access and flexible fair use regulations, it is possible to achieve a balance between compensating creators and providing broader public access to knowledge and cultural expression.³¹

Cybersecurity regulation in the artificial intelligence (AI) ERA

Cybersecurity regulations in the AI era are of paramount importance as the integration of AI into various sectors continues to accelerate. The rapid advancements in AI technology have brought forth both immense opportunities and significant risks, necessitating a comprehensive regulatory framework to ensure its responsible and secure development and deployment.

In India, the existing legal framework for cybersecurity and data protection is primarily governed by the Information Technology Act, 2000 (IT Act), and the rules and regulations framed under it. However, the emergence of AI has exposed gaps and limitations in these laws, prompting the need for an updated and AI-specific regulatory regime.

One of the key challenges in regulating AI is the inherent complexity and opaqueness of AI systems, particularly those based on deep learning and neural networks. These systems can be vulnerable to adversarial attacks, data poisoning, and other forms of manipulation, posing significant cybersecurity risks. Ensuring the robustness, transparency, and accountability of AI systems is crucial to maintain public trust and mitigate potential harm.

The Indian Government has recognized the need for a comprehensive AI governance framework and has taken initial steps in this direction. The National Strategy for Artificial Intelligence, released in 2018, outlines the principles and approaches for the responsible development and deployment of AI in India. Additionally, the NITI Aayog has proposed the establishment of an AI-specific regulatory framework to address issues related to data governance, ethical considerations, and cybersecurity.

At the international level, various organizations and initiatives have been established to address the challenges posed by AI and cybersecurity. The European Union's General Data Protection Regulation (GDPR) and the proposed AI Regulation provide a robust framework for data protection and AI governance, emphasizing principles such as privacy by design, transparency, and accountability.

The Organisation for Economic Co-operation and Development (OECD) has also developed principles and guidelines for the responsible development and use of AI, including recommendations for enhancing cybersecurity and addressing potential risks associated with AI systems.

Furthermore, the United Nations (UN) has been actively involved in discussions and initiatives related to AI governance and cybersecurity. The UN's Centre for Artificial Intelligence and Robotics (UNICRI) has proposed a framework for AI governance, focusing on issues such as ethical considerations, data protection, and cybersecurity."

Lessons from Germany

In 2017, the Indian Supreme Court affirmed the intrinsic value of privacy as an essential facet of fundamental rights enshrined within the Indian constitution. Germany, in a pivotal moment in 1983, through its Federal Constitutional Court ("FCC"), delineated a more specific 'fundamental right to informational self-determination' in response to the burgeoning risks to privacy posed by advancing digitalization. Over two decades later, the FCC expanded upon this by articulating a fundamental right to confidentiality and the integrity of information technology ("IT") systems. Notably, in 2016, the FCC broadened its stance, asserting that the protection of IT systems encompasses networked computers (utilized by individuals) in conjunction with cloud storage (encompassing data hosted on external servers), and online tracking mechanisms. Consequently, the incorporation of Artificial Intelligence (AI) within such network frameworks could conceivably fall under the purview of this newly enunciated fundamental right. Should India witness a similar judicial evolution in the future, the trajectory and parameters of AI deployment may undergo significant transformation.³²

Lessons from the EU

AI-specific regulations, when enacted in isolation, might prove inadequate unless they are intricately entwined with the sector-specific environments in which AI operates. While India's forthcoming digital data legislation including the proposed Digital Personal Data Protection Act ("DPDP") and the DIA, respectively, may pertain to AI within the realm of digital data processing broadly, such statutes could also offer an initial blueprint for crafting robust safeguards within other regulatory frameworks.³³

For example, in Europe, Article 35(1) of the EU's General Data Protection Regulation ("GDPR") necessitates prior impact assessments in cases of high-risk processing, particularly where novel technologies are employed. Furthermore, GDPR's Article 35(3)(a) mandates such impact assessments when comprehensive evaluations of personal attributes pertaining to individuals are conducted through automated processing, including via profiling and decision-making technologies.³⁴

Similarly, Clause 11(2)(c) of the extant draft of India's DPDP (pertaining to additional obligations of 'significant data fiduciaries') also mandates impact assessments and periodic audits to be conducted by specific classes of notified entities handling substantial volumes of sensitive data – especially in instances involving risks to individual welfare, public interest, or national security.

Additionally, GDPR advocates for the prospect of 'regulated self-regulation'. It encourages associations or other entities to devise codes of conduct aimed at ensuring effective implementation of GDPR (Recitals 77 and 98). Such codes could encompass guidelines concerning the use of AI as well, at least to the extent that personal data protection legislation (like GDPR) applies to it. Moreover, GDPR's Article 41 allows for accreditation by competent bodies to monitor compliance with such codes of conduct. EU member states are also encouraged to establish certification mechanisms and data protection seals and marks (Article 42). Analogous legal mechanisms may be developed outside GDPR as well.³⁵

Although certification by publicly-accredited or Governmental bodies, particularly concerning high-risk AI developments and/or deployments, may be contemplated, incentivizing enforcement – such as by exempting or limiting liability, e.g., in the realm of robotics under product liability law – could prove beneficial. In sensitive arenas, certification might even be made obligatory.

The integration of AI presents distinctive challenges necessitating meticulous governance. As AI systems become more sophisticated and autonomous, traditional apprehensions regarding accountability, bias, and potential threats to both individual rights and societal welfare may persist. Complex AI algorithms, often referred to as ‘black boxes’, may yield decisions that even their creators struggle to fully comprehend. Consequently, demands for transparency in AI decision-making algorithms might escalate in the forthcoming years.

Lessons from Japan

Countries adopting disparate approaches to regulating AI (in contrast to the EU) also offer valuable insights. For instance, instead of imposing binding regulations on AI systems, Japan concentrates on voluntary initiatives undertaken by corporations towards AI governance. Analogous to NITI Aayog’s Responsible AI Report, the AI Governance Report published by the Japanese Ministry of Economy, Trade, and Industry advocates for agile governance and non-binding guidance to support a responsible AI regime. This approach seeks to circumvent rigid legislation that might stifle innovation.

Japan’s dual-pronged strategy concerning AI governance encompasses a harmonious blend of regulation and encouragement. On one front, the nation has enacted and/or amended sector-specific statutes to regulate AI deployment across various industries. For instance, amendments to the Financial Instruments and Exchange Act, 2006 oversee algorithmic high-speed trading, while the Antimonopoly Act, 1947 now extends to concerns pertaining to unfair trade practices conducted via algorithms. Furthermore, the Act on the Protection of Personal Information, 2003 (“APPI”) recently introduced the notion of pseudonymized information to alleviate the burden of obligations concerning such data, thereby incentivizing businesses to ensure that input data utilized in AI systems is appropriately pseudonymized.³⁶

Conversely, Japan has also embarked on regulatory reforms across sectors to promote AI utilization. For instance, amendments to the Road Traffic Act, 1960, and Road Transport Vehicle Act, 1951 empower manufacturers to develop self-driving vehicles. Similarly, revisions to the Installment Sales Act, 1961 enable credit card companies to leverage AI for determining user credit ratings. Moreover, recent modifications to the Copyright Act, 1970 endorse the use of data in Machine Learning (ML), while analogous amendments to the Unfair Competition Prevention Act, 1934 safeguard artists and creators by ensuring equitable compensation for underlying datasets sold to developers.

Conclusion

The rapid incorporation of artificial intelligence into several industries has initiated a new age of unparalleled possibilities and complexities. With the increasing sophistication and autonomy of AI systems, there is a growing need to implement strong cybersecurity safeguards and intellectual property protection. This study has examined the complex relationship between artificial intelligence (AI), cybersecurity, and intellectual property rights (IPR), emphasising the rising risks, difficulties, and possible remedies.

A significant obstacle is effectively managing the intricacies of copyright and authorship rights in AI-generated work. The increasing complexity of generative AI models has made it difficult to distinguish between human and machine innovation, leading to issues over copyright violation and unauthorised use of data. The article has emphasised the significance of achieving a careful equilibrium between safeguarding current intellectual property rights and promoting innovation in the field of artificial intelligence.

Moreover, the research has illuminated the distinct issues related to safeguarding data produced by individuals under the age of 18 and the susceptibilities this group encounters in the era of artificial intelligence. Given the ongoing development of AI systems, it is imperative to establish strong protective measures and regulatory structures to guarantee the privacy and well-being of children, who are particularly vulnerable to exploitation and danger.

The absence of borders on the internet and the differences in how laws are enforced in different countries have presented substantial difficulties in maintaining the protection of intellectual property rights. The paper emphasises the need of aligning international intellectual property rights (IPR) regulations and explores the possibilities of new technologies, such as blockchain and smart contracts, in simplifying rights administration and guaranteeing equitable remuneration for authors.

In addition, the report has thoroughly examined the current cybersecurity legislation and their shortcomings in dealing with the intricacies brought about by AI systems. The study highlights the need of developing a comprehensive AI governance framework that takes into account international frameworks and efforts. This framework should strike a balance between promoting innovation, ensuring protection, and addressing ethical concerns.

In order to tackle the complex difficulties arising from the integration of AI, it is crucial for Governments, industry stakeholders, and researchers to work together. This paper is a plea for taking immediate action and adopting a proactive stance towards cybersecurity and intellectual property rights in the age of artificial intelligence.

To fully use the transformational power of AI while minimising its hazards, we must create a supportive atmosphere that promotes responsible innovation, protects intellectual property rights, and ensures data privacy. Continuous communication, cooperation across many sectors, and a dedication to ethical standards are crucial for guaranteeing a future in which AI and human creativity may coexist in a balanced manner, promoting advancement while upholding the basic rights and values that form the foundation of our society.

Reference

1. All You Need to Know About Intellectual Property Rights in The Digital World, *All You Need To Know About Intellectual Property Rights In The Digital World*, June 3, 2020, <https://iptse.com/intellectual-property-in-cyberspace/>, Accessed on 01/11/2025.
2. Keerthana16n, "Patent Misuse in Cyber Space, *Legal Desire*, August 8, 2020, <https://legaldesire.com/patent-misuse-in-cyber-space/>, Accessed on 01/11/2025.
3. *Ibid*.
4. Cyber Crimes against Society & Government, <https://www.lawyered.in/legal-disrupt/articles/cybercrime/>, Accessed on 01/11/2025.
5. Rahaman, M. A., Cybercrime affects society in different ways. The Financial Express. <https://thefinancialexpress.com.bd/views/reviews/cyber-crime-affects-society-in-different-ways/>, Accessed on 11/04/2023.
6. Twitter account of India's top UN diplomat hacked, The Times of India- <https://timesofindia.indiatimes.com/india/twitter-account-of-indias-top-un-diplomat-hacked-restored/articleshow/62494760.cms/>, Accessed on 01/11/2025.
7. Gorman C. (2022) Recent Developments in AI and National Security: What You Need to Know, Lawfare, Washington, D.C., 3 March 2022.
8. Yampolskiy, Roman V., and Spellchecker, M. S. (2016) Artificial intelligence safety and cybersecurity: A timeline of AI failures. *arXiv preprint arXiv:1610.07997*, Cornell University, arXiv.org, Ithaca, NY. <https://doi.org/10.48550/arXiv.1610.07997>, Accessed on 12/11/2025.
9. *Ibid*
10. IPLF, Scrutinizing the Nuances of the Napster Case - IPLF (IPLF, September 29, 2021), <https://www.ipandlegalfilings.com/scrutinizing-the-nuances-of-the-napster-case/>, Accessed on 01/11/2025.
11. Somu, C. S. (2006) Intellectual Property Rights In Cyberspace. *Paradigm*, 10(1), 62–68.
12. *Ibid*
13. Zaidi K, (2022) IPR Issues In Cyberspace (*IP Bulletin*, February 8, 2022), <https://ipbulletin.in/ipr-issues-cyberspace/>, Accessed on 01/11/2025.

14. *Ibid*
15. Apple Inc. v. Samsung Elecs. Co. - 786 F.3d 983 (Fed. Cir. 2015)
16. Zaidi K, IPR Issues In Cyberspace (*IP Bulletin*, February 8, 2022) <https://ipbulletin.in/ipr-issues-cyberspace/>, Accessed on 01/11/2025.
17. Nishith Desai Associates, "Emerging Legal Issues with use of Generative AI, <https://www.nishithdesai.com/NewsDetails/10818>, Accessed on 01/11/2025.
18. AIR 2017 SC 4161
19. Lindberg, V. (2022) Building and Using Generative Models under US Copyright Law. *Rutgers Bus. LJ*, 18, .1.
20. *Generative AI, data minimization, and the gold rush of the early 2020s*, <https://www.jdsupra.com/legalnews/generative-artificial-intelligence-data-4578397/>, Accessed on 01/11/2025.
21. 510 U.S. 569 (1994)
22. *Supreme Court of the United States*. https://www.supremecourt.gov/opinions/22pdf/21-869_87ad.pdf, Accessed on 01/11/2025.
23. Eaton, J. (2020) Trends in Advertising: How the Rise in Artificial Intelligence May Influence the Field of Content Strategy. Doctoral dissertation, East Tennessee State University, Johnson City, Tennessee.
24. Srinivas, S. & Liang, H. (2022) Being digital to being vulnerable: does digital transformation allure a data breach?. *Journal of Electronic Business & Digital Economics*, 1(1/2), 111-137.
25. Leong, S. H. & Saw, C. L. (2007) Copyright Infringement in a Borderless World—Does Territoriality Matter?. *International Journal of Law and Information Technology*, 15(1), 38-53.
26. Bhat, S. R. (2018) Innovation and intellectual property rights law—an overview of the Indian law. *IIMB Management Review*, 30(1), 51-61.
27. Matheson, Scott (2018) Access versus ownership: A changing model of intellectual property. Law library collection development in the digital age. Routledge, New York, NY, 153-176.
28. Bhat, S.R. (2018) Innovation and intellectual property rights law—an overview of the Indian law." *IIMB Management Review*, 30(1), 51-61.
29. Srinivas, S. & Liang, H. (2022) Being digital to being vulnerable: does digital transformation allure a data breach?. *Journal of Electronic Business & Digital Economics*, 1(1/2), 111-137.
30. Stack, A. J. (2011) *International patent law: cooperation, harmonization, and an institutional analysis of WIPO and the WTO*. Edward Elgar Publishing, Cheltenham, UK.
31. Elkin-Koren, N. & Fischman-Afori, O. (2017). "Rulifying fair use. *Ariz. L. Rev.*, 59, 161.
32. Kavyn, Sviatoslav; Ivan Bratsuk and Anatoliy Lytvynenko (2021) Regulatory and Legal Enforcement of Cyber Security in Countries of the European Union: The Experience of Germany and France. *Teisė* 121, 135-147.
33. Chander, Harish, and Gagandeep Kaur (2022) *Cyber laws and IT protection*. PHI Learning Pvt. Ltd., Delhi.
34. *ibid*
35. Kasper, Agnes and Alexander Antonov (2019) *Towards conceptualizing EU Cybersecurity Law*. , ZEI Discussion Paper C253/2019. Zentrum für Europäische Integrationsforschung, Rheinische Friedrich Wilhelms-Universität Bonn, Genscherallee Germany. ISBN 978-3-941928-96-1.
36. Katagiri, Nori (2021) From cyber denial to cyber punishment: What keeps Japanese warriors from active defense operations?. *Asian Security* 17,(3), 331-348.

====00====