Quest Journals
Journal of Research in Humanities and Social Science
Volume 12 ~ Issue 10 (2024) pp: 71-74
ISSN(Online):2321-9467
www.questjournals.org

Research Paper

A Critical Analysis of the Safeguarding Of Intellectual Property Rights in India Through Cybercrime

Mr. Md Jiyauddin[1]
Dr. Sunita Banerjee[2]
[1,2]*Assistant Professor, Department of Law, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Tamil Nadu, India*

ABSTRACT: *This study explores the relationship between cybersecurity and intellectual property rights (IPR) in the context of India. Intellectual property security is becoming more and more important as a result of the sectors' rapid digitisation and businesses' rising reliance on digital platforms. But the digital world also brings with it new risks and difficulties, therefore strong cybersecurity defences are needed to protect intellectual property. This study looks at the state of IPR and cybersecurity in India today, highlights major issues, looks at current cybersecurity efforts and legislative frameworks, and suggests ways to improve IP protection online.*
The protection of genuine works in a variety of media, including audio and video files, writing, photography, paintings, and literature, is the focus of intellectual property rights. IPR protects the aforementioned works in both tangible and intangible ways. IPR encompasses trademarks, copyrights, geographical indications, industrial designs, and so on. The original inventor has access to a number of legal remedies against any internet infringements, sometimes known as cybercrimes. Cybercrimes are on the rise every day and include infringement of intellectual property rights as well as cyberstalking, cyberbullying, spamming, and phishing. Every online work is susceptible to attacks. Cyberspace has made it easier to do business, connect with friends and family, share information, and publish literary works, but it has also made patented works more vulnerable to cyberattacks.
KEYWORDS: *Digitisation, Businesses, Digital Platforms, Cybersecurity and Legal remedies.*

R*eceived 04 Oct., 2024;* ***R****evised 14 Oct., 2024;* ***A****ccepted 16 Oct., 2024 © The author(s) 2024.*
P*ublished with open access at* ***www.questjournas.org***

I. INTRODUCTION

It's said that the 21st century is a century of science and technology. This century has seen a fast improvement in both science and technology. Law and jurisprudence are impacted by evolving technology in both direct and indirect ways. If the law doesn't adapt to the rapid advancements in science and technology, it will eventually become outdated. In the internet age, intellectual property rights infringement is a widespread occurrence. The possibilities of cyberspace have expanded due to advancements in science and technology as well as the growing need for information access. Anybody can infringe against the intellectual property rights or other rights of anybody living anywhere in the world by working or sitting in a remote area of the globe. Although the internet has given humanity many benefits, it has also turned into a place where people engage in a variety of illegal acts. Due to its border lessness, the cyberspace has created a number of legal and jurisprudential issues as well as difficulties for the creation, application, and interpretation of laws. A multitude of domestic laws have been passed by different sovereign nations in response to the evolving needs of the internet. A number of international conventions have also been passed on intellectual property rights and cyberspace. Concurrently, several global organisations are striving to address the obstacles presented by cybercrimes and intellectual property rights transgressions. State-level domestic courts have been addressing the issues raised by the internet, but their conclusions have been contradictory.

II. RESEARCH METHODOLOGY

The Doctrinal Research Methodology, sometimes referred to as library-based research, has been used by the researcher. Using the critique and analysis of other jurists, authors, or writers, this research approach is used to evaluate or analyse laws, rules, regulations, judicial declarations, legal doctrines, and principles.

III. OBJECTIVES

- To analysis Intellectual Property Rights and Cyber Crime in India.
- To discuss relationship between Intellectual Property Rights and Cyber Security.
- To analysis Indian perspective on Cyberspace Jurisdiction.

IV. RESEARCH'S SCOPE AND LIMITATIONS

The study's focus is limited to issues related to jurisdiction, challenges facing India's adversarial criminal justice system, and copyright infringement and linking. The jurisdictional issue is restricted to Indian criminal laws, case laws, and guiding principles. The issues that confront an adversarial criminal justice system are limited to those that arise when it interacts and collaborates with nations that have an inquisitorial criminal justice system. The researcher has not taken into account linking and trademark infringement or violations of tort law; the issue raised by linking is restricted to copyright infringements exclusively.

V. CYBERCRIME AND INTELLECTUAL PROPERTY RIGHTS IN INDIA

Cybercrimes can be generically categorised as offences against "person, property, or government." The "Byzantine Empire," where monopolies over "recipes" were established, is where the idea of intellectual property originated. In a paper published by the World Intellectual Property Organisation (WIPO), it was said that intellectual property rights indicate that human history is the history of applying imagination, or invention and creativity, to an existing body of knowledge in order to solve issues. Innovation in the arts and sciences is fueled by imagination. The word intellectual property (IP) refers to concepts, technology, works of art, music, and literature that are initially ethereal but gain value when produced in concrete form. It is reasonable to state that intellectual property (IP) is the commercial use of creative ideation to overcome creative or technological obstacles. It is not the product per se, but rather the unique concept that underpins it, the manner in which it is articulated, and the unique method it is labelled and explained. The term property is used to characterised its significance since it solely refers to creations, works, and names that an individual or group of individuals claims ownership over. Ownership is significant since past performance has demonstrated that the possibility of financial benefit serves as a strong motivator for innovation. The underlying tenet of intellectual property rights is that no one should be able to monopolies on information, communication, ideas, or factual building blocks. The internet of modern civilisation makes knowledge sharing public, which poses security risks and jeopardises intellectual property rights. One major problem with virtual workplaces, which are readily entwined by internet access, is intellectual property rights violations.

VI. CONVENTIONAL WISDOM AND ITS RELEVANCE TO CYBERSP

The issue of jurisdiction in cyberspace cannot be solved by applying conventional legal rules. The idea of territorial sovereignty is taken into consideration while developing the conventional theories and precepts of international law concerning jurisdiction. Since the online is de-territorial and global, anybody can commit a crime there from anywhere. The crime may be committed simultaneously against several different nations. Therefore, it is not possible to effectively address the issue of jurisdiction in cyberspace using the geographical principle, nationality principle, effect doctrine, protective or security jurisdiction, or universal jurisdiction. Because actions in online are not subject to territorial constraints, the territorial principle cannot be a comprehensive approach to deal with copyright infringement in cyberspace. The territorial principle states that any activity taking place on a sovereign state's territory should be governed by the law. The violation of copyright in internet transcends national borders. Furthermore, if victims are from different nations, this approach cannot be applied to compensate them. Therefore, the geographical theory on jurisdiction cannot be a full answer to overcome the problem of various jurisdictions in cyberspace. The issue of jurisdiction in cyberspace cannot be fully resolved by the nationality concept, which includes both passive and active nationality principles. A nation may utilise the notion of nationality to reward or punish its citizens. The issue of various jurisdictions in cyberspace cannot be effectively resolved by the nationality concept. Additionally, it cannot be utilised to pay damages to victims of online copyright infringement who are from other countries.

If the violation is committed against a single nation, the "effect doctrine" may be employed as a strategy to address the jurisdictional issue in cyberspace. It is ineffective as a remedy to the jurisdictional issue in cases of copyright infringement against several nations. There is no system in place to compensate the victims of several nations, or the offender cannot be held accountable and punished in accordance with the "effect doctrine" by various countries. Only in very few circumstances may protective or security jurisdiction be beneficial. It is not possible to assert the protective or security jurisdiction over every common offence. It may be asserted in situations where actions taken overseas jeopardies the safety, integrity, or appropriate operation of the sovereign state. The protective or security jurisdiction may be invoked in cases of assault on the vital infrastructure or websites of the sovereign state, including attacks on the websites of the armed forces or military. This means that

under the security or protection principles of international law, sovereign governments cannot assert jurisdiction over cases of online copyright infringement.

VII. RELATIONSHIP BETWEEN CYBER SECURITY AND IPR

The digitalisation has created a number of connections between cyber security regulations and intellectual property rights. The following examples show how cybersecurity and IPR law are related:

1. **To Preserve Private Information**: Businesses, as well as people, produce and keep a great deal of sensitive data in this digital age, including trade secrets, patents, copyrights, and other intellectual property. Protecting this data from theft, unauthorised access, and data breaches requires cybersecurity.

2. To Prevent Cyber Theft and Infringement: Intellectual property, such as research data, designs, or proprietary software, can be stolen as a result of cyberattacks. IPR law is involved in the prosecution of cyberthieves and the imposition of legal repercussions for their acts.

3. Regarding Data Protection and Privacy: Intellectual property may contain sensitive personal information about a person. Cybersecurity safeguards aid in preventing data breaches and guaranteeing adherence to data protection regulations. Maintaining privacy cybersecurity procedures so becomes essential for businesses managing personal information and intellectual property.

4. To safeguard digital copyrights: Since digital replication is so simple, copyrighted work is increasingly being pirated and distributed without authorisation. By limiting illegal access and third-party dissemination of copyrighted content, cybersecurity measures can aid in the protection of digital copyrights.

5. Regarding Patent Protection: Patents may be available for cybersecurity innovations. Cybersecurity ideas and technologies are protected by intellectual property regulations, such as patent law, which incentivises innovators to continue developing their fields.

6. Trade Secrets Protection: Trade secrets are important intellectual property that must be protected, and cybersecurity is crucial for this. Trade secrets may be disclosed without authorisation as a result of cybersecurity breaches, which might seriously hurt organisations. IPR law provides legal recourse for trade secret protection and theft prosecution.

7. Regarding Digital Theft and Forgery: In order to combat digital piracy and counterfeiting, cybersecurity measures can assist prevent the unauthorised replication of intellectual property and the dissemination of digital information, including software, music, movies, and books.

VIII. INDIAN PERSPECTIVE ON CYBERSPACE JURISDICTION

A thorough examination of the jurisdictional clauses included in the Information Technology Act of 2000 and the Bharatiya Nyaya Sanhita 2023 reveals that Indian people are only partially relieved by these provisions. According to its terms, this Sanhita will apply to any crime committed by anybody anywhere in the world that targets a computer resource that is situated in India. The Information Technology Act, 2000 stipulates under section 75 that computer resources must be situated within Indian territory. The word 'involves' is used in section 75 of IT Act, 2000. It has a very wide interpretation. It could involve a foreign national committing a crime against another foreign national over a computer network situated within Indian territory. These kinds of cases involve the possibility that an Indian network may be used to perform a crime between two sovereign states. Neither Indian citizens nor territorial interests are at stake in the aforementioned situations. Consequently, the territorial sovereignty concept of international law is at odds with the kind of expansive language used in the statute.

It is important to notice that section 1 of the BNS, 2023 uses the term "targeting" in sub-section 5(c). The bill doesn't provide a definition or explanation for the term "targeting." "Aiming at" is what "targeting" means in the dictionary. Since the rule of rigorous interpretation applies to criminal law, it is necessary to emphasise the literal or dictionary meaning of terms employed in the legislation. The stringent interpretation rule requires that criminal legislation be interpreted strictly and literally. It is argued that, under the rigorous interpretation criterion, it is unclear if BNS would be used when:

a) A human is the aim or target, not a computer resource. It indicates that the goal is to harm the person via or with assistance from computer resources, such as by posting defamatory remarks, rather than to cause unlawful loss to computer resources, including computers or data per se. "Target" and "means" are not the same in this scenario. A human is the "target," while the computer resource is the "means." As a result, rather than intentionally targeting a computer resource, an offence is committed in the case above with its assistance.

b) Via a network based in India, a foreign national commits an offence against another foreign national from each country;

c) When data is duplicated from a computer outside of India's borders and made available to the whole globe, including India, unlawful loss is inflicted upon the individual.

d) A passive website, such as a photography website that is accessible in India, is registered and created outside of India. Similar to this, a website that contains content that is illegally protected by copyright may be accessed in India without specifically aiming at Indian computer resources. The objective in these instances is not the Indian

computing resources in and of themselves. The objective is to make it available to the entire planet. By the way, it will be available in India.

IX. LINKING IN RELATION TO ONLINE COPYRIGHT VIOLATIONS

According to the examination of hyperlinking and copyright infringement, connecting parties may be held directly liable for copyright infringement in cases of framing and inline linking under Indian copyright laws. With the exception of framing and inline linking, the linking parties are not liable for direct infringement in cases of deep linking. Furthermore, since maintaining a linked page online does not in and of itself constitute a copyright infringement, connecting parties are not liable for contributory infringement. Usually, the linked site is maintained by the author or someone who has been given permission by him. When the copyrighted resource is given by the author or with permission from the author, they (the connecting parties) are not liable for contributory responsibility. Generally speaking, copyright infringement cannot be held against internet users. Thus, the connected party cannot be held accountable for indirect infringement. The author currently suffers a wrongful loss as a result of deep linking, yet Indian copyright laws do not provide a legal recourse. Thus, via judicial interpretation, the judiciary might rule that framing and inline linking, at the very least, violate copyright under current Indian legislation. Apart from inline linking or framing, the current copyright regulations in India do not bolster the author's claim in cases of deep linking. Deep linking is not in line with the goals that the websites are trying to accomplish either. Because implicit limits or limitations apply, the implied authority claim is not persuasive. Accordingly, under Section 14 of the Indian Copyright Act, 1957, the framing, inline linking, and deep linking shall be deemed exclusive rights of the work's creator. In order to strike a balance between the interests of society and the writers of the copyrighted work, search engine linking must not be considered illegal. Without search engine linkage, at the very least, the internet cannot function efficiently. Thus, preventing search engines from connecting would be detrimental to the expansion of the internet and the interests of society as a whole.

X. CONCLUSION

The relationship between cybersecurity and intellectual property rights in India is thoroughly examined in this study paper. It looks at the difficulties right holders experience in the digital era and how technology might help to lessen those difficulties. This study intends to contribute to the protection of cybersecurity and intellectual property rights in India by making proposals for improving enforcement mechanisms, bolstering the legislative framework, and raising awareness and educating the public. To stop any unauthorised usage or system theft, there is an urgent need to educate Indian society on the need of copyright protection on all fronts. Cyberspace copyright analysis yields a mixed bag of new opportunities and dangers. Since these dangers frequently outweigh the advantages that the internet presents, further rules are required to safeguard copyrights. Additionally, the absence of globally recognised guidelines for copyrights in cyberspace allows for a great deal of variation in country laws. Thus, in order to further enhance Indian cyber laws pertaining to intellectual property rights, these factors should be kept in mind. There are other legal options open to IP rights holders for the resolution of issues outside resorting to legal action by filing a case with the court or another legitimate body. It is imperative that owners of patents, copyrights, trademarks, and other intellectual property take reasonable precautions to secure their creations and stay up to speed on the most recent technical advancements in IPR protection.

REFERENCES

[1] H. Rawat, (2023) Protection of IPR in Cyberspace. Retrieved September 25, 2024, from https://www.legalserviceindia.com/legal/article-13122-protection-of-ipr-in-cyberspace.html#:~:text=Section%2075%20IT%20Act%2C%202000,effective%20Jurisprudence%20and%20Judicial%20Activism

[2] J. P. Sanjay, (2023), Intellectual Property Rights and Cybersecurity in India: A Comprehensive Analysis. Retrieved September 23, 2024, from https://theamikusqriae.com/intellectual-property-rights-and-cybersecurity-in-india-a-comprehensive-analysis/

[3] Ashwin (2022). Role of Intellectual Property in Cyber Law. Retrieved September 26, 2024, from https://enhelion.com/blogs/2022/09/01/role-of-intellectual-property-in-cyber-law/

[4] T. Prateek, (2024). Intellectual property rights and cyber security in india. Retrieved September 29, 2024, from https://taxguru.in/corporate-law/intellectual-property-rights-cyber-security-india.html

[5] T. Khare, (2023). Intellectual Property Rights In The Cyber Space. Retrieved September 24, 2024, from https://www.legalserviceindia.com/legal/article-13557-intellectual-property-rights-in-the-cyber-space.html

[6] W. Sejal, (2024). Cybercrime Involving Intellectual Property Rights. Retrieved September 19, 2024, from https://juriscentre.com/2024/04/21/cybercrime-involving-intellectual-property-rights/

[7] B. Poorva, (2023). INTELLECTUAL PROPERTY RIGHTS AND CYBERSECURITY IN INDIA: COMPREHENSIVE ANALYSIS. 5(1), International Journal of Advanced Legal Research. Retrieved October 03, 2024, from https://ijalr.in/volume-4-issue-2/intellectual-property-rights-and-cybersecurity-in-india-comprehensive-analysis-poorva-bhawsar/

[8] B. Pawanpreet, (2023). THE FUTURE OF INTELLECTUAL PROPERTY RIGHTS IN THE AGE OF CYBER CRIME OPPORTUNITIES AND CHALLENGES. Retrieved September 20, 2024, from https://www.jusscriptumlaw.com/post/the-future-of-intellectual-property-rights-in-the-age-of-cyber-crime-opportunities-and-challenges

[9] A. Singhal, (2022). CRITICAL ANALYSIS OF INTELLECTUAL PROPERTY RIGHTS. 7 Indian Politics & Law Review Journal (IPLRJ).