International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 21s, 2025
https://www.theaspd.com/ijes.php

Legal Considerations in Protecting Intellectual Property from Cyber Theft

Ankita Das[1], Dr Manish Kumar Singh[2]
[1]Research Scholar, (NIMS School of Law), NIMS University Rajasthan, Jaipur, ad1298208@gmail.com
[2]Assistant Professor, (NIMS School of Law), NIMsS University Rajasthan, Jaipur,manishsinghlaw@gmail.com

Abstract
IP protection against cyber theft is crucial in this information age. Due to the increased usage of digital platforms for IP management and distribution, cyber theft is a worry for organisations. This has major legal and financial consequences. This study discusses intellectual property theft protection's multiple legal frameworks, challenges, and emerging issues. It begins with a basic overview of IP, including patents, trademarks, copyrights, and trade secrets, and cybercrime, including hacking, malware, and phishing. This article discusses how national laws like the DMCA, CFAA, GDPR, and NIS Directive and international treaties like the TRIPS Agreement and WIPO conventions safeguard IP. Famous cases of intellectual property theft demonstrate the intricacy of cyber threats and their legal ramifications. Administrative, criminal, and civil remedies are used to demonstrate how different governments address cyber theft. The preventative measures area covers organisational, technical, and legal solutions include contracts, non-disclosure agreements, encryption, network security, employee training, and incident response plans. The report also discusses jurisdictional issues, AI and IoT cyber threats, and how to balance privacy and security, especially for GDPR compliance. Policy recommendations focus on strengthening national legislative frameworks, promoting public-private partnerships, encouraging cybersecurity technological innovation, and increasing international cooperation. Combining these strategies, the study proposes a complete IP protection plan that accounts for the ever-changing cyber threat environment. In the conclusion, innovation, global cooperation, and proactive IP protection are stressed. This in-depth investigation can help policymakers, companies, and legal practitioners preserve intellectual property in the digital era and prevent cyber crime
Keywords: *Intellectual property (IP), cyber theft, cybersecurity, legal frameworks, TRIPS Agreement*

1. INTRODUCTION

Business IP includes inventions, literary and artistic works, designs, symbols, names, and photographs. Artists can benefit from public recognition and financial gain through many forms of intellectual property legislation. Trade secrets, copyrights, patents, and trademarks are the most common intellectual properties. Any product or procedure that solves an old problem or improves efficiency might be patented, giving the owner exclusive usage rights. The innovation cannot be made, used, distributed, or sold without the patent holder's consent. Trademarks distinguish one company's goods and services from another. Intellectual property rights protect trademarks, which can be words, logos, or both[1]. Copyright protects authors, artists, and publishers' literary and visual art. Copyright includes written word, moving image, sound, computer code, databases, advertisements, maps, and technical drawings. Trade secrets include recipes, processes, designs, tools, patterns, and data collections. Without official registration, a company can protect its trade secrets and gain a competitive edge with confidentiality agreements and other internal security measures.

Cybercrime or cyber threat is theft or unlawful action committed online. IP theft by cyber means is part of this. Intrusions into company databases to steal proprietary information, malware to steal trade secrets, and phishing to access confidential files are all IP-related cybercrimes. Consider Sony Pictures Entertainment. They were hacked in 2014, losing emails and unreleased films. In 2017, NotPetya ransomware stole intellectual property from Merck & Co. All these cases demonstrate how vulnerable digital data is and how fraudsters are becoming more adept at exploiting it. Intellectual property cyber theft prevention is crucial for various reasons. Intellectual property theft is costly. Businesses invest heavily in R&D to generate innovative product, process, and other ideas. These thefts cost businesses money and innovation. IP theft is a substantial

[1]Badway EE, McGuinness C. The Criminal, Regulatory, and Civil Issues Surrounding Intellectual Property and Cybersecurity. Brook. J. Corp. Fin. & Com. L..2019; 14:181.

contributor to cybercrime's $400 billion annual economic damage. Companies decreasing innovation expenditure and laying off people could hinder the economy. IP theft is a serious crime. Companies face complicated legal processes when seeking damages or protecting IP. Criminal prosecution and civil litigation for injunctions and damages are part of this process. Long, expensive lawsuits strain already-strapped finances. IP theft can also damage a company's reputation, consumer trust, and market position. Lawful prevention of intellectual property cyber theft is the focus of this investigation. It will examine the global and domestic legal system, highlighting relevant treaties, statutes, and regulations. Real-world case studies will support cyber theft analysis and demonstrate how these crimes damage businesses and the economy. It will also discuss IP holders' civil, criminal, administrative, and judicial enforcement options. The paper will also discuss integrating organisational, technical, and legal strategies to prevent IP theft. It will address jurisdictional issues, shifting cyber dangers, and the delicate balance between privacy and security. The report will advocate public-private partnerships, international cooperation, better national legislative frameworks, and cyber security innovation to improve cyber security. The study examines these aspects to contribute to the digital era intellectual property debate and inform policymakers, companies, and attorneys.

2. LEGAL FRAMEWORK FOR IP PROTECTION

International collaboration and regulatory frameworks are needed to protect intellectual property (IP), which is essential to international trade and innovation, and encourage economic growth while protecting individual rights. Important international treaties and agreements enforce intellectual property laws worldwide. TRIPS administer the World Trade Organization, making it a significant intellectual property agreement. The 1994 TRIPS accord prioritizes copyrights, patents, trademarks, industrial designs, trade secrets, and geographical indications[2]. TRIPS sets minimum requirements for member states to adopt to avoid intellectual property limitations hindering international trade. TRIPS require member states to patent technical breakthroughs that are original, inventive, and industrially applicable. This standardized method fosters innovation and technical advancement by sharing information and protecting innovators. TRIPS impose administrative, civil, and criminal penalties for intentional IP infringement. It emphasizes strong legal safeguards for IP and its owners. TRIPS dispute settlement methods provide fairness and openness in international economic exchanges involving intellectual property rights. TRIPS affect international IP. TRIPS consistency increased IP law enforcement domestically. Harmonization of IP standards gives international companies more assurance and visibility.

TRIPS has helped developing nations share knowledge and technology. TRIPS' intellectual property protection promotes economic growth and research. Intellectual property protection has drawn investors and tech holders to emerging nations, helping them integrate economically. In addition to the TRIPS Agreement, WIPO administers several international treaties that standardize and strengthen IP protection worldwide. WIPO promotes innovation and creativity by efficiently protecting intellectual property rights and using IP for economic, social, and cultural growth[3]. The 1883 Paris Convention, administered by WIPO, was one of the first international IP accords. It describes how to protect trademarks, patents, industrial designs, trade names, and geographical indications. The agreement defines national treatment to ensure that non-domestic applicants in member nations have the same intellectual property rights as domestic applicants. Global fair competition and mutual benefit are promoted by this principle.

The 1886 Berne Convention protects literature, art, music, and film. It sets minimum copyright protection requirements like authorship recognition and automatic protection upon creation. Berne Convention members promise to ensure adequate and effective copyright protection so creators can have legal certainty and control over their creations in worldwide markets. In 1996, WIPO created the WIPO Copyright Treaty

[2]Taherdoost H. Legal, Regulatory, and Ethical Considerations in E-Business. InE-Business Essentials: Building a Successful Online Enterprise 2023 Sep 5 (pp. 379-402). Cham: Springer Nature Switzerland.

[3]Sikder AS, Allen J. An In-depth Exploration of Emerging Technologies and Ethical Considerations in Cross-border E-commerce: A Comprehensive Analysis of Privacy, Data Protection, Intellectual Property Rights, and Consumer Protection in the context of Bangladesh.: Technologies and Ethical Considerations in Cross-border E-commerce. International Journal of Imminent Science & Technology. 2023;1(1):116-37.

(WCT) and WIPO Performances and Phonograms Treaty (WPPT) to address digital technology and internet challenges. These accords modify and expand the Berne Convention and Rome Convention to address digital issues like copyrighted work dissemination online and phonogram producer and performer protection. Finally, the TRIPS Agreement and other WIPO-managed international accords shape global intellectual property protection. These frameworks establish basic standards, facilitate international cooperation, and promote innovation by protecting the rights of inventors, creators, and enterprises worldwide. These treaties will help solve emerging digital economy difficulties and protect intellectual property rights in a globalised society. International collaboration and commitment to these values are essential to foster innovation, creativity, and long-term economic success across boundaries.

3. CYBER THEFT AND IP INFRINGEMENT

Cybercrime, especially IP theft, is growing in the information age. Cybercriminals often steal valuable intellectual property. Most methods involve insider threats, phishing, hacking, and malware. Phishing is a popular cybercrime method. Deceptively solicit passwords or confidential data from unwary web users. Phishers often impersonate government agencies or trusted coworkers. Breaking into systems and stealing login credentials can pilfer confidential information. Cybercriminals utilise malware. It includes viruses, worms, Trojan horses, malware, and ransom ware. Malware usually enters via tainted software downloads, compromised websites, and email attachments. Once installed, malware can steal data, spy on user activity, encrypt files and demand payment to decode them, or all three. Several firms have had their IP locked and kept prisoner by ransom ware.

Hacking, or unauthorised computer access, is another direct and often more dangerous kind of cyber theft. Software and network security flaws allow hackers to break into systems and steal data. Software security flaws, brute-force password guessing, and advanced persistent threats (APTs) can be used to discreetly stay on a system for a long time. High-profile cyber attacks that generate large data breaches often result in IP theft and sale on the dark web or industrial espionage. Threats from within are another big issue. Contractors and employees with legitimate access to sensitive information pose the biggest risk to businesses. Retaliation against their employer, personal gain, or competitor benefit are reasons insiders steal IP4. Since they have access to the company's data and systems, insiders' malicious behaviour is harder to detect and halt. Businesses should train personnel, audit frequently, and implement strict access restrictions to reduce insider threats.

Recent high-profile cyber-intellectual property theft cases have highlighted the seriousness of the consequences and the intricacy of the legal concerns. These events show how scammers can breach even strong systems. A good example is the 2014 Sony Pictures Entertainment cyber attack. The Lazarus outfit, a North Korean hacking outfit, entered Sony's network and took scripts for upcoming films, employee data, and emails.

The culprits broke into Sony's system using phishing emails and advanced software. The incident caused financial losses, reputation damage, and legal conflicts over employee data and the breach. This incident underlined the need for adequate incident response procedures and cyber security precautions. Pharmaceutical company Merck & Co. got involved in another scandal in 2017. NotPetya targeted Merck using a compromised accounting software upgrade from a Ukrainian firm. Starting as ransom ware, NotPetya was a destructive wiper malware that encrypted data irretrievably. The attack shut down manufacturing and cost Merck a lot of money. The complexity of identifying and responding to cyber intrusions was highlighted in Merck's later legal issues, which included insurance coverage disputes[5].

[4]Mostert F. Digital tools of intellectual property enforcement: their intended and unintended norm setting consequences. InResearch Handbook on Intellectual Property and Digital Technologies 2020 Jan 7 (pp. 553-576). Edward Elgar Publishing.

[5]Babikian J. Navigating legal frontiers: exploring emerging issues in cyber law. Revista Espanola de DocumentacionCientifica. 2023 Dec 30;17(2):95-109.

A massive OPM data breach in 2015 jeopardised the personal data of over 21 million government employees. Investigators believe Chinese state-sponsored entities took social security numbers, fingerprints, and security clearance data from OPM's network. The hack raised worries about government-held intellectual property protection, affecting national security. Cyber espionage requires strict cyber security legislation and global collaboration, as shown by the OPM attack's legal and political ramifications. Another example is the 2020 SolarWinds hack, which attacked the IT management corporation. Russian hackers corrupted hundreds of SolarWinds software upgrades installed by government agencies and large corporations. This supply chain attack allowed hackers to steal critical networks, IP, and data for months. Regulators and courts investigated supply chain vulnerabilities after SolarWinds. Businesses harmed by the incident struggled to recognise, mitigate, and resolve legal issues.

These cases demonstrate how intricate cybercrime affects companies. These occurrences demonstrate the need for vulnerability assessments, staff education, incident response plans, and regulator-law enforcement collaboration in cyber security. Businesses that deal with cyber theft should be conversant with intellectual property and cybercrime regulations after these court decisions. In conclusion, digital IP theft is a severe and evolving issue that requires continual monitoring and intervention. By studying case studies and cyber theft strategies, organisations may better protect their IP and handle legal challenges after cyber-attacks.

4. LEGAL REMEDIES AND ENFORCEMENT

Civil remedies, which allow IP owners to seek compensation and stop infringements, are crucial to fighting internet IP theft. These remedies enable courts to quickly and effectively defend the rights of creators, inventors, and enterprises in the digital age, making them essential to IP protection systems worldwide. The owner of intellectual property may seek a court injunction to stop unauthorized use. Intellectual property is rapidly and globally distributed, making cyber theft injunctions essential. Parties can obtain preliminary injunctions to stop violations before a final determination. Interim actions are necessary since the infringement may continue to use the IP and hurt the owner. Thirteen, the court may issue a permanent IP injunction in its final conclusion. They protect the owner's assets and reputation by prohibiting others from using, distributing, or profiting from infringed intellectual property. Courts can adjust injunctions to prevent unauthorized use on different platforms and jurisdictions6.

IP owners can sue for damages after cyber theft. The IP owner receives their money back if there are damages. Actual damages may pay the intellectual property owner for lost earnings, market share, or infringement defense costs. If actual losses cannot be calculated to sufficiently compensate for the harm, statutory damages may apply. Statutory damages are a legal compensation standard. They help IP owners receive their money's worth when infringement costs are hard to calculate. Courts can assess punitive damages for willful and malicious infringement. Punitive damages are monetary sanctions that exceed the actual injury to deter future offences. The courts take purposeful IP theft seriously, and this punishment underscores how vital IP rights are online. In addition to injunctive relief and damages, civil remedies include a variety of legal actions to restore the IP owner's legitimacy and deter future wrongdoing. Restitution orders require the infringer to restore intellectual property earnings to remedy unfair enrichment. This technique restores IP ownership by taking financial gains from infringement. An intellectual property dispute court may issue a declaratory ruling to clarify rights and duties. Declaratory remedy establishes intellectual property rights' validity and breadth to avoid future disagreements and simplify legal compliance. If things or materials were used to commit an infringement, courts may order their seizure and destruction to halt unauthorized copies or sales.

IP litigation might be difficult, but civil remedies can preserve IP. Cyber theft claims and damages must be supported by appropriate evidence, which can consume civil litigation resources7. Digital evidence is complicated and cyber threats are global, therefore forensic analysis and knowledge may be needed to prove

[6]Allahrakha N. Balancing cyber-security and privacy: legal and ethical considerations in the digital age. Legal Issues in the digital Age. 2023(2):78-121.

[7]Segate, R. V. (2020). Securitizing Innovation to Protect Trade Secrets between" the East" and" the West": A Neo-Schumpeterian Public Legal Reading. *UCLA Pac. Basin LJ*, *37*, 59.

culpability. Civil remedies in cross-border cases depend on court enforceability. Legal systems must cooperate to enforce injunctions and monetary awards worldwide. International collaboration and judicial recognition can improve civil remedies for cross-border IP theft. Finally, IP owners need civil remedies to fight cyber theft and exercise their rights. Injunctions and damages can stop illegal use, compensate losses, and prevent future wrongdoing. Declaratory judgments and restitution enhance equity and IP compliance. Legal frameworks must promote global cooperation to protect intellectual property from emerging cyber threats. Civil remedies that work is becoming increasingly crucial in the digital age. Innovative and meticulous legal measures can protect intellectual property rights in a technologically evolved and globally networked economy.

Criminal prosecution deters online IP theft by emphasizing the crime's seriousness and the sanctions for perpetrators. Many laws prohibit police enforcement from engaging in cybercrime or associated activities. The US Computer Fraud and Abuse Act prohibits computer hacking and theft, notably of intellectual property. CFAA offences can result in jail time and large fines. Another key regulation is the EEA, which prohibits trade secret theft. The European Economic Area distinguishes commercial theft from foreign government theft. Due to the significance of trade secrets and sensitive information, EEA violators face long prison sentences and substantial fines. The Digital Millennium Copyright Act (DMCA) criminalises those who circumvent digital rights management technologies to illegally access and distribute intellectual property.

States and federal legislation can criminalise online IP theft. State computer crime laws supplement federal laws to help prosecutors fight cybercrime. California's Comprehensive Computer Data Access and Fraud Act penalise illicit IP and computer data access.

In cyber theft charges, the FBI, DOJ, and international law enforcement often collaborate on complex investigations. Complex forensic methods are needed to determine where the hack came from, who perpetrated it, and what evidence can be used in court. Cybercrime impacts people worldwide, making it impossible to prosecute without international conventions and cross-border collaboration, such as the Budapest Convention on Cybercrime. Administrative actions by regulatory and intellectual property offices are vital to combating IP theft outside of court.

These measures include assessing IP rights, issuing sanctions, and punishing infringers. The USPTO and EPO are essential to protecting intellectual property rights. These departments can investigate intellectual property infringement claims and revoke erroneously granted patents, trademarks, and copyrights. The IP office can re-examine and perhaps revoke an unlawfully patented patent, such as a stolen trade secret, to protect the real owner. The US Federal Trade Commission (FTC) enforces intellectual property through consumer protection and anti-competition laws. Businesses that steal or abuse IP are investigated by the FTC. Infringement injunctions and fines are available through FTC administrative actions.

The FTC can force companies to improve cybersecurity to prevent future violations. Customs stop interfering with imports and exports. When CBP inspectors seize counterfeit or otherwise illegal goods at the border, they can stop their distribution. Customs authorities may take administrative measures to protect domestic markets and IP. Administrative enforcement is faster than court processes for intellectual property theft8. These may limit remedy options and enforcement across jurisdictions. Civil and criminal IP enforcement is vital, but administrative actions can reinforce this defense. Finally, online intellectual property theft includes many enforcement tools and legal remedies. Intellectual property owners can seek injunctions, damages, and other civil remedies. Criminal prosecution deters cybercrime by emphasising its gravity. Administrative processes also help regulatory agencies and IP offices combat IP infringement and preserve IP rights. These laws and enforcement measures combat cyber theft, a major issue in the digital age.Effective IP protection legislation requires strict monitoring and enforcement. Employees must follow company non-disclosure, contract, and intellectual property policies. Regular audits, training, and reviews can promote a conscientious and compliant IP protection culture. Immediately enforce intellectual property rights if there is suspicion of breach. Companies should have legal or other options for IP infringement or cyber theft. 20. In today's technologically advanced and globally linked world, protecting intellectual property from cyber theft is essential9. This company's swift action shows its commitment to innovation and competition. Policies, non-

[8]Zonghui, L. (2021). In-Depth Interpretation of Intellectual Property Provisions in Chinese Cybersecurity Law. *China Legal Sci.*, *9*, 106.

[9]Malik JK, Choudhury S. Law Relating to Cyber Crimes-Comparative Perspective.

disclosure agreements, and contracts protect critical intellectual property. By outlining rights, duties, and enforcement, organizations can decrease cyber risk, boost regulatory compliance, and stay competitive globally. Legal approaches must be updated to combat new cyber dangers and protect intellectual property in the digital age.

Stopping cyberspace IP theft requires cyber security technologies and standards. Top data security technology is encryption. Even if someone intercepts your data in transit, it is encrypted. Following strict regulations, data should be encrypted while in motion and kept to protect information security (IP). Another important tech measure is network security. In compliance with protocols, intrusion prevention, detection, and firewalls monitor all network data entering and leaving the network.

To prevent thieves from exploiting security gaps, software and hardware must be patched regularly. Network segmentation, which separates critical data from less important data, can help limit breach damage and prevent IP leaks10. Multi-factor authentication and security access controls protect intellectual property. Multi-factor authentication (MFA) prevents unauthorised access to critical systems by requiring multiple forms of identification. Only authorised workers should access certain data and systems based on their duties. Secure access limitations do this. Hard password policies and password upgrades are also security measures. Businesses must also have data backup and recovery policies. Data backups safeguard critical intellectual property against ransom ware and allow for easy restoration. To avoid simultaneous compromise in an attack, secure and segregate backup systems from the primary network.

Organizational measures are needed to prevent IP theft. Employee training is essential since human error causes security breaches. In a complete training programme, employees should learn to recognize and avoid phishing attempts, safe online activities, and security rules. Staff should also get IP protection policy and procedure training to protect confidential information. Company IT system audits are needed to detect and repair security issues. Security audits evaluate security controls, policies, and processes. These audits can help the company enhance its cyber security by identifying vulnerabilities and offering solutions. External experts can examine the company objectively and identify issues the internal team may miss.

When cybercrime occurs, an incident response strategy helps mitigate the damage. A security breach requires a timely and effective response plan. Recognizing the breach, reducing the harm, eliminating the threat, and recovering should be in this strategy. The incident response team needs clear tasks in the strategy to perform well11. Simulations and exercises can test and prepare the organization's incident response strategy. Employee safety must also be promoted. Leadership should priorities cyber security and IP protection and advocate for prevention. Incentivizing staff to adopt best practices and report suspicious activity helps promote organization-wide security. Through partnerships with cyber security businesses and industry groups, you may obtain current threat intelligence and best practices. Sharing information about new dangers and mitigation methods may help firms stay ahead of hackers and improve security.

5. CHALLENGES AND EMERGING ISSUES

Internet globalization and cybercrime's complexity make it harder to overcome jurisdictional constraints in the battle against intellectual property theft. Cybercriminals are challenging to catch since different jurisdictions have varied laws and enforcement procedures. The worldwide nature of the internet makes cybercrime allegations difficult to resolve. When perpetrators, victims, and data servers are in various countries, intellectual property theft claims may be harder to resolve. The inconsistent interpretation of several statutes makes it harder to determine judicial jurisdiction in this case.

Without a worldwide framework, cyber and IP rules are hard to enforce. International accords like TRIPS protect IP, but legal processes and enforcement instruments vary widely. Inconsistency makes it hard to

[10]Wan V, Jiming Y. Torts and intellectual property in Industry 4.0: a comparative study of Chinese and American jurisprudence. Peking University Law Journal. 2021 Jan 2;9(1):111-42.

[11]Gupta PK, Prasanna DV, Raghunath SS. How artificial intelligence can undermine security: an overview of the intellectual property rights and legal problems involved. Applications in Ubiquitous Computing. 2021:37-58.

prosecute cybercriminals who operate across borders, hindering international cooperation between judicial institutions and law enforcement. Example: a nation with strong IP regulations may have trouble prosecuting a cybercriminal from a country with weaker IP laws. The lack of legal standardization makes investigations and cybercrime prevention tougher.

Mutual Legal Assistance Treaties help governments seek and provide legal aid in criminal matters, including cybercrime investigations. However, international legal collaboration causes bureaucratic inefficiencies and delays in MLAT processes[12]. If prosecution is delayed owing to evidence or cooperation issues, cyber thieves may have more time to escape or commit crimes. Language barriers, evidentiary standards, and extradition treaties hinder cross-border legal collaboration for MLATs. MLATs provide complicated diplomatic challenges and procedural constraints, so streamlined methods are needed to speed up information and coordination across foreign law enforcement authorities. International cooperation is needed to resolve jurisdictional issues.

Europol and INTERPOL help member governments cooperate and share information. These groups research and create worldwide cybercrime strategies, including IP theft (IP theft 24). We must harmonies cyber regulations, expedite legal procedures, and boost international collaboration and confidence to develop comprehensive and successful international frameworks. Facilitate worldwide IP enforcement and standardize cybercrime laws.

International agreements and initiatives help combat intellectual property cyber theft. Multinational groups formed the Budapest Convention on Cybercrime to fight intellectual property theft and other cybercrimes. The Budapest Convention harmonized legal frameworks and established mutual legal aid to combat cybercrime globally. The ASEAN Cyber security Strategy and ASEAN Framework Agreement on Intellectual Property Cooperation combat cybercrime and preserve IP rights. These efforts encourage information sharing, skill development, and coordinated operational activities to improve cyber security and fight cybercrime. Jurisdictional considerations make internet intellectual property theft difficult to combat in today's globalised culture (25).

International collaboration and cyber law harmonization are needed due to complex legal frameworks, bureaucratic mutual legal aid procedures, and cross-border enforcement issues. Fighting global cybercrime requires simplifying legal processes, boosting mutual legal aid networks, and increasing law enforcement collaboration. By promoting universal legal standards, information sharing, and multinational alliances, stakeholders can better protect intellectual property rights and prevent cyber theft in the global digital economy. Unwavering commitment is needed to create a safe space for global innovation, creativity, and economic progress.

Due to the development of IoT devices, hackers have more targets. These devices can access larger networks due to their weak security. IoT devices can steal IP data or launch DDoS assaults, making them a security risk[13]. In an interconnected IoT environment, one vulnerable item can endanger an entire network, highlighting the need for strict security measures and frequent monitoring. Block chain provides immutable and transparent transaction records, but 51% attacks and smart contract vulnerabilities might compromise it. As block chain systems become more popular, hackers will have more opportunity to acquire IP through security weaknesses. To tackle these evolving threats, cyber security must evolve. These initiatives should include cyber security awareness, threat intelligence, and adaptive security solutions. The public and private sectors must work together to keep hackers at bay and protect intellectual property from new dangers.

Since the EU's General Data Protection Regulation (GDPR) requires strong privacy protection, intellectual property protection must balance security and privacy. GDPR protects EU residents' privacy by regulating data collection, processing, and storage. While improving privacy, these rules hinder intellectual property protection for companies 27. Maintaining GDPR compliance while implementing effective cyber security safeguards is difficult. Preventing privacy violations requires properly managing network monitoring and

[12]Pringgohadi KA, Alvianti CA, Prasetyo MF, Taalungan LF. Legal protection for creators in copyright infringement through e-commerce. Indonesian Journal of Law and Islamic Law (IJLIL). 2023 Dec 24;5(2):28-39.

[13]Kashyap AK, Chaudhary M. Cyber security laws and safety in e-commerce in India. Law & Safety. 2023:207.

documentation, which are essential for identifying and responding to cyber threats. Data processing must follow GDPR principles including data reduction and purpose limitation, and companies must balance security and data protection.

Privacy concerns include how personal data is handled before, during, and after cyber-attacks. GDPR requires organisations to notify affected individuals and regulatory agencies of data breaches within 72 hours, outlining their nature and effects. To satisfy this fast reaction need, incident response strategies must combine transparency and data security. Big data and AI-powered analytics have raised privacy issues. These systems need a lot of data processing power yet can spot trends and predict threats. Businesses should anonymize or pseudonymize data to protect privacy and comply with GDPR on AI and big data analytics. Businesses must design and implement data protection from the start to comply with GDPR's privacy by design and by default principles.

This method requires continual collaboration between data privacy and cyber security teams to protect intellectual property without invading privacy[14]. Protecting intellectual property from cyber theft has many moving elements and new issues. Jurisdictional difficulties complicate cross-border enforcement; therefore, international collaboration and law harmonisation are needed. Modern technologies like AI and the IoT cause growing cyber threats.

To stay current, security systems must be updated and upgraded. In light of GDPR, cyber security measures that respect privacy rights must be carefully planned and implemented to balance security and privacy. Today's complex and interconnected digital world requires a proactive legal, technological, and organisational strategy to protect intellectual property.

6. POLICY RECOMMENDATIONS

The improved international collaboration is needed to curb IP theft. Cybercrime affects all nations, thus jurisdictional concerns and enforcement must be addressed collaboratively. Nations should seek international treaties and accords to standardise cyber laws and IP protection. Nations can expand on the TRIPS Agreement to adopt more rigorous and consistent policies to make cross-border investigations and prosecutions simpler. Improving MLAT protocols can speed up evidence gathering and international law enforcement coordination. To foster international cooperation, WIPO, Europol, and INTERPOL are vital. These organisations can share cyber security knowledge, best practices, and innovative technology. Governments should participate more in cybercrime and IP-focused global forums and working groups. Countries can collaborate to solve cybercrime by sharing resources and efforts. Multinational and bilateral agreements for real-time information exchange are also important. Sharing data about emerging threats, known hackers, and good protection methods helps countries respond faster to cyber events. Cyber diplomacy channels and cyber envoys should be created to facilitate international coordination and ensure intellectual property protection is a top cyber security priority worldwide.

Preventing online IP theft requires strengthening national laws. To combat cyber attacks, nations should evaluate and update their laws. New cybercrime approaches like AI attacks and IoT vulnerabilities require legislation. Any complete cyber security law should protect IP owners, detect, prosecute, and prevent cybercrime. Stronger sanctions must dissuade cybercrime. To deter IP theft, substantial fines and severe prison terms are needed. Laws should regulate cyber theft prosecution, including digital evidence collection and admissibility. Police and courts need cybercrime training. National governments should also ready to include IP protection in broader cyber security policies. These initiatives must outline police, IP, and regulatory collaboration. Police investigate and prosecute IP theft via cybercrime teams. Governments must also sponsor cybercrime and IP awareness efforts.

Encourage public-private alliances to use public and private strengths to fight cybercrime. Private companies' cutting-edge knowledge and resources, especially technology firms', can aid government endeavours. Public and private entities can collaborate to protect intellectual property more efficiently. Information-sharing mechanisms can assist public and private sectors share danger intelligence. These frameworks can help identify new cyber dangers and weaknesses to protect intellectual property. Governments may encourage

[14]Abdusatarov J, Turdialiev MA. The Issues of Intellectual Property in the Realm of Metaverse. Available at SSRN 4694628. 2024.

private companies to participate by offering tax advantages, grants, or recognition. Public-private collaborations can improve cyber security technologies through research and development.

We need to promote innovative cyber security technologies to stay up with fraudsters and protect IP in the digital age. The government should prioritise cyber security research and development, funding block chain, AI, and ML projects. These solutions improve IP security by improving threat detection, response automation, and data transaction protection.

Private companies, research groups, and universities get public cyber security innovation funding. Research grants, subsidies, and tax incentives promote cyber security solution development. To accelerate technology development, governments might create innovation centres or incubators for academics, entrepreneurs, and established firms. Promoting cyber security standards is crucial. Governments can develop and share cyber security best practices for different industries and business sizes to protect intellectual property. The private sector can be protected against cyber-attacks by governments forcing enterprises to follow cyber security best practices.

7. CONCLUSION

Digital IP theft prevention requires a multifaceted approach. The introduction warned of the financial and legal risks of intellectual property and cyber theft. International and state laws protect intellectual property, according to legal study. Famous case studies and cyber theft methods show that cyber threats are complex and widespread. IP theft was combated through administrative procedures, criminal prosecution, and civil lawsuits. Cyber risk reduction needs legal, technological, and organizational efforts. We explored jurisdictional issues, cyber threats, and the delicate balance between privacy and security to demonstrate how difficult it is to preserve intellectual property in the digital age. Businesses, governments, and international organisations must adapt quickly and take charge. R&D and flexible regulations are needed to stay ahead of hackers. Anti-piracy efforts require public-private cooperation worldwide. IP protection campaigns that teach about IP's value in today's digital world benefit businesses and consumers. To maintain global innovation, creativity, and competitiveness, cyber theft of intellectual property must be prevented for ethical and practical reasons. Everyone must collaborate to address these complex issues. Global collaboration and legal reform must be led by states. Private companies should employ industry standards and contemporary cybersecurity solutions to protect their assets. As cyber threats evolve, academic and research institutions must innovate. Everyone must join this collaboration.

Acknowledgment

The authors would like to express their gratitude to NIMS University Rajasthan, Jaipur, and professors who contributed to the research.

Credit Authorship Contribution Statement

Ankita Das[1] :Conceptualization, Methodology, Writing – Original Draft, Investigation.

Dr Manish Kumar Singh[2] : Data Curation, Formal Analysis, Writing – Review & Editing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

[1.] Badway EE, McGuinness C. The Criminal, Regulatory, and Civil Issues Surrounding Intellectual Property and Cybersecurity. *Brook. J. Corp. Fin. & Com. L.* 2019;14:181.

[2.] Taherdoost H. Legal, Regulatory, and Ethical Considerations in E-Business. In *E-Business Essentials: Building a Successful Online Enterprise* 2023 Sep 5 (pp. 379-402). Cham: Springer Nature Switzerland.

[3.] Sikder AS, Allen J. An In-depth Exploration of Emerging Technologies and Ethical Considerations in Cross-border E-commerce: A Comprehensive Analysis of Privacy, Data Protection, Intellectual Property Rights, and Consumer Protection in the context of Bangladesh. *International Journal of Imminent Science & Technology*. 2023;1(1):116-37.

[4.] Elpina E. Legal Challenges in Managing Intellectual Property Rights in Business Information Systems. *Jurnal Minfo Polgan*. 2024 Mar 12;13(1):270-7.

[5.] Hamza R, Pradana H. A survey of intellectual property rights protection in big data applications. *Algorithms*. 2022 Nov 8;15(11):418.

[6.] Mostert F. Digital tools of intellectual property enforcement: their intended and unintended norm setting consequences. In *Research Handbook on Intellectual Property and Digital Technologies* 2020 Jan 7 (pp. 553-576). Edward Elgar Publishing.

[7.] Babikian J. Navigating legal frontiers: exploring emerging issues in cyber law. *Revista Española de Documentación Científica*. 2023 Dec 30;17(2):95-109.
[8.] Allahrakha N. Balancing cyber-security and privacy: legal and ethical considerations in the digital age. *Legal Issues in the Digital Age*. 2023(2):78-121.
[9.] Segate, R. V. Securitizing Innovation to Protect Trade Secrets between "the East" and "the West": A Neo-Schumpeterian Public Legal Reading. *UCLA Pac. Basin LJ*, 2020;37:59.
[10.] Zonghui, L. In-Depth Interpretation of Intellectual Property Provisions in Chinese Cybersecurity Law. *China Legal Sci.*, 2021;9:106.
[11.] Malik JK, Choudhury S. *Law Relating to Cyber Crimes-Comparative Perspective*.
[12.] Wan V, Jiming Y. Torts and intellectual property in Industry 4.0: a comparative study of Chinese and American jurisprudence. *Peking University Law Journal*. 2021 Jan 2;9(1):111-42.
[13.] Gupta PK, Prasanna DV, Raghunath SS. How artificial intelligence can undermine security: an overview of the intellectual property rights and legal problems involved. *Applications in Ubiquitous Computing*. 2021:37-58.
[14.] Pringgohadi KA, Alvianti CA, Prasetyo MF, Taalungan LF. Legal protection for creators in copyright infringement through e-commerce. *Indonesian Journal of Law and Islamic Law (IJLIL)*. 2023 Dec 24;5(2):28-39.
[15.] Kashyap AK, Chaudhary M. Cyber security laws and safety in e-commerce in India. *Law & Safety*. 2023:207.
[16.] Abdusatarov J, Turdialiev MA. The Issues of Intellectual Property in the Realm of Metaverse. *Available at SSRN 4694628*. 2024