Journal of Intellectual Property Rights
Vol 30, November 2025, pp 708-717
DOI: 10.56042/jipr.v30i6.12793

Safeguarding Intellectual Property in the Digital Age through Artificial Intelligence

Chitra Saxena Nagpal[†], Anita Rao Raviwada and D Ganesh Kumar

School of Law, GITAM (Deemed to be) University, Visakhapatnam — 530 045, India

Received: 27th July 2024; revised: 5th May 2025

The landscape of Intellectual Property is facing various challenges with the onset of rapid digitalization. The current Intellectual Property (henceforth 'IP' in short) protection is dependent on the traditional law for enforcement and implementation of the Intellectual Property Rights (henceforth 'IPR' in short) Holder's rights, but the significant technological advancements and threats from cyberspace are highlighting threats and challenges towards IP protection, leading IP experts to delve into the ramifications of Artificial Intelligence (henceforth 'AI' in short) assisted problem-solving for IP related issues in cyberspace. Whereas the world is looking at a cohesive effort to ideally eradicate the issues that lead to cybersecurity breaches, a comprehensive and sustained effort towards addressing IP-related cyber threats is also being explored. At present, there are no tangent solutions for this. The authors attempt to address the potential of AI-assisted solutions to target IP infringements in cyberspace. By responsibly leveraging AI capabilities, we can fortify IP protection in the digital era and foster innovation and creation in a cyber-secure environment.

Keywords: Cyberthreat, Cybersecurity, AI, IPR, Digital, Internet

With the advent of new technologies and ushering in of the digital age era, the field of intellectual property has also been impacted in a substantial manner and is facing novel challenges towards Intellectual Property rights protection. The increase in the use of AI is also leading to its rise in the use of AI in the creation of content. Whether it is the rapid growth in access to digital platforms or one considers the instant availability of digital reproduction, various reasons are attributable to the attrition in the intellectual property protection ethos.[1] There is an increasing ease in downloading copyrighted material from a digital platform without the consent of the copyright holder, leading to monetary loss to the Intellectual Property rights holder. Furthermore, to magnify the issues, it is difficult for the copyright holder to hold an infringer accountable over the internet and initiate infringement action effectively through identification and enforcement[1]. With research and development in Artificial Intelligence (AI) systems making substantial advances and impacting different facets of everyday life, there are widespread open discussions amongst IP specialists on the profound impact that AI is going to usher in the field of IPR. Francis Gurry, the previous Director General of the World Intellectual Property Organization (henceforth 'WIPO' in short), commented in 2018 that AI was the new digital frontier capable of deep transformation due to its multifarious impacting capabilities.[2] Therefore, wherein traditional laws of IP Protection are found to have a lacuna towards effective enforcement of IP rights across cyberspace, it is possible to bring AI-assisted systems in place for the effective implementation of IPR protection in the digital age.

Cybersecurity and IP: Current Landscape

Cybersecurity refers to a bundle of such technologies and practices that are used to protect and defend any kind of software, data, or network from attacks or unauthorized use and access.[3] In a swiftly evolving digital world that is globally interconnected and creates, stores, and shares the IP assets of all businesses that have an online presence, new challenges have surfaced for the industry to protect their IP from cyber threats.

Cyber-attacks target not just national security but also businesses and unsuspecting individuals. From Crypto-currency scams to Investment scams to phishing scams across various metaverses, from ChromOs threats to Web 3 threats, the scare of cyber attacks is real. IC3 2021, financial scams are causing increasing yearly losses, with 2021 marking the scale

[†]Corresponding author: Email: jur.dgkumar76@gmail.com

up to $1,455,943,193.[4] The effect of cyber breaches is a potential threat not only to developing countries and least-developed nations but also challenges the digital superpowers who are still struggling with a cohesive global policy to counter an alarming rise in cyber attacks.[5] Amidst the myriad concerns related to cyber-criminal activity are the robust functioning of businesses and industries in a globalized world. As the digital era is swiftly unfolding through an internet boom, all IP activity remains at the mercy of cyber threats and casts a dampening effect on the protection granted to IPR holders through traditional law. With digital publicity rising in popularity for E-Commerce platforms, businesses functioning through the World Wide Web are easily accessible to any online surfer and have the potential for cybercrime. A web page is not dissimilar to a hard print of a book or magazine with audio-visuals that are copyrightable material, thereby requiring IP protection for the owner of the web page as well.[6]

Evolution of Digital IP Threats

Copyright Issues

Digital technology, especially AI, has fundamentally transformed the arena of copyright protection, bringing unprecedented challenges to the fore with regard to the prevention and control of rampant unauthorized reproduction. Copyright owners are facing unprecedented digital piracy through vast, sophisticated networks that are able to allow instantaneous distribution of copyrighted material across various global platforms. The primary IP domain that is being adversely impacted is Copyright, with infringements being observed rampantly throughout cyberspace. Since copyrighted material is now readily available online with easy access, people are freely downloading and using protected material for reasons other than fair use. India is no exception to this trend, with the legislative protection granted of the author's lifetime plus sixty years not being a sustainable protection tenure in the digital era. It is becoming increasingly difficult for the copyright holder to protect his/ her works from digital piracy, leading to financial losses due to downloading and sharing of their protected works without any permission/license. The ease with which people have access to and can replicate, share, and spread copyrighted content is a red flag for creators worldwide. The internet provides anonymity to the infringer and makes it nearly impossible for the copyright owner to initiate legal action against the offender. Moreover, various websites have mushroomed that are flagrant in their copyright violation. Recently, open-source software called Movie-web was shut down following copyright complaints by the majority of Hollywood production houses, such as Netflix, Disney, Warner Bros, Universal, and Paramount, with a message on their Discord posted by the owners of the software stating that they were shutting down due to court action. The argument that Movie-web advanced during the proceedings is that they were not hosting any pirated files; in fact, it was merely a search engine that connected its users to third-party content, much akin to how Google works.[7] It is pertinent to mention that though the streaming website shut down, the code with which the company built the app is still publicly available on GitHub for other software developers to build upon[7]. This one case cited above is merely a minute example of innumerable blatant copyright violations in global cyberspace.

With online content creation becoming easy and widespread amongst the population having access to the internet and AI tools, there are rampant violations of copyrighted works all across cyberspace. AI Prompts can create content that draws from huge data sets for which the AI company has not procured a prior training license. In 2023, Getty Images sued Stability AI Inc., claiming the respondents had scraped Getty's copyrighted images without any legal paperwork or permission and that Stability's AI Inc. had used their AI model that generates images known as Stable Diffusion for training on Getty's image.[8] Given the fact that with a tsunami of AI apps and systems being launched continuously and the fact that these are trained on available data sets on the internet, whether permissions are secured by the AI companies from those companies owning those data sets is again a pertinent issue.

Digital piracy is a burning problem that encompasses all the copyrighted works available online. Files that were earlier shared on peer-to-peer networks have now evolved into complex acts of digital theft, with online piracy having global networking.[9] Unauthorized downloading and sharing of infringed material are adversely impacting copyright owners. The existing legislation spanning various jurisdictions that cater to the protection of IP has found it increasingly challenging to cater to the rising online breaches and cyber threats. The anonymity offered to online copyright infringers

makes it a growing concern to effectively trace the infringers and bring them to justice, as they can be downloading copyrighted material sitting in any country, as long as the material is available online and it is accessible to the internet users since online operations provide no territorial limit.

Trademark and Domain Name Issues

Another IP domain that gets compromised due to such cyber threats is Trademarks and Domain names. A trademark determines the source of origin of goods and services in the minds of the user and differentiates one product from another in order to enable the customer to make informed choices. Tata, Samsung, Reliance, Apple, and Honda are such examples of trademarks, and with the companies having their presence on online platforms, it has become consistently easier for cyber users to access their trademarks and infringe upon them. Complexities have arisen in the digital age with regard to trademark protection, especially in online spaces. Trademark violations are evolving beyond traditional counterfeiting and developing into highly sophisticated forms of digital infringement.

Therefore, while businesses benefit from having an online presence, they are also at risk of exposing their vulnerability to cyber criminals who take advantage of the goodwill generated by the original company and manufacture counterfeit products to pass off as the original to unsuspecting users. E-commerce websites are flooded with fake products that sell first copies to the public who cannot differentiate between or are first-time users of the original product. One such example is luxury perfumes that are copied to such perfection that it becomes difficult for even an experienced nose to catch a fake.

Similarly, a domain name floated by a company is a readable address for a person to identify and connect with the company to its Internet Protocol address[6]. Domain names function at two levels, with '.net, .com, .org, .in' which are considered to be the first level domain, and the name chosen by the company is termed as the second level domain, such as Jaypore, Ellementry, Decornama, etc. Cyber-squatting has presently grown into a major concern, where domain names are registered that are similar to famous trademarks with mala fide intent, and thereafter frequently demanding ransom from established trademark owners or in the alternative, misleading consumers. Hijacking of the domain names presents another serious challenge, whereby cyber-attackers attempt unauthorized access into domain registrar accounts and try to transfer domain ownership, thereby leading to a severe loss of reputation and financial loss to the business. The exponential rise of e-commerce has also adversely impacted trademark protection, with fake products found rampant across online marketplaces. Due to various cyber issues such as cybersquatting, domain name hijacking, and meta tags[6], the intellectual property protection accorded to trademark owners and domain name holders is threatened. Indian judiciary has addressed these challenges in some landmark cases, such as Yahoo Inc (1999)[10], wherein the Delhi High Court gave protection to Yahoo's trademark against a deceptively similar domain name "yahooindia.com", as well as the case of Tata Sons (2013)[11], which fortified safety against domain name misuse. These cases spotlighted the need for trademark protection in India's digital space, giving impetus to the court's recognition of the requirement to adjust traditional trademark concepts to the digital environment.

In India, cases filed by Yahoo Inc.(1999)[10] and Tata Sons(2013)[11] are indicative of the issues faced by big companies with regard to cyber-squatting and domain name protection, respectively.

Trade Secret Violations

With technology coming of age, cyberspace has become the most viable medium of theft relating to Trade Secrets, which is also another form of Intellectual Property. WIPO's report states that business houses equate secrecy in trade to be at par with that of patents and other kinds of intellectual property.[12] However, increased cyber dependence paves the way for corporate espionage. In the current industrial landscape, where businesses are becoming progressively technology-dependent, vulnerability to cyberattacks has become widespread due to the cost-effectiveness and low conviction rates associated with corporate espionage. From the process of manufacturing Chinese Porcelain going back to the 18th century to Proctor Gamble obtaining Unilever's Shampoo secrets in 2001, industrial spying has a long history and is fast becoming an industry in its own right.[13] The 2010 cyber attacks on Google that found their origin in China and compromised Google's intellectual property through malware is another example of pivoting the fact that even the best software giants are not insulated against corporate

espionage[13]. Cybercriminals use sophisticated tools in their arsenal by exploiting modern-day technology in order to gain access to trade secrets that are being protected by industry.[14] Some forms of these cyberattacks that make a business prone to intellectual property theft are finding a weak link and introducing malware or ransomware, software vulnerabilities, insider threats, phishing, risks to cloud security, supply chain vulnerabilities, Distributed Denial of Service Attacks, and Advanced Persistent Threats wherein the modus operandi is to consistently target a business organization over a sustained duration.[15] Data breaches that happen as a result of cyber attacks not only lead to monetary losses for a company but can also adversely impact morale and reputation. FireEye's Red Teams tools were hacked in 2020, which is in itself an advanced cybersecurity system that can countermeasure cyberattacks.[16] This highlights the sophistication and expertise of cybercriminals who operate behind the veil of anonymity and leave a trail of economic loss in their wake.

AI Applications in IP Protection

Needless to say, the current legislative regime worldwide and in India is not adequate enough to fortify the industry against cyber attacks and cyber threats. The law providing IP protection is not able to keep pace with the rapid progression of technology-driven innovations. The superior tools and technological know-how at the disposal of the cyber attackers also impede the efforts of the authorities to bring them to task for IP infringements. International law is not in harmony with successfully tracing, identifying, and prosecuting the faces behind transborder cyber attacks. Even if cybercriminals get traced and identified, and proceedings against them are initiated, the penalties for IP infringement are not strict enough to act as a deterrence for future threats. Moreover, the ease with which information gets transferred and exploited online damages a company's IP within moments of its theft.

In order to combat the looming clouds of IP cyberattacks, legal theorists and industry experts are brainstorming on the various means and modes of making the law as watertight as possible. The flexibility that IP-infringing cyber actors get due to porous borders and weak transborder IP penalties needs to be fixed and made stronger to prevent and deter IP-related cyber attacks. With Artificial Intelligence fast gaining ground and pervading all sectors of industry and everyday life, it is but natural to look for solutions for AI-assisted mechanisms to help in IP protection in cyberspace.

AI systems train on huge data sets and can produce results in seconds using Machine Learning. When the world stands on the brink of Generative AI (hereinafter, 'GenAI' in short) , and computers are now fast gaining the ability to think and reason like humans but at a much-accelerated speed, this disruptive technology can also be employed to find novel solutions for targeting cyber criminals and securing the IP interests of the industry. However, abundant caution must be deployed in harnessing the power of AI for IP protection in cyberspace, as AI technology is a double-edged sword. Cybercriminals and hackers are also looking at AI to fuel their quest for IP infringement, which has the potential to wreak havoc on the economy through substantial and far-reaching IP thefts. Therefore, it is the need of the hour to synergize the potential of AI for the early detection and prevention of IP-related cyber threats and cyber attacks on a global scale and bring harmony in relevant laws across borders to tackle this issue effectively.

Legal Framework and Challenges

International Approaches

At the world level, countries are galvanized in efforts to protect intellectual property against cyber attacks. European Union is also looking at protecting the privacy of its citizens and has tightened the noose around data breaches by applying the General Data Protection Regulation (henceforth 'GDPR' in short) to any organization that is handling the personal data of Europeans, whether located in Europe or elsewhere. Their fine structure is substantial and will act as a deterrent to ensure that data privacy is considered sacrosanct by the organizations storing it.[17] As the regulations require data minimization, the organizations that are collecting data need to balance sufficient data vs. minimal data that is to be collected/ retained from European citizens while ensuring transparency and access to the citizens whose data is being stored[17]. The GDPR intersects with IP protection in various ways. GDPR's principle of data minimization requires organizations to seek a judicious balance between their IP protection requirements with data privacy rights. For example, when monitoring copyright through AI, companies need to collect only the data that is necessary for

infringement detection. Moreover, GDPR's strict cross-border data transfer clauses directly impact how organizations can monitor and enforce IP rights across various jurisdictions. In addition, GDPR's breach notification gives an early warning for potential IP theft, because many a times, IP breaches also include personal data compromise.

Moreover, the new Artificial Intelligence Act, though drafted to regulate the use of AI, is not found incompatible with GDPR.[18] The EU AI Act categorizes AI systems used for IP enforcement as being "high-risk," and involves strict checks for accuracy, rigor, and cybersecurity. The said classification ensures that the AI tools to be deployed for the detection of copyright infringement, trademark theft, or trade secret violations maintain high reliability. The Act mandates transparency in AI-infused IP protection systems, requiring organizations to document and account for their training data sources as well as their decision-making processes that have a bearing on content recognition systems used for copyright enforcement and AI tools used for monitoring online marketplaces for counterfeit products.[19] Both GDPR and EU AI ACT can be harmoniously constructed to provide a solid foundation for the protection of European IP in cyberspace. While GDPR handles personal data during IP enforcement activities, the AI Act ensures that automated IP protection systems continue with their accuracy and accountability. Organizations need to comply with both regulations whilst adopting AI-powered IP protection tools, thereby ensuring the dual objective of privacy preservation and efficient IP enforcement.

Along similar lines, the State of California has also introduced draft regulations on AI while dealing with the profiling of consumers and employees of an organization under the California Consumer Privacy Act (henceforth 'CCPA' in short)[20], coupled with efforts to bring about California Artificial Intelligence Transparency Act (henceforth 'CAITA' in short) that requires companies to tag AI generated content and also allows users to use AI tools to decide on whether the content is artificially generated. The said legislation is proposed as a Bill by Senator Becker and is in the process of being adopted by the Assembly.[21]

Indian Context

India has been a victim of the rising trend of cybercrimes, with a report highlighting that India faced the largest number of cyber attacks in Asia in the year 2022 and was second only to the United States on a global level.[22] The Indian E-Retail sector faced an unprecedented attack recently in 2024 when hackers called 'Shiny Hunters' stole customer information comprising women who had bought lingerie from Zivame and sold the data for cryptocurrencies. The details of the Zivame customers whose data was breached were later discovered on the dark web. The hackers claimed that the Zivame data theft was not new to them, and they had, on previous occasions, also hacked other companies, including Rentomojo and Linkedin.[23] Such attacks not only affect the business prospects of e-retail companies but also erode customer trust in the companies.

India's current legislative path to digital IP protection has journeyed through multiple frameworks, including the Information Technology Act 2000 and its subsequent amendments. However, these frameworks face struggles in keeping pace with the rapid evolution of digital threats. The enforcement mechanisms, especially while dealing with cross-border violations, suffer from technological complexities as well as jurisdictional limitations. While the Information Technology Act 2000 provides the fundamentals for addressing cybercrime, there remains a serious lacuna so far as IP protection is concerned. There remains a serious requirement for bringing in new legislation that caters to IP protection in cyberspace.[6]

The year 2023 marked significant progress in the country in both digital IP violations and digital data protection. The *Neetu Singh* v *Telegram case* (2023)[24] pinpointed a key development in digital copyright enforcement. The Delhi High Court, taking a stand that continuous copyright infringement required a trace of the infringer and that the foreign privacy laws could not take precedence over orders passed by an Indian Court, directed Telegram to disclose user information, thereby establishing platform liability and bringing forth a landmark precedent for digital copyright infringement.

New dimensions to IP protection were also introduced in the digital sphere with the Digital Personal Data Protection Act, 2023. While the primary focus of the Act was on personal data protection, the provisions of the legislation also delve into how organizations can ensure IP protection. Data processing and cross-border data transfers under the Act directly affect AI-powered IP protection systems and cybersecurity measures.[25]

Dr. V.K. Saraswat (Member, NITI Aayog) also gives a detailed report at the Cyber Security Conclave at Vigyan BHAWAN, New Delhi in 2018 and mentions the threat of theft of IP or data from sources like a) Nation States b) Cyber Criminal Organisations c) Terrorists, DTOs, etc., d) Hackers / Hacktivists while discussing enhanced tactical cyber security.[26]

With India keen to adapt to the changing global scenario and willing to adopt the latest AI technology, the stage is set for a radical approach toward efforts to solve the issue of rampant cyber attacks on different sectors, including e-retail businesses and companies found present in the Indian cyberspace.

In keeping with the spirit of fostering technological advances and weaving them within the nation's fabric, India should also explore IP enforcement mechanisms through AI-assisted systems in cyberspace. There is a direct connection between commerce and IP, and with rapid globalization and digitalization, changes have to be made in the present IP ecosystem to combat cyberattacks.

Recommendations for AI-Enhanced IP Protection

Technical Implementation

It is apparent that nations are realizing both the threat and potential of AI toward cyber security, and efforts are underway across various jurisdictions to bring out best practices for using AI in enhancing and ensuring IP protection across the vast expanse of cyberspace.

In addition, more novel methods and ideas are required to address the threat of cyber attacks using AI as a tool for effective implementation and protection of IP. With the passage of time, wherein cybercriminals are getting better funded and have access to cutting-edge technology to carry out attacks, AI-assisted cyber security is the way forward for countries and businesses to protect their valuable IP assets. For these cyber-security systems to function effectively, it becomes imperative that data protection principles are incorporated into AI systems at the very outset from inception to full lifespan to ensure full protective benefits.

AI System Training Requirements

With machine learning and deep mining algorithms becoming more complex and evolved over time, AI systems can be trained to detect cyber attacks, though at present, there has been a gap found in training AI on such huge labeled data sets with one solution arising as combining such labeled data sets with NetFlow data to enhance the training capabilities of AI.[27]

With new versions of malware flooding cyberspace that are capable of eluding the present detention systems, AI needs to be trained not only on historical and current data sets but on exhaustive data sets of the latest malware that can help AI learn and adapt for effective predictions and prevention of cyber attacks. Organizations should prioritize establishing robust frameworks involving data governance as AI language models train extensively on them. As deep learning is possible for advanced AI systems through these exhaustive data sets, impetus should be given to determine the preciseness and overall alignment to the threat perception of a specific company in question.[28] Therefore, though it is a challenge at present to find competent data sets for deep learning, organizations need to work towards training their AI systems on newer and comprehensive data sets that will help AI in helping them ward off any impending malware attacks and provide potent Intrusion Defence System.[29] Furthermore, extensive and regular training cycles on various types of IP violations, cyber attack signatures, and legitimate use cases in order to prevent false positives is required.

Through thorough training on external sources towards detention of threats, sensors, and logs, AI systems can train extensively to detect intrusive cyber attacks early and help maintain the sanctity of the cybersecurity ecosystem, which is a continuous process of training with updated data made available to AI algorithms.[30] This extensive training will last the lifetime of that particular AI system; the model will assist in securing cyberspace from attacks and ensure a safe environment for IP to thrive.

Integration with Existing Security Systems

A successful strategy to seamlessly integrate AI-powered IP protection tools with existing cyber-security infrastructure can be made possible by sharing real-time data between different security components whilst maintaining the integrity of the system. Organizations need to have clarity on protocols as to how AI systems interact with security tools, firewalls, and intrusion detection systems. The integration of all security components should include watertight mechanisms to ensure continued protection even if the AI system experiences initial issues.

Continuous monitoring of this integrative process is crucial to ensure success in the endeavour.

Allocation of Funds

More funds need to be allocated towards research and development of the latest versions of AI systems with a focus on training AI algorithms in cloud security. A well-planned blueprint is the need of the hour by skilled software experts to train AI from the very outset and make the AI systems compatible with the latest developments in cloud security.[31] A well-thought-out strategic allocation of financial resources across critical areas and budgeting for operational costs post intial implementation is crucial to ensure implementability long term.

Data Governance Frameworks

The data governance framework needs to be fortified in order to lay the foundation for effective AI-powered IP protection. Organizations need to establish effective and clear protocols for data collection, data storage, and data usage in AI training. Quality assurance of data, regular auditing of the data, and policy compliance are some mechanisms that can be deployed towards this objective. The sourcing and processing of data need to have transparency. Additionally, data security needs to be fortified to make it impenetrable against unauthorized access, transfer or manipulation.

Accountability of AI Companies

Moreover, the authors are of the opinion that AI companies that are creating systems and programs to assist in cybersecurity should be made accountable to their end users by way of introducing penal provisions in their licensing agreements. This will ensure that in case of any cyber breach, while the AI system is employed, the company behind the AI detention is held legally accountable. This will ensure that the AI developers delve deep into ensuring the system's robustness before making it available to businesses for cybersecurity and protection of their precious IP assets. Defending itself from cyber threats is crucial for a business to thrive. Moreover, as seen from Zivame's case, in an event when their data gets breached, the company is impacted in terms of its reputation and also loss of faith amongst its customers. Therefore, it is imperative that the cyberspace where the businesses operate must be made secure and robust to withstand any targeted attack on their intellectual property.

Legal and Policy Measures

Legislative Framework Enhancement

Existing IP laws require specific modernization to effectively address the issue at hand. Suggestions include amendments to prevalent copyright, trademark, and patent laws to recognize AI detection and enforcement mechanisms. Legislature needs to bring about fresh laws or amendments to existing laws to establish clear parameters in order to address the validity of AI-detected violations as per the law of evidence and establish standards for verification and enforcement.

Platform Liability Rules

Taking a leap from the Telegram judgment, novel legal enactments should clearly earmark the scope of liability for platforms using AI for IP protection towards platform responsibilities in cases of false positives or incorrect enforcement actions. In addition, mandatory reporting of significant AI enforcement actions will ensure transparency and accountability.

International Cooperation and Cross Border Mechanisms

International treaties require updation towards facilitating AI-powered IP protection across jurisdictions, including standardized protocols for acknowledging and sharing AI-detected violation data, mutual recognition of AI-generated evidence between nations, harmonized mechanisms for cross-border cooperation, specialized dispute settlement mechanisms etc.

AI Applications in Law Enforcement and Commercial Sector: Implications for IP Protection

The advent of AI in law enforcement is assisting the law enforcement in effective policing, and the software can be tweaked and deployed in digital space to help in nabbing cyber-criminals. For instance, AI facial recognition was used by the Chinese police in nabbing a man wanted for economic crimes from a concert that had close to sixty thousand attendees. Reports say that the nabbed person looked completely taken by surprise (Shelton, 2018)[32]. The facial recognition technology being used by the London Metropolitan Police is also helping the department in crowd contro.[33] In other such instances, the Los Angeles Police Department uses AI to predict potential crime hotspots and takes preemptive measures to ensure that area remains crime-free.[34] It is the potency of AI to identify and pinpoint on a

specific individual in a gathering of thousands, and the same capability can be employed in identifying cyber criminals in the digital realm.

Similarly in the world of business, companies are employing AI tools to do business the smart way. One such example is the e-commerce platform -Alibaba - which upgraded its IP protection by being able to pinpoint fakes in an expeditious manne.[35] Along similar lines, Amazon utilizes 'Project Zero' that is a machine learning programme geared towards brand protection by identifying counterfeits.[36] YouTube is also using AI to detect copyright violations.[37] Therefore, it is observed that companies are effectively employing AI tools and Machine Learning Models to detect counterfeits effectively and the same technology can be also applied to detect cyber-crime after making it suitable for digital protection.

The successful use of AI in law enforcement and commercial applications reiterates its scope for IP protection in cyberspace. Similar to facial recognition wherein AI can identify individuals in large crowds, similar pattern recognition algorithms can be formulated to predict digital signatures of IP theft across various and vast networks. AI's predictive capabilities evidenced in crime prevention can be re-directed towards anticipating potential IP infringement patterns and towards identifying vulnerable online assets. In addition, the success rate of AI in identifying counterfeit products and pinpointing copyright violations provides an established framework for broader IP protection applications towards monitoring, tracking, tracing, predicting IP infringements.

Other Suggestions

Business organizations that are keen to adopt AI-empowered cybersecurity measures to protect their IP should make a note of certain suggestions for effective implementation and optimal utilization of the AI systems. It is essential to go for a planned strategy while incorporating AI-assisted cyber protection and keeping the company's overall objectives in consideration. A clear roadmap to implementation will help determine the specific usage that the company desires from the AI system, the data sources required for the task, the desired infrastructural requirements as well as the criteria for establishing the success of the AI system that is being used to protect IP in cyberspace.[38]

A deep analysis of previous cyber attacks will also help develop a fortified AI system that is capable of warding off any perceived threats through accurate prediction and diagnostics.[39] Software professionals need to be trained and upskilled towards developing and integrating the most advanced version of anti-theft AI systems to ensure the integrity of an AI-assisted cyber security system.

Working in close association with industry experts and similarly aligned stakeholders will help ensure a watertight AI system that can enable a strict cyber-secure environment for trade and industry to flourish. If similar attacks are identified and isolated, more skilled professionals at work can develop a better strategy for effective AI-powered defense mechanisms.[40] Predictive AI can be a potent saviour from cyber-attacks if the modus operandi of previous such cyber intrusions is researched thoroughly.

Various nationals from countries for whom English is not their primary language are often found to be either victims of cybercrime or perpetrators of cyber attacks; AI can also help the industry in cutting across multilingual hurdles with its algorithms having the capability for swiftly mining threat intelligence in various languages.[22] This gives an edge to AI-assisted cyber protection systems over that of human capability and functionality. To achieve this goal, WIPO stresses the sharing of resources by nations to protect their IP and has launched a sophisticated tool for neural machine translation called WIPO Translate that can deep mine large data sets to fuel AI systems for effective IP administration.[2] The growing need of the hour necessitates the development of more such tools that can look into aspects of protecting IP from cyber threats.

Conclusion

IP innovations often feed off Big Data and lead to a technological boom in intellectual assets. However, the very technologies that facilitate growth in IP innovations in cyberspace also leave a business vulnerable to cybercrime.[41] Today, the digital footprint of IP in cyberspace is vast, and effective mechanisms are required to help protect the IP assets of a company in the digital world. Adopting new technologies is a double-edged sword, and businesses need to balance out their interest with the involved risks to arrive at a fortified system to ensure the protection of their IP from cyber attacks. With GenAI bringing about radical changes in how nations and economies functioned previously, this disruptive technology needs to be harnessed mindfully and worked to the advantage of the industry. Moreover, a

new impetus towards sharing resources to combat cyberattacks and training a large workforce of skilled professionals to develop and research this field will also help enhance cybersecurity in the business world. With the world evolving into a global village, digital interconnections are ripe. Cumulative efforts from governments and industry are required to translate the vision of a safe, innovation-driven cyberspace into ground reality by utilizing AI-assisted systems to ensure the cyber protection of IP assets.

Traditional legal frameworks struggle to provide solutions to the complex challenges faced by the intersection of intellectual property protection and cybersecurity in the digital era. Sophisticated cybercriminals target vulnerable IP assets, and copyright violations, trademark infringements, and trade secret theft all seek innovative solutions to the problem at hand. AI is emerging as a potent solution to these issues, having powerful capabilities for preventing cyber attacks and also enforcing IP rights. The successful deployment of AI in law enforcement and commercial applications has ably demonstrated AI's potential for providing comprehensive IP protection in the cyber world. However, pursuing this pathway requires careful consideration of technical requirements, strong legal and policy frameworks, and international cooperation. As businesses, organizations and countries try to grapple with rapidly evolving online threats, the strategic use of AI-powered systems will become essential in safeguarding IP. The future of a robust IP environment lies in endeavouring to strike an effective balance between technological innovation and legal compliance, and in ensuring that AI systems fortify rather than compromise the integrity of IP rights in the digital space.

References

1 Torous M, Intellectual property rights in the digital age: challenges and solutions, *Journal of International Business Research*, 23 (1) (2024).

2 Gurry F, Artificial intelligence and intellectual property: An interview with Francis Gurry (2018), available at https://www.wipo.int/wipo_magazine/en/2018/05/article_0001.html.

3 Kaur R, Gabrijelcic D & Klobucar T Artificial intelligence for cybersecurity: Literature review and future research directions, *Information Fusion*, 97 (2023) 101804, ISSN 1566-2535, available at https://www.sciencedirect.com/science/article/pii/S1566253523001136.

4 McAfee Report, (2023), McAfee 2023 threat predictions: Evolution and exploitation, available at https://www.mcafee.com/blogs/security-news/mcafee-2023-threat-predictions-evolution-and-exploitation/.

5 Shackelford S J, Protecting intellectual property and privacy in the digital age: The use of national cybersecurity strategies to mitigate cyber risk, *Chapman Law Review* (2016), Available at https://elsevier-ssrn-document-store- prod.s3. amazonaws.com/15/07/23/ssrn_id2635035_code1195469.pdf.

6 Jaybhaye A S, Cyber law and IPR issues, *Bharti Law Review*, (April-June) (2016) 166, available at https://docs.manupatra.in/newsline/articles/Upload/19A86CE4-2FBD-432B-B166-AFBA9087A834.pdf.

7 Ernesto Van der Sar, 'Movie-web' domain shut down by hollywood complaint (2024), available at https://torrentfreak.com/movie-web-domain-shut-down-by-hollywood-complaint-240224/.

8 Brittain B, Getty images lawsuit says Stability AI misused photos to train AI, *Reuters*, (2023), available at www.reuters.com/legal/getty-images-lawsuit-says-stability-ai-misused-photos-train-ai-2023-02-06/.

9 Prasanna S & Lavanya P, Navigating the digital age: Challenges in Indian Intellectual Property Rights Law, ILE Lawletter, 1 (1) (2023) 34, APIS – 3920 – 0058 | ISBN - 978-81-964391-3-2.

10 *Yahoo! Inc* v *Akash Arora & Anr*, 1999 (Delhi High Court); 1999IIAD (DELHI) 229, 78(1999)DLT285 Available at https://indiankanoon.org/doc/1741869/.

11 *Tata Sons Ltd & Anr* v *Arno Palmen & Anr* (Delhi High Court), AIR 2013 (NOC) 232 (DEL.), 2013 (1) ADR 115, (2013) 114 CORLA 10, (2013) 199 DLT 437 Available at https://indiankanoon.org/doc/27722663/.

12 Hull J, Protecting trade secrets: How organizations can meet the challenge of taking "reasonable steps", WIPO Magazine, 5 (2019, available at https://www.wipo.int/wipo_magazine/en/2019/05/article_0006.html.

13 Vashisth A & Kumar A, Corporate espionage: The insider threat, *Business Information Review*, 30 (2) (2013) 83, https://doi.org/10.1177/0266382113491816.

14 Lunker D & Isiri S D, Protecting trade secrets: Need for law amidst growing e-Espionage, NLUI-IP Journal, (2020), Blog, available at https://csipr.nliu.ac.in/technology/protecting-trade-secrets-need-for-law-amidst-growing-e-espionage/.

15 Khanna P, Emerging cybersecurity chreats and countermeasures: A comprehensive review, *International Journal of Computer Research and Technology*, 11 (7) (2023) 609, available at https://ijcrt.org/papers/IJCRT2307659.pdf.

16 Prey R C, Applebaum S L & Traurig G, Protecting your most valuable intellectual property from cyberattacks, Westlaw *Thomas Reuters* (2021).

17 Bergelt K, Cybersecurity innovation and the patent landscape, *Security*, (2019), available at www.securitymagazine.com/articles/90106-cybersecurity-innovation-and-the-patent-landscape.

18 Sartor G, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, STUDY, Panel for the Future of Science and Technology, European Parliamentary Research Service, Scientific Foresight Unit (STOA) PE 641.530 (2020).

19 Assets Ey (2 February 2024) The European Union Artificial Intelligence Act latest developments and key takeaways, https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/ai/ey-eu-ai-act-political-agreement-overview-february-2024.pdf.

20 McMenemy S J, Nalty S P, Perry B W & Zagger Z V, California privacy protection agency releases first draft regulations of AI and other automated decision technology, *Ogletree Deakin* (2023), available at https://ogletree.com/insights-resources/blog-posts/california-privacy-protection-agency-releases-first-draft-regulations-of-ai-and-other-automated-decision-technology/.

21 Becker J, Senate advances ground breaking transparency bill empowering consumers to identify AI generated content, (2024), available at https://sd13.senate.ca.gov/news/press-release/may-21-2024/senate-advances-groundbreaking-ai-transparency-bill-empowering.

22 Chatterji S, Krishna H, Misra S & Varma P, Cybersecurity laws and regulations generative AI & cyber risk in India 2024 (I) ICLG.com, (2023), available at https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/02-generative-ai-and-cyber-risk-in-india.

23 Pandagle V, The Cyber Express, (2024), available at https://thecyberexpress.com/zivame-data-breach-details-put-on-sale/.

24 *Neetu Singh and Another* v *Telegram FZ LLC and Others* [2023] CS(COMM) 282/2020 (Del HC).

25 Qureshy A A, Cross-border data transfer requirements under India DPDPA, Securiti, (2024), https://securiti.ai/cross-border-data-transfer-requirements-under-india-dpdpa/

26 Saraswat V K, Cyber Security, Cyber Security Conclave at Vigyan Bhavan Delhi, (2018) https://www.niti.gov.in/sites/default/files/2019-07/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf.

27 Buczak A L & Guven E, A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18 (2) (2016) 1153, available at https://doi.org/10.1109/COMST.2015.2494502.

28 Sarker I H, Furhad M H & Nowrozy R, AI-driven cybersecurity: An overview, security intelligence modeling and research directions, *SN Computer Science,* 2 (2021) 173, available at https://doi.org/10.1007/s42979-021-00557-0.

29 Khraisat A, Gondal I, Vamplew P & Kamruzzaman J, Survey of intrusion detection systems: Techniques, datasets and challenges, Cybersecurity, 2 (1) (2019) 1, https://doi.org/10.1186/s42400-019-0038-7.

30 Xin Y, Kong L, Liu Z, Chen Y, Li Y, Zhu H & Wang C, Machine learning and deep learning methods for cybersecurity, *IEEE Access*, 6 (2018) 35365, available at https://doi.org/10.1109/ACCESS.2018.2836950.

31 Nedunoori V, AI in cloud security: Transformative potentials and pressing challenges, India AI (2024), available at https://indiaai.gov.in/article/ai-in-cloud-security-transformative-potentials-and-pressing-challenges.

32 Shelton T, Facial recognition technology spots wanted man in crowd of 60,000 Chinese concert-goers. ABC News (17 April 2018), https://www.abc.net.au/news/2018-04-17/chinese-man-caught-by-facial-recognition-arrested-at-concert/9668608.

33 Metropolitan Police, https://www.met.police.uk/advice/advice-and-information/fr/facial-recognition-technology/.

34 Lapowsky I, How the LAPD uses data to predict crime, Wired (2018), https://www.wired.com/story/los-angeles-police-department-predictive-policing/.

35 Megget K (2017). Alibaba introduces 'speedy' IP protection platform, Securing Indistry, https://www.securingindustry.com/clothing-and-accessories/alibaba-introduces-speedy-ip-protection-platform/s107/a5343/.

36 Tech2 News Staff Amazon's Project Zero aims to let brands and machine learning tackle counterfeiting, First Post (1 March 2019) https://www.firstpost.com/tech/news-analysis/amazons-project-zero-aims-to-let-brands-and-machine-learning-tackle-counterfeiting-6177791.html.

37 Van de Sar E, YouTube Content ID Copyright Claims Increased 25% in a Year, Torrent Freak (29 February 2024), https://torrentfreak.com/youtube-content-id-copyright-claims-increased-25-in-a-year-240229/.

38 Protiviti, Global Business Consulting (2024), available at https://www.protiviti.com/us-en/whitepaper/enabling-enterprise-ai-adoption.

39 Kaloudi N & Li J, The AI-based cyber threat landscape: A survey, ACM Computing Surveys (CSUR), 53 (1) (2020)1, available at https://doi.org/10.1145/3372823.

40 Pitropakis N, Panaousis E, Giannetsos T, Anastasiadis E & Loukas G, A taxonomy and survey of attacks against machine learning, *Computer Science Review*, 34 (2019) 100199, https://doi.org/10.1016/j.cosrev.2019.100199.

41 Basuchoudhary A & Searle N, Snatched secrets: Cybercrime and trade secrets modelling a firm's decision to report a theft of trade secrets, *Computers & Security*, 87 (2019) 101591, ISSN 0167-4048.