INVISIBLE HEISTS: THE GROWING LINK BETWEEN CYBERCRIME AND INTELLECTUAL PROPERTY INFRINGEMENT

BY KASHIKA VERMA[1]

ABSTRACT

The rise of digital technology and internet has provided a new platform for innovation, ideas and growth but it has also led to an increase in cybercrime related to Intellectual property (IP). This article delves into how cyber threats like phishing, malware, social engineering and advanced persistent threat (APT) are being used to steal these intangible objects such as trademark, copyright, patents and trade secrets. These internet crimes are not restrained by geography and can be committed from anywhere in the world, making the enforcement of intellectual property rights more complex.

The article also addresses the gap in current Indian legal framework, especially in dealing with cross border cybercrimes. There are laws such as Information Technology Act,2000 and relevant provisions in Bharatiya Nyaya Sanhita and Indian Penal Code which tries to extend jurisdiction but ambiguous language and outdated approach makes its enforceability difficult. Indian courts have demonstrated initiative by implementing global legal standards such as the Minimum Contacts and Effects Test, however, there is still a deficiency in robust legislation and international collaboration.

India must update its law, increase its international cooperation and raise awareness about increasing cyberattacks to protect Intellectual property in the digital era. The article emphasizes the need for enhanced legal clarity, more stress on international agreements, and improved technological safeguards to tackle this escalating problem.

[1] The Author is a law student at the Institute of Law, Nirma University.

Keywords: Cybercrime, Intellectual Property, Phishing, Malware, Copyright Infringement, Trademark Violation, Jurisdiction, Indian Cyber Law, Cross Border Enforcement, Digital Theft.

1. Introduction

Cybercrime

With the growing era of technology and increasing dependence on it, the realm of threat in cybersecurity and cyberthreats is increasing. Number of cyberattacks worldwide increased by 30% in 2025. The cybersecurity market worldwide is predicted to reach $538.3 billion by the end of 2030. Over 2,200 cyber-attacks occur daily worldwide. 1,636 organizations faced cyber-attacks weekly.[2] Cyberattacks are flourishing because it is not restrained by geography unlike physical attack and require minimal resources. Many cybersecurity experts believe that malware is the key choice of weapon to carry out malicious intends to breach cybersecurity efforts in the cyberspace[3].Malware, or "malicious software," is an umbrella term that describes any malicious program or code that is harmful to systems. Hostile, intrusive, and intentionally nasty, malware seeks to invade, damage, or disable computers, computer systems, networks, tablets, and mobile devices, often by taking partial control over a device's operations.[4] Taking advantages of new Internet technologies with millions and billions active users, cyber criminals utilize these new technologies to reach out to a vast number of victims quickly and efficiently. After the growth of internet connectivity an increasing number of populations is now using the internet and exposing themselves to the threat of cyberthreats by giving personal information unknowingly. Number of steps should be taken to address the growing issue of cyberthreats such as Global-scale identity management and traceback techniques. Global-scale identity management concerns identifying and authenticating entities such as people, hardware devices, distributed sensors when accessing critical information technology systems from anywhere[5]. Special focus should be given on user privacy and there should be secure internet and connectivity.

---

[2] Naveen Kumar, 83 Cybersecurity Statistics (2025): Worldwide Data & Trends, DEMAND SAGE (Nov. 11, 2024), https://www.demandsage.com/cybersecurity-statistics/.
[3] House of Representatives Standing Comm. on Commc'ns, *Tackling the Problem of Cyber Crime*, Parliament of Austl. (Aug. 2004), http://www.aph.gov.au/house/committee/coms/cybercrime/report/full_report.pdf.
[4] Malwarebytes, *What is Malware? Malware Definition, Types and Protection*, Malwarebytes (2025), https://www.malwarebytes.com/malware.
[5] Shibboleth Consortium, *Shibboleth Project*, Internet2, http://shibboleth.internet2.edu/.

Intellectual Property

Intellectual property is a broad categorical description of a set of intangible assets that are owned by a company or individual. It is legally protected from outside use or implementation without consent. An intangible asset is a non-physical asset. The concept of intellectual property relates to the fact that certain products of human intellect should be afforded the same protective rights that apply to physical property, called tangible assets. Most developed economies have legal measures in place to protect both forms of property.[6] Companies are very stringent about protecting intellectual property as it requires high heavy investment in skilled labour and creativity. Intellectual property consists of many types of intangibles assets including patents, copyrights, trademark, franchises, trade secret, digital asset etc. Intellectual property rights give owners the ability to bar others from recreating, mimicking, and exploiting their work. Extracting value from intellectual property and preventing others from deriving value from it is an important responsibility of any company. It is an intangible asset but intellectual property can be far more valuable than a company's physical assets. It can represent a competitive advantage and is fiercely guarded and protected by the companies that own the property as a result.[7] There is a growing intersectionality between Cybercrime and Intellectual Property.

2. **Interconnection of Cybercrime and IPR-**

Modern web-based technology, smartphones, and the internet have improved our ability to conduct e-commerce, conduct financial transactions, and swiftly electronic commerce. The way that current businesses operate, including online advertising, online ordering, online shopping, online education, publishing, banking, entertainment, investment, auction, professional services, etc., has been altered by the new internet culture and cyberspace. The global reach of the internet gives intellectual property owners access to an infinite market. Since most trade and commercial organizations use the internet as a platform for commerce, there is a lot of pressure on businesses and individuals to preserve their intellectual property rights (IPR). Nowadays cybercrime is not limited to cyberattacking, hacking but is also extended to infringement of copyrights and trademarks of numerous companies which is a growing threat. But the same internet provides a platform to various criminals to commit cybercrime. The owners must be actively aware of the growing infringement of

[6] Investopedia, *Intellectual Property (IP): What It Is and Types*, Investopedia (2025), https://www.investopedia.com/terms/i/intellectualproperty.asp.
[7] Alexandra Twin, *Competitive Advantage Definition with Types and Examples*, Investopedia (May 21, 2025), https://www.investopedia.com/terms/c/competitive_advantage.asp.

intellectual property through online means. The Intellectual Property owners must be aware of new forms of infringement of Intellectual Property that occurs due to new internet technology. World Intellectual Property Organisation WIPO & World Trade Organisation WTO gives protection to Intellectual Property by maintaining balance between return on investment in knowledge Intellectual property owner & giving unrestricted access, benefits of knowledge to the Intellectual property user [8].

Some of the examples *of IPR and Cybercrime* are as follows-

2.1. Copyright-

Section 14 of the Copyright Act, 1957 defines the word 'Copyright'. Copyright (or author's right) is a legal term used to describe the rights that creators have over their literary and artistic works. Works covered by copyright range from books, music, paintings, sculpture, and films, to computer programs, databases, advertisements, maps, and technical drawings.[9]Copyrights violation occurs when someone illegally publishes or create a duplicated copy of the owner's product without his knowledge, Section 51 of the Copyright Act,1957[10] deals with infringement of copyright while Section 63 of the Copyright Act [11]mentions the offences for infringement. Software piracy can be defined as the use of software that is not properly licensed. That might include copying, modifying, distributing or selling the software in ways that contravene copyright laws or license terms.[12] International legal instruments such as the Berne Convention, TRIPS Agreement, and the WIPO Copyright Treaty provide a robust legal framework mandating the protection of software as intellectual property. Despite these frameworks, enforcement is a big challenge due to the nature of piracy.

2.2 Trademark-

Trademarks are governed by the *Trademarks Act, 1999 ('Act')* [13]and the *Trade Marks Rules, 2017 ('Rules').*[14] A trademark means a mark capable of distinguishing the goods or services of one person from those of others. It includes a device, brand, heading, label, ticket, name,

[8] Amit A. Dongare, *Intellectual Property Rights and Cyber Crime*, 11(1) S. Asian J. Mgmt. Res. 864, 864–72 (2021).
[9] World Intellectual Prop. Org., *Copyright*, WIPO, https://www.wipo.int/en/web/copyright.
[10] The Copyright Act, 1957, § 51, No. 14, Acts of Parliament, 1957 (India).
[11] The Copyright Act, 1957, § 63, No. 14, Acts of Parliament, 1957 (India).
[12] Revenera, *Software Piracy*, Revenera, https://www.revenera.com/software-monetization/glossary/software-piracy.
[13] The Trade Marks Act, No. 47 of 1999, India Code (1999).
[14] The Trade Marks Rules, 2017, Noti. No. G.S.R. 876(E), Gazette of India, Pt. II, Sec. 3(i) (India).

signature, word, letter, numeral, shape of goods, packaging, or combination of colours or any combination thereof.[15] In this growing world of e-commerce, it is important for companies to have a domain name and its own website. It plays a very important role in showcasing the goodwill of the company in the market. The legal norms which are applicable on IPR are applicable on domain name as well yet there is no concrete law to protect these domain names in India. Cybersquatting is a form of cybercrime where the perpetrator buys or registers a domain name that is identical or similar to existing domain with the intention of profiting from a recognizable trademark.[16] This practice erodes the original owner from his works and causes financial loss.

2.3 Digital Vandalism or Website Defacement –

Defacement (also website or web defacement) is an attack on a website that alters its visual appearance or informational content. [17] Another common process called Web Hijacking refers to the process of illegally taking control of another person's website without his permission. In such cases, the original owner loses control over his work. Defacement can damage the goodwill associated with a company, which is protected under trademark law. It can also breach trade secret protection and cause economic loss.

3.Techniques and Entry Points in Cyber-Driven IP Theft-

3.1 Phishing and Social Engineering

Valuable and sensitive data for the benefit of cyber criminals. Social engineering challenges network security regardless of the strength of its firewalls, intrusion detection systems, encryption methods and antivirus software systems. Social engineering, also known as human piracy, is the art of phishing and traces the victim to revealing his or her credentials and then is used to access networks or accounts. It uses deception and manipulation of the victim or just a follow-up, discovery and curiosity. Phishing and harmful activities affect victims psychologically by revealing their confidential information and breaking security barriers[18]. Cybercriminals often use deceptive mails and messages to obtain sensitive

[15] IndiaFilings, *Trademark Definition: What It Is and Why It Matters*, IndiaFilings (Dec. 7, 2024), https://www.indiafilings.com/learn/trademark-definition/.
[16] Kaspersky, *What is Cybersquatting?*, Kaspersky, https://www.kaspersky.com/resource-center/preemptive-safety/cybersquatting.
[17] Kaspersky, *Website Defacement*, Kaspersky IT Encyclopaedia, https://encyclopedia.kaspersky.com/glossary/deface/.
[18] Abeer F. Al-Otaibi & Emad S. Alsuwat, *A Study on Social Engineering Attacks: Phishing Attack*, 7(11) Int'l J. Recent Advances Multidisciplinary Res. 6374, 6374–80 (2020).

information such as passwords, bank account by tricking the employees. Once granted the access, they extract intellectual property.

3.2 Malware Infiltration-

Malware, short for malicious software, refers to any software or code specifically designed to damage, disrupt, or gain unauthorized access to computers, networks, and devices. Malware typically infiltrates a system through different attack vectors, such as email attachments, malicious links, compromised software downloads, or vulnerabilities in outdated software. Once inside a system, malware can execute a variety of harmful activities[19].Several distinct types of malwares are frequently employed to compromise intellectual property such as keyloggers, spyware, ransomware, remote access trojans (RATs), rootkits. The infiltration of malware into the system by law firms, government institutions, research centres can result into-loss of trade secrets, financial damage, erosion of competitive advantage, reputational harm and national security risks.

3.3. Cloud Exploits and Data Mismanagement-

Cloud Computing is a type of technology that provides remote services on the internet to manage, access, and store data rather than storing it on Servers or local drives. This technology is also known as Serverless technology.[20] Many organizations are moving their sensitive date including intellectual property to a third-party cloud platform, it introduces a line of security risks. Some security gaps make cloud infrastructure attractive targets for Intellectual Property theft such as Misconfigured Permissions and Access Controls, Unsecured APIs Application Programming Interfaces, Weak or Absent Encryption.

3.4. Advanced Persistent Threats (APTs)-

An advanced persistent threat (APT) is a broad term used to describe an attack campaign in which an intruder, or team of intruders, establishes an illicit, long-term presence on a network in order to mine highly sensitive date. The targets of these assaults, which are very carefully chosen and researched, typically include large enterprises or governmental networks. [21] Theft of extremely sensitive intellectual property, such as military technology,

[19] Xcitium, *What is Malware?* Xcitium (2024), https://www.xcitium.com/knowledge-base/malware/.
[20] GeeksforGeeks, *Security Issues in Cloud Computing*, GeeksforGeeks (May 24, 2023), https://www.geeksforgeeks.org/security-issues-in-cloud-computing/.
[21] Imperva, *What is APT (Advanced Persistent Threat)*, Imperva (2025), https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/.

biotech research, proprietary algorithms, and other strategic assets vital to economic and national security interests, is a common objective of APTs. Because these attacks are so covert, the attackers can stay within systems for months or even years, harvesting data continuously while dodging conventional security procedures. Attackers can interrupt innovation pipelines, undermine competitive advantages, and inflict substantial economic harm by compromising intellectual property through APTs. This emphasizes the importance of having strong, proactive security measures.

4, Judicial precedents on intellectual property infringement in cyberspace

In the case of **UTV Software Communication Ltd. And Ors vs 1337X. To And Ors on 10 April, 2019[22],**

The ***main issue*** raised was whether an infringer of copyright in the cyberspace is to be treated differently from the infringer of copyright in the physical world? The ***facts summary*** of the case was that eight law suits was filed by a company involved in content creation. The Plaintiffs sought injunction restraining the Defendants from infringing the Plaintiff's copyrighted works in cinematograph films by communicating it to the public without any authorization. The Plaintiffs produced samples of infringing content to support their one-point case that the infringing websites were primarily engaged in hosting pirated content and allowed streaming and downloading of Plaintiffs copyrighted works without any authorisation[23]. It was held that the defendant website was liable for copyright infringement under section 51 of the Copyrights Act, 1957.[24] The court passed a website blocking order to disable the access granted to the defendant website. The Court adopted the relief of dynamic injunction drawing its inspiration from the case of *Singapore High Court's decision in Disney Enterprise v. MI Ltd. (2018) SGHC 206* which essentially aims to block new means of accessing the same infringing website. A plaintiff can avail the blocking injunction against a new website by filing an additional affidavit, giving the court an explanation as to how a new website is within the purview of an existing blocking order. [25]The court further added that a policy should be issued to warn the consumers against watching infringing content.

[22] UTV Software Commc'n Ltd. & Ors. v. 1337x.to & Ors., [2019] CS(COMM) 724/2017 (Del. HC).
[23] UTV Software Commc'n Ltd. & Ors. v. 1337x.to & Ors., CS(COMM) 724/2017 (Del. HC Apr. 10, 2019), reported in (2019) 78 PTC 375 (Del.).
[24] The Copyright Act, 1957, § 51, No. 14, Acts of Parliament, 1957 (India).
[25] Obhan & Assocs., *Dynamic Injunctions to Tackle Digital Piracy in India*, Obhan & Assocs. Blog (Dec. 17, 2020), https://www.obhanandassociates.com/blog/dynamic-injunctions-to-tackle-digital-piracy-in-india/.

5. Existing Legal Provision on IPR and Remedies

Governing Regulations- Intellectual properties rights in India are governed under the following Acts:

- Trade Marks Act, 1999
- The Patents Act, 1970 (amended in 2005)
- The Copyright Act, 1957
- The Designs Act, 2000
- The Geographical Indication of Goods (Registration and Protection) Act, 1999
- The Protection of Plant Varieties and Farmers Rights Act, 2001
- The Information Technology Act, 2000[26]

There are various remedies that are available to an aggrieved in case of infringement of Intellectual property rights.

- **Civil remedies** include- In accordance with *section 55 of the Copyright Act*[27], the copyright owner is entitled to all civil remedies for copyright infringement, including injunctions(court order refraining a person from doing certain acts), damages(it aims at compensating the losses that a person has occurred due to infringement) accounts of profit (it covers the profit that a person has made due to the infringement),delivery or destruction of the infringing item (the court may in addition to injunction ,order the delivery of the infringed items or could order to destroy the items) and other remedies that may be granted by law. The court may order the seizure of copies that are infringing and their delivery to the copyright owner under *Section 66.* When instances of infringement and passing off occur, in case of the trademark, the owner can approach to the district court for grant of interlocutory injunction, anton pillar orders, damages and account of profits. In case of patent same civil remedies are available to the holder.[28]

[26] IndiaFilings, *Intellectual Property Laws in India*, IndiaFilings, https://www.indiafilings.com/learn/intellectual-property-laws-in-india.
[27] The Copyright Act, 1957, § 55, No. 14, Acts of Parliament, 1957 (India).
[28] Dr. B.L. Wadehra (ed.), *Law Relating to Intellectual Property* 176, 342 (5th ed. Delhi, Universal Law Publ'g Co. Pvt. Ltd.).

- **Criminal remedies-** According to *section 63 of the Copyright Act*[29], anyone who wilfully violates or encourages the violation of a work's copyright is guilty of a crime, will be punishable with a fine of not less than fifty thousand rupees but not more than two lakh rupees, and term of imprisonment that will not be less than six months but may extend to three years.[30]
- **Administrative remedies**- It consists of moving the registrar of copyrights to ban the import of infringing copies into India when the infringement is by the way of such importation and the delivery of the confiscated infringing copies to the owner of the copyright and seeking delivery. [31]
- **Remedies available for infringement in cyberspace-** *Information Technology (Intermediaries Guidelines) Rules 2011* [32]*and Section 79 IT Act, 2000* [33]grant conditional safe harbour from liability of the online intermediaries, though keeping it open for interpretation on their liability under any other civil or criminal Act. IT Act 2000 makes an intermediary non-liable for any third-party content hosted on its site. The 2011 Guidelines provide a diligence framework to be followed by intermediaries to avail the exemption granted in Section 79 IT Act, 2000. This makes it important for proactive judicial interpretation depending on the facts of each case.[34]

6. Identifying the Legal Blind Spots in Cyber IP Enforcement and the Need for Reform.

In the era of digital world when the internet is growing at a fast space and is eliminating physical and territorial barriers cybercrime including Intellectual property can occur remotely or from anywhere in this world instantly and anonymously. The traditional legal framework guarding Intellectual property rights becomes obsolete in addressing such cross-border issues. Though India has tried and made an effect to keep pace with the growing problem yet the question of jurisdiction gap is something which has not yet been answered.

6.1 The current legal framework and its limitation

[29] The Copyright Act, 1957, § 63, No. 14, Acts of Parliament, 1957 (India).
[30] The Copyright Act, No. 14 of 1957, § 63, India Code (1957).
[31] Dr. B.L. Wadehra (ed.), *Law Relating to Intellectual Property* 176, 342 (5th ed., Universal Law Publ'g Co. Pvt. Ltd., Delhi).
[32] Information Technology (Intermediaries Guidelines) Rules, 2011, Noti. No. G.S.R. 314(E), Gazette of India, Pt. II, Sec. 3(i) (India).
[33] The Information Technology Act, 2000, § 79, No. 21, Acts of Parliament, 2000 (India).
[34] Nupur Mitra, *Intellectual Property Rights Law in Cyberspace*, iPleaders Blog (Nov. 22, 2021), https://blog.ipleaders.in/intellectual-property-rights-law-in-cyberspace/.

Section 75 of the Information Technology (IT) Act, 2000 [35]and *Section 1(5)(c) of the Bharatiya Nyaya Sanhita (BNS), 2023,* [36]reveals that it aims at answering juridical questions in the domain of Indian cyber law yet leaves a gap and does not answer important questions. As long as the offense includes a computer, system, or network situated within Indian territory, section 75 of the IT Act expands its jurisdiction to include offenses committed outside of India. This implies that if the digital infrastructure is headquartered in India, Indian law may still be applicable even if the victim and the offender are not physically present in India.[37] However, the word 'involves' that has been used is broad, vague and open to multiple interpretations. This broad scope of application could result in application of this law in cases where no Indian party or interest in directly involved. For example, if a cybercrime is committed between two foreign nationals but the same has occurred using a server located in India then Indian laws will be applied in such a case. This raises the issue of sharp conflict between international legal principle mainly the principle of territorial sovereignty which implies that a nation's law should be applied within its own country.

Similarly, in the BNS,2023 the word 'targeting' has been used in Section 1(5)(c), stating that the law implies when a computer network located in India is targeted. Still, the word has not been properly defined which leads to ambiguity. Since "targeting" could mean simply "aiming at" in a general sense, it becomes unclear whether the law covers scenarios where:

- The real target is a **person**, not the computer resource;
- The computer resource is merely a **tool** for committing the crime, such as in cases of online defamation;
- Foreign nationals use an **Indian-based server** to commit an offence against another foreign national;
- **Data is copied** from a server outside India and shared globally, unintentionally reaching Indian users;

[35] The Information Technology Act, 2000, § 75, No. 21, Acts of Parliament, 2000 (India).
[36] The Bharatiya Nyaya Sanhita, 2023, § 1(5)(c), No. 45, Acts of Parliament, 2023 (India).
[37] Md. Jiyauddin & Sunita Banerjee, *A Critical Analysis of the Safeguarding of Intellectual Property Rights in India Through Cybercrime*, 12(10) J. Res. Human. & Soc. Sci. 71 (2024), https://www.questjournals.org/jrhss/papers/vol12-issue10/12107174.pdf.

- A passive website with pirated content, **hosted outside India**, is accessible in India without being specifically directed at Indian users.[38]

The lack of clear definition and improper implementation highlights how the present laws have failed to address the issue of IP theft in cyberspace.

6.2 The role of Judiciary and Global legal theories

While Indian laws and statutes have tried to extend jurisdiction in cyberspace yet a lot depends on interpretation and legal reasoning. Indian courts have shown flexibility and initiative while handling cybercrime and Intellectual Property cases continuously adapting to the evolving digital context. However, this activism alone cannot compensate for the lack of a well-defined legislation. Given the challenges of enforcing national laws in a global digital environment, courts around the world including in India have increasingly looked toward jurisdictional tests developed in international jurisprudence, especially by U.S. courts. These include:

- **Minimum Contacts Test**: This test checks whether the defendant has had sufficient, deliberate interactions with the jurisdiction of the court (e.g., business transactions or targeted communication).
- **Effects Test**: Here, jurisdiction is based on where the harmful impact of the act is felt, regardless of where it originated.
- **Sliding Scale or Zippo Test**: This test evaluates the degree of interactivity and commercial nature of a website. The more interactive and commercial a site is, the more likely it falls under a court's jurisdiction.[39]

These frameworks can help Indian courts in going through cases involving foreign websites and international users.

6.3 Need for Stronger Legislative Framework and International Cooperation

Despite the extraterritorial reach provided by Section 75 of the IT Act and Section 4 of the Indian Penal Code (IPC), 1860[40], which extends jurisdiction to offences committed outside India under certain conditions, current laws are not adequately equipped to tackle modern

[38] Md. Jiyauddin & Sunita Banerjee, *A Critical Analysis of the Safeguarding of Intellectual Property Rights in India Through Cybercrime*, 12(10) J. Res. Human. & Soc. Sci. 71 (2024), https://www.questjournals.org/jrhss/papers/vol12-issue10/12107174.pdf.
[39] Nupur Mitra**,** *Intellectual Property Rights Law in Cyberspace*, IPLEADERS (Nov. 22, 2021), https://blog.ipleaders.in/intellectual-property-rights-law-in-cyberspace/.
[40] The Indian Penal Code, 1860, § 4, No. 45, Acts of Parliament, 1860 (India).

cybercrimes, particularly in the IP domain. The borderless nature of the internet, combined with the ease of duplicating and sharing copyrighted material, makes enforcement particularly difficult.[41] Cross border IP disputes are becoming increasingly common which calls for not just reforms in domestic laws but also greater international cooperation. India must strengthen its cross border, bilateral, trilateral treaties and participate more in internation dialogues to effectively address this growing issue of IP infringement in cyberspace.

7. Conclusion

The growing use of digital technology and internet has made it increasingly challenging to protect intellectual property such as patents, trademark, copyrights etc. New technique such as phishing, malware and hacking is being used by cybercriminals to steal important data and original work. This poses a great threat to people, companies and government. Even though India has laws to combat cybercrime and infringement of IPR, many of these rules and regulation are insufficient to cope with the infringement of IPR committed in the online space especially when individuals from other nations are involved. There is an additional problem of determining which countries law will be applicable in such a case. Indian courts have attempted to resolve problem by applying international regulations, but more work has to be done.

India has to modernize it law, strengthen international cooperation, focus more on stringent enforcement and develop better guidelines for dealing with cybercrime related to IPR. Companies and people should be more vigilant and mindful of these cyber hazards. Only by working together through laws, technology, and global support can we keep intellectual property safe in today's digital age.

[41] Juris Centre, *Cybercrime Involving Intellectual Property Rights*, JURIS CENTRE BLOG (Apr. 21, 2024), https://juriscentre.com/2024/04/21/cybercrime-involving-intellectual-property-rights/.

Bibliography

Books

- Wadehra, B.L. (ed.), *Law Relating to Intellectual Property*, 5th ed., Universal Law Publishing Co. Pvt. Ltd., Delhi.

Statutes

- The Copyright Act, 1957, No. 14, Acts of Parliament, 1957 (India).
- The Trade Marks Act, 1999, No. 47, Acts of Parliament, 1999 (India).
- The Patents Act, 1970, No. 39, Acts of Parliament, 1970 (India), amended by The Patents (Amendment) Act, 2005, No. 15, Acts of Parliament, 2005 (India).
- The Designs Act, 2000, No. 16, Acts of Parliament, 2000 (India).
- The Geographical Indications of Goods (Registration and Protection) Act, 1999, No. 48, Acts of Parliament, 1999 (India).
- The Protection of Plant Varieties and Farmers' Rights Act, 2001, No. 53, Acts of Parliament, 2001 (India).
- The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
- The Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).
- The Indian Penal Code, 1860, No. 45, Acts of Parliament, 1860 (India).
- Information Technology (Intermediaries Guidelines) Rules, 2011, Noti. No. G.S.R. 314(E), Gazette of India, Pt. II, Sec. 3(i) (India).

Journal Articles

- Dongare, Amit A., *Intellectual Property Rights and Cyber Crime*, 11(1) South Asian Journal of Management Research 864–872 (2021).
- Jiyauddin, Md. & Banerjee, Sunita, *A Critical Analysis of the Safeguarding of Intellectual Property Rights in India Through Cybercrime*, 12(10) Journal of Research in Humanities and Social Science 71 (2024), https://www.questjournals.org/jrhss/papers/vol12-issue10/12107174.pdf.

Cases

- UTV Software Communication Ltd. & Ors. v. 1337x.to & Ors., CS(COMM) 724/2017 (Del. HC Apr. 10, 2019), reported in (2019) 78 PTC 375 (Del.).

Web Sources

- Malwarebytes, *What is Malware? Malware Definition, Types and Protection*, Malwarebytes (2025), https://www.malwarebytes.com/malware.
- Investopedia, *Intellectual Property (IP): What It Is and Types*, Investopedia (2025), https://www.investopedia.com/terms/i/intellectualproperty.asp.
- Twin, Alexandra, *Competitive Advantage Definition with Types and Examples*, Investopedia (May 21, 2025), https://www.investopedia.com/terms/c/competitive_advantage.asp.
- Shibboleth Consortium, *Shibboleth Project*, Internet2, https://shibboleth.internet2.edu/.
- Kaspersky, *What is Cybersquatting?*, Kaspersky, https://www.kaspersky.com/resource-center/preemptive-safety/cybersquatting.
- Kaspersky, *Website Defacement*, Kaspersky IT Encyclopaedia, https://encyclopedia.kaspersky.com/glossary/deface/.
- Xcitium, *What is Malware?* Xcitium (2024), https://www.xcitium.com/knowledge-base/malware/.
- GeeksforGeeks, *Security Issues in Cloud Computing*, GeeksforGeeks (May 24, 2023), https://www.geeksforgeeks.org/security-issues-in-cloud-computing/.
- Imperva, *What is APT (Advanced Persistent Threat)*, Imperva (2025), https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/.
- Obhan & Associates, *Dynamic Injunctions to Tackle Digital Piracy in India*, Obhan & Associates Blog (Dec. 17, 2020), https://www.obhanandassociates.com/blog/dynamic-injunctions-to-tackle-digital-piracy-in-india/.
- IndiaFilings, *Trademark Definition: What It Is and Why It Matters*, IndiaFilings (Dec. 7, 2024), https://www.indiafilings.com/learn/trademark-definition/.
- IndiaFilings, *Intellectual Property Laws in India*, IndiaFilings, https://www.indiafilings.com/learn/intellectual-property-laws-in-india.

- Mitra, Nupur, *Intellectual Property Rights Law in Cyberspace*, iPleaders Blog (Nov. 22, 2021), https://blog.ipleaders.in/intellectual-property-rights-law-in-cyberspace/.