Scope
Volume 15 Number 02 June 2025

Artificial Intelligence Based Strategic Framework for Protection Against Counterfeiting in India

Avinash Mandal
Final Semester Student of BBA-LLB at Jindal Global Law School,
O.P. Jindal Global University, Sonipat, India

Abstract: The intersection of Artificial Intelligence (AI) and IPR in India presents both promising opportunities and significant challenges. Two distinct issues are being debated widely: (1) adapting legal frameworks to accommodate AI-generated content and assets' IP Rights (IPR), addressing ownership issues, and (2) leveraging AI for efficient IPR protection. The research article sets out to evaluate issue number 2 - more specifically, how various AI-driven solutions could be leveraged to address the multifaceted challenges infringing the IPR (IP rights) and brand, namely, illicit trade (counterfeiting, smuggling, diversion, infringement, etc.). The objective is to deliver an exhaustive examination of brand protection, the detrimental effects of infringement and counterfeiting on brands and their clientele, and the transformative effect of developing AI-driven solutions on IP safeguarding. Specifically, this paper advocates the adoption of a unique and effective IPR protection and anti-counterfeiting action framework, involving an integrated multi-layered approach: (a) AI-Driven Technology Layer, (b) AI-Driven Legal Tech Layer and (c) AI-Driven Governance Layer. This unique approach, together with increased collaboration among stakeholders — which includes industry players, brands, consumers, and law enforcement — enables them to navigate the intricacies of handling challenges in IPR management in the digital, on-demand, always-connected era. This research paper also seeks to promote policies that harmonize innovation utilizing risk management, societal interests, and ethical considerations, thereby cultivating an atmosphere that supports creativity while safeguarding IP rights.

Key Words: Brand Protection, Artificial Intelligence (AI), Machine Learning (ML), Anti-Counterfeit, Data Privacy, Data Security, Intellectual Property Rights (IPR), Anti-counterfeit, Cloud Computing, Legal Tech

1. Introduction

Illicit trade, which includes counterfeiting, smuggling, diversion, and infringement, is still a major issue for consumers and businesses worldwide. To secure what businesses

value most—customers, brand identity, reputation, and revenue—a well-thought-out IP and brand protection programme was the most important compared to ever due to the growing amount of counterfeit goods being trafficked worldwide and infiltrating various supply chains.

India had₹2.6 trillion of spurious goods traded in FY 2019-20 [1], and it is impacting more than 20 industries in various ways – some of which are narrated briefly in this section.

1.1 Anti-counterfeiting: A key strategic pillar of the IPR infringement protection umbrella

IPR infringement protection is the umbrella under which copyrights, patents, trademarks, and anti-counterfeiting are legally shielded, leveraging the broad framework that encompasses:

- Legal ownership of IP (registration, portfolio management)
- Detection and enforcement against unauthorized use
- Remedies (takedowns, lawsuits, customs seizures)

1.2 Anti-Counterfeit Measures under Unified IPR Infringement Protection Strategy

Anti-counterfeiting is the "enforcement and deterrence arm" that directly combats the physical and digital threats of counterfeits and is focused specifically on identifying and eliminating fakes or unauthorised copies of a genuine product. These are most closely tied to trademark infringement (fake logos, packaging) and copyright infringement (fake media or software) and sometimes involve patents (e.g., knockoff products using patented designs or mechanisms).

1.3 Objectives of this Research Paper

Brand protection is necessary to prevent tangible losses (eroded revenue: damaged reputation, eroded consumer trust leading to lost customers) and intangible losses (negative reviews, social media complaints, diminished brand loyalty, demoralised employees resulting in stifled creativity, and potentially legal expenses). Protecting the brands offline and online in 2025 and beyond is a complex process that incorporates more than just the policing of online marketplaces [2].

In the current world of instant access and constant connectivity, there is a surge in product offerings along with a significant rise in illegal trading and IP rights violations concerning these items. Traditional legal methods often find it hard to protect IP rights effectively due to the rapid changes in the environment—such as an overwhelming amount of data, documents, and digital media (audio, video, andimages), along with swiftly evolving laws and regulations that aim to keep up with the changing landscape, including data privacy issues and cybersecurity challenges, as well as ethical concerns around AI usage in some situations.

This research paper seeks to fill this void by promoting the use of AI and ML technologies that can quickly adapt to the changing factors impacting IP rights and enhance the legal protection mechanisms for these rights [3]. Specifically, this paper advocates the adoption of a unique and effective anti-counterfeiting action framework involving an integrated multi-layered approach:

(a) AI-Driven Technology Layer: (i) Blockchain-Based "Clean Supply Chain", (ii) Physical product safeguards, (iii) Digital/online strategies,
(b) AI-Driven Legal Tech Layer
(c) AI-Driven Governance Layer.

Furthermore, the research advocates for a holistic approach to IP protection that considers various perspectives and addresses ethical, privacy, and security challenges by bringing together government bodies, industry players, academic institutions, and other stakeholders.
Lastly, the paper highlights the significance of educating and raising awareness about counterfeiting amongst stakeholders—including industry participants, brands, consumers, and law enforcement—so that they can navigate the complexities of IP rights protection in the digital era.

2.0 Anti-Counterfeit Legal Framework in India

2.1 Anti-counterfeit measures in **India,** across legal frameworks, enforcement agencies, and online commerce regulation, are given in Table 1.

Table 1: Anti-Counterfeit Legal Framework in India

Category	Anti-counterfeiting framework in India
Legal Basis for IP Enforcement	• Trademarks Act, 1999 • Designs Act, 2000 • Geographical Indications of Goods Act, 1999 • Copyright Act, 1957
Consumer Protection Law	• Consumer Protection Act, 2019 (CPA) • Legal Metrology Act, 2009 • Drugs and Cosmetics Act, 1940 • Food Safety and Standards Act, 2006
Online Counterfeits Regulation	• Consumer Protection (E-Commerce) Rules, 2020 • Information Technology Act, 2000
Criminal Enforcement	• Trademarks Act, 1999 • IPC Sections 420, 482, 486 (cheating and counterfeiting)

Category	Anti-counterfeiting framework in India
Customs Role	• Customs Act, 1962 • IPR (Imported Goods) Enforcement Rules, 2007
Civil Remedies	• Injunctions, damages, and accounts of profits under IP laws and CPA
Product Safety Recalls	• The Bureau of Indian Standards (BIS) handles certification. • No formal central recall system for all categories
IP Enforcement Tools/Portals	• ICEGATE (Indian Customs) IPR Module • IP India portal • Recent use of blockchain in pharma (Track & Trace)
Cross-Border Cooperation	• Limited but increasing via WIPO, INTERPOL, and bilateral MoUs. • Follows WTO TRIPS commitments
Centralized IP Customs Record	• ICEGATE portal

2.2 Key Anti-Counterfeit Law Enforcement Agencies in India

In India, anti-counterfeit law enforcement involves a combination of central and state agencies that operate under various ministries and departments. These agencies are responsible for preventing, investigating, and prosecuting the manufacture, sale, and distribution of counterfeit goods. The key agencies involved are given in Table 2.

Table 2: Key Anti-Counterfeit Law Enforcement Agencies in India

Agency	Role in Anti-Counterfeiting	Governing Ministry
Police Departments (State CID/Crime Branch)	Investigate counterfeit goods cases under IPC, Drugs and Cosmetics Act, Trademark Act, etc.	Respective State Governments
Central Bureau of Investigation (CBI)	Handles complex IP-related crime, especially if interstate or international.	Ministry of Personnel, Pension & Public Grievances
Directorate of Revenue Intelligence (DRI)	Intercepts counterfeit imports at borders, especially luxury goods, electronics, and FMCG.	Ministry of Finance

Agency	Role in Anti-Counterfeiting	Governing Ministry
Customs Department	Seizes counterfeit goods at ports and airports under IPR (Imported Goods) Enforcement Rules, 2007.	Department of Revenue, Ministry of Finance
Drug Control Authorities (CDSCO + State Drug Controllers)	Enforce anti-counterfeit measures for medicines and healthcare products.	Ministry of Health and Family Welfare
Food Safety and Standards Authority of India (FSSAI)	Acts against counterfeit and adulterated food items.	Ministry of Health and Family Welfare
Legal Metrology Department	Cracks down on counterfeit or mislabelledprepackaged consumer goods.	Ministry of Consumer Affairs
Economic Offences Wing (EOW)	Investigates financial fraud, including counterfeiting-related financial crimes.	State Police Forces
Enforcement Directorate (ED)	Prosecutes money laundering linked to counterfeiting under PMLA.	Ministry of Finance
Intellectual Property Rights (IPR) Cells	Operate within the state police or as special task forces for brand protection.	State Governments / IP Division
Bureau of Indian Standards (BIS)	Investigate the counterfeit use of ISI marks and certify quality compliance.	Ministry of Consumer Affairs
Telecom Enforcement Resource & Monitoring (TERM) Cells	Tracks counterfeit mobile handsets (IMEI issues).	Ministry of Communications

Types of Goods Commonly Targeted by Enforcement [4]

Counterfeiting is most prevalent in apparel (31%), FMCG (28%), and automotives (25%), which are the top segments where consumers came across a counterfeit product,

followed by pharmaceuticals (20%), consumer durables (17%), and agrochemicals (16%).

2.3 Reform in Law: In the nascent stage

However, while the patent application numbers are on the rise, the industry has expressed concerns over the patent prosecution and examination regime in India.A few recent developments in this regard are mentioned below:

(a) In the report "Unpacking India's IP Ecosystem", the industry body NASSCOM [5], advocates for procedural changes, like fixing the time limit to file a pre-grant opposition and introducing clarity and specific guidelines concerning technology patents.

(b) MeitY published"Report on AI governance guidelines development" [6] recently. which has received more than 100 suggestions to date, which prompted NASSCOM to opine that AI model training on copyrighted data needs public review as well as guidelines from the government to address broader concerns related to the training of AI models and AI-generated outputs.

(c)CoRE-AI, a policy think tank which is a multi-stakeholder initiative on AI, emphasised that privacy and transparency need to be balanced – while full data set transparency may not be feasible due to proprietary considerations and extremely high levels of competition, a high-level summary of data sets used for training should be possible [7].

3. AI-driven anti-counterfeiting framework

3.1 AI-Driven Technology Layer

3.1.1 AI-Driven Blockchain-Based "Clean Supply Chain" for Track & Trace

Supply chains have various challenges, including (1) building trust among multiple stakeholders; (2) cyberattacks; (3) cargo theft; and (4) the introduction of counterfeits, among others. The concept of a blockchain-based supply chain system, encompassing the flow of physical items, information, blockchain records, and their updates, as well as the verification and matching of crucial information within blockchain smart contracts, is elucidated in Fig. 1. To create an effective and dependable supply chain management system, manufacturers must utilise advanced technologies, such as blockchain, IoT, and AI. An AI, IoT, and blockchain-enabled data-driven clean supply chain is the most effective solution to the aforementioned challenges. Blockchain is fundamentally a decentralised and safeguarded distributed digital ledger that securely and transparently records transactions, which are immutable, traceable, auditable and interoperable. Thesedistinguishing characteristics ofblockchain, along with reduced costs and improved efficiency (by streamlining processes, automation through smart

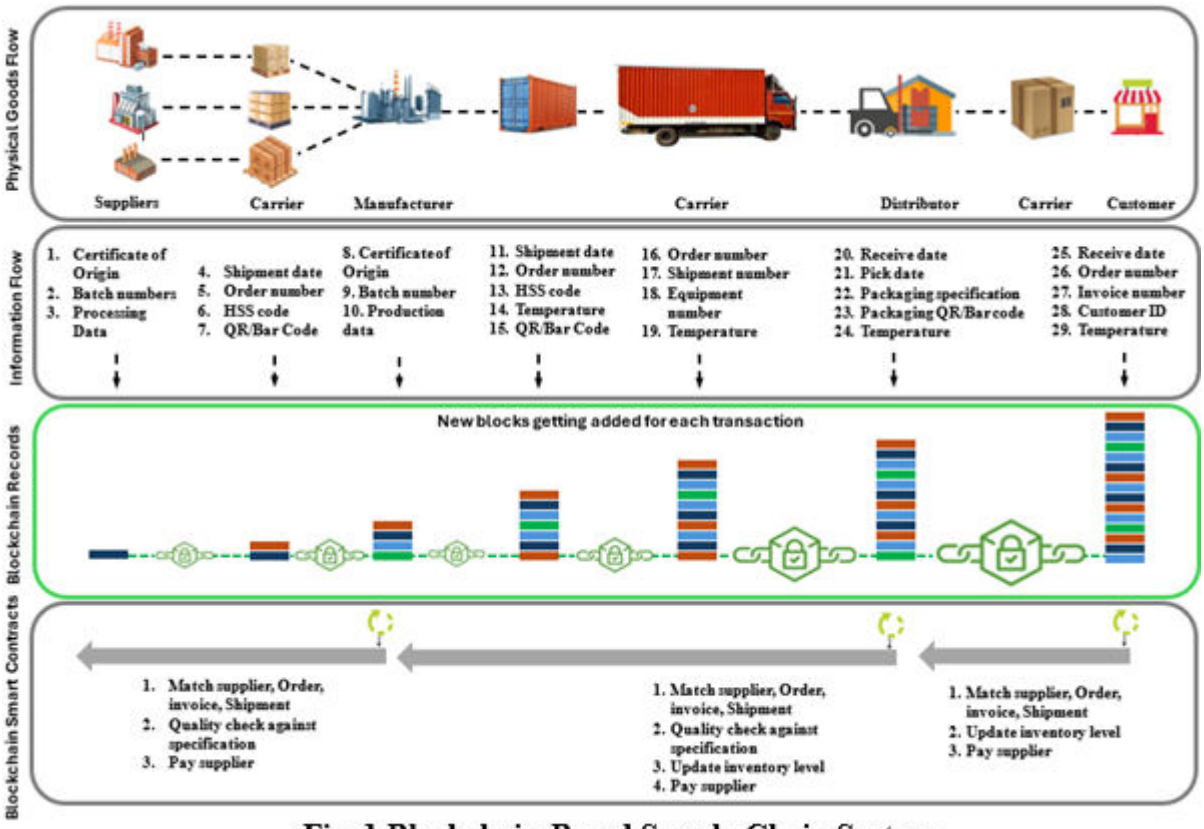

Fig. 1 Blockchain-Based Supply Chain System

contracts and eliminating intermediaries), blockchain, foster trust and collaboration amongst the supply chain players [8].

How AI Tools help :

An AI-driven blockchain-based supply chain, with serialization

- AI algorithms can analyse data from the supply chain (e.g. for Predictive Analytics, Automation of routine tasks, NLP based document verification, Straight through Process without human intervention – reducing error and frauds as well as cost)
- Blockchain and serialization provide real time tracking, prevention of thefts, frauds and injection of counterfeits, traceability, digital smart contracts with digital audit trails, accurate inventory data and overall cost reduction.

3.1.2 Physical Product Safeguards [9]

Anti-counterfeiting technologies for safeguarding physical products encompass a range of techniques and methodologies employed to prevent, identify, and authenticate products, thereby safeguarding OEM brands and consumers from fraudulent goods. These physical anti-counterfeiting items are applied on product packaging, the product itself, or both (please refer to Fig. 2) to protect products from directand indirect patent infringement, tampering, grey market sales, diversion, and other illicit activities. There

is no universally ideal anti-counterfeit approach, as it differs depending on the specific circumstances. In most instances, the most effective solution involves integratingseveral technologies, rendering cloning exceedingly costly and practically unfeasible for large-scale production[10].

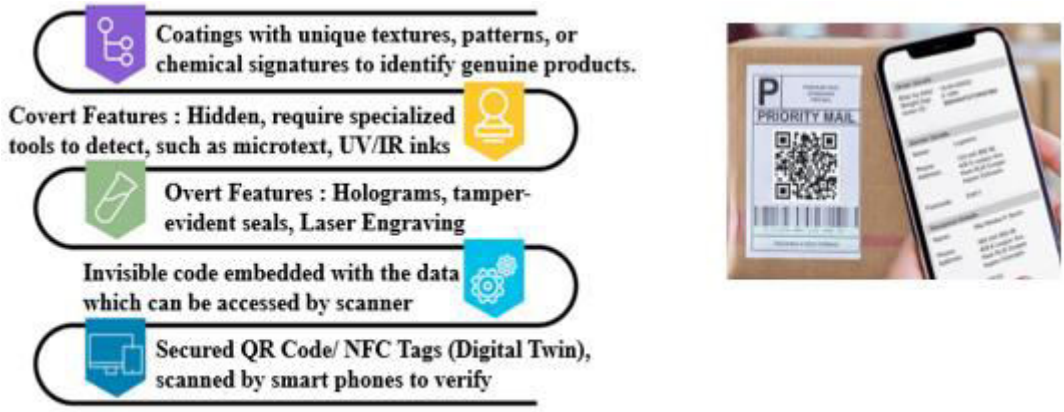

Fig. 2 Anti-Counterfeit Technologies for Physical Product

How AI Tools help :

Smart Packaging Authentication

- AI can power mobile apps that verify products via visual inspection (e.g., authenticating by scanning digitally certified QR code using a phone camera).
- Deep learning models can identify fake packaging based on high-resolution image analysis, even if counterfeits are visually similar.

3.1.3 Digital/Online strategies

These technologies are leveraged to supplement physical product authentication technologies, as well as for online IPR infringements like – Cybersquatting, Online/ TV/ Social/ Digital Media Impersonation (deepfake),online copyright infringement (unauthorised distribution, reproduction, or presentation of a secured copyright, literary works, photographs, videos, and other media), etc.

(a) Brand Monitoring and Enforcement

i. Monitor e-commerce sites, social media, forums, and the dark web.
ii. Detect unauthorised sellers, fake listings, and counterfeit advertisements.
iii. Actively report infringing content and request takedowns.

(b) Customer Education – Educate users on:

i. How to verify using serial numbers or authentication apps.
ii. Identifying real vs. fake products and reporting the same
iii. Identifying real vs. fake products and reporting the same

How AI ToolsHelp:

Customer Feedback Analysis

- Use NLP to analyse product reviews, complaints, or return reasons across channels.
- Identify and recognize counterfeits (e.g., "broken seal," "different label")
- Analyse vast existing customer data and use GenAI-powered to automatically generate personalized content to educate customers
- Self-service chatbots to automate consumer interaction on FAQs in real-time to improve trust (e.g. share data privacy & protection policy).

(c) E-commerce Platform Collaboration

Work with platforms like Amazon, Flipkart, and Alibaba to:

i. Register in brand protection programmes (e.g. Amazon Brand Registry).
ii. Enable platform-specific counterfeit detection tools.
iii. Get faster resolution and removal of fakes

How AI Tools help :

Brand Protection & Monitoring Tools

AI can scan and analyse vast volumes of online data to:

- Detect counterfeit listings on e-commerce marketplaces and third-party websites.
- Identify lookalike domains or websites using fake branding.
- Monitor image similarity across the web to catch unauthorized use of product visuals.
- Social Media Surveillance
  - AI can track mentions of a brand or product and flag suspicious sentiment or unauthorized resale behaviour.
  - Detect influencer-led counterfeit promotion through engagement pattern analysis and network behaviour.

Tools/techniques used:

- NLP for text-based fraud detection (e.g., suspicious product descriptions).
- Image recognition for logo misuse.
- AI bots for automated reporting and takedown.

3.2 AI-driven Legal Tech Layer

3.2.1 Maintain continuous oversight of the changing legal framework and interpretation of legislation pertaining to intellectual property rights and brand protection within your jurisdiction.

As the legal landscape changes, it is essential for stakeholders to stay aware about their rights and responsibilities to effectively navigate this intricate area of law. Proposed

legislation may enhance the right to repair, matching legal standards with the increasing need for consumer rights in the repair sector.

Compliance risk monitoring is an efficient method for navigating the changing legal environment, employing NLP-based surveillance of IPR and brand protection legislative advancements. This guarantees (a) notifications and impact assessments for legal and compliance teams and (b) proactive legal alignment, thereby diminishing costs associated with litigation and penalties for compliance violations.

3.2.2 Utilise AI for Intellectual Property Legal Task Management

AI tools are trained on extensive datasets related to legislation, norms, and procedures. New legislations and novel forms of intellectual property rights infringements are always emerging. Consequently, utilising real-time, verified quality data from credible and authentic sources is essential for efficient AI-driven intellectual property legal task management. The most efficient method to guarantee this is delineated in the steps mentioned below:

(i) **Establish a data lake within a cloud computing framework**, incorporating data from diverse internal generation sources (e.g., ERP, DWH, SaaS applications, textual data, unstructured data, streaming device/sensor data, etc.) and external sources (e.g., social and other digital media, economic statistics and surveys, policy documents issued by government agencies, etc.) utilising suitable cloud data integration tools.

(ii) **Employ cloud-hosted tools for assessing data quality**, conducting data discovery, and developing data dictionaries and classifications.
Centralised, cloud-hosted data pertaining to hundreds of cases and gigabytes of data can be handled effectively, increasing the speed and precision of legal tasks, as proven in the case of Eversheds Sutherland, rated as one of the top ten law firms in the world, and the adoption of cloud-hostedOpenTexteDiscovery [11].

(iii) Use the clean, error-free, quality data and AI and ML tools and techniques mentioned below for IP legal task management, as elaborated in Table 3.

Table 3: AI/ML Tool & Technique and IP Legal Task Management

IP Legal Task	AI and ML tools and techniques	How the AI Tools Help
Search and Clearance for Trademarks	ML-based Image Recognition, NLP	Improves risk evaluation by indicating comparable or contradictory textual and visual information.
Monitoring Trademarks	NLP + ML Monitoring Tools	Searches databases and the internet constantly for trademarks that are either contradictory or infringing.

IP Legal Task	AI and ML tools and techniques	How the AI Tools Help
Application Drafting for Trademarks	LLMs, Form-Filling AI	Helps with classification rules and precise descriptions of goods and services.
Infringement Detection of Copyright	Image/Audio/Video Recognition, NLP	Uses content-matching AI to find illegal use of creative works on several platforms.
Registration for Copyright	NLP + LLMs	Helps writers complete and check copyright paperwork and metadata for submission
Patent Prior Art Search	Semantic Search + NLP	Searches comparable patents to transcend simple keyword searching and matching
Patent Drafting	LLMs + Templates	Generates early versions of abstracts, specifications, and patent claims.
Management of Patent Portfolio [12]	ML Dashboards	Track filings, deadlines, and renewals, and evaluate portfolio risks and strengths.
Patent Litigation Approach	Legal Analytics + ML	Examines case results, judge behaviour, and litigation history to refine legal strategies.
IP Valuation and Licensing	Predictive Analytics	ML models help estimate licensing prospects, competitive strength, and patent value.
Software EULA and Licensing Terms Management	NLP, LLMs	Ensure appropriate clauses on Warranty, Indemnity, Limits on Liability, Software and hardware updates/upgrades, and maintenance and support policies, including bug fixes, SLA for issue resolution, etc.

IP Legal Task	AI and ML tools and techniques	How the AI Tools Help
Customs and Border Control Collaboration (Register IP with customs authorities)	Pattern recognition ML models	Monitoring and seizure of counterfeit imports/exports to identify patterns of shipments or regions with a high risk of counterfeit trafficking.

3.2.3 Streamlining Routine Legal Tasks: Routine legal tasks, which can be automated with improved accuracy using various AI and ML tools, are given below in Table 4.

Table 4: AI/ML Tool & Technique for Streamlining Routine Legal Tasks

Legal Task	AI and ML tools and techniques	How the Tool Helps
Document Review / e-Discovery	Natural Language Processing (NLP), LLMs	Automatically categorises, ranks and flags pertinent legal documents or evidence
Contract Analysis	NLP, Named Entity Recognition	Finds important clauses, errors, and risks in contracts for quicker and more accurate examination
Legal Research	Language Models, Semantic Search	Uses context-aware search and summarising to expedite legal precedent research.
Predictive data analytics	Machine Learning Classification/Regression	Forecasts case results using historical court decisions, judge behaviour, and legal considerations.
Due Diligence	NLP, Text Classification	Review vast amounts of data automatically during M & A
Regulatory Compliance Monitoring	Rule-based AI, NLP	Track changes in legislation and evaluate compliance automatically

Legal Task	AI and ML tools and techniques	How the Tool Helps
Efficient Electronic Evidence Gathering	NLP, LLMs, ML Tracking (Date, Time, Location, etc.)	From its acquisition to its presentation in court, use a digital footprint to demonstrate custody of the electronic record, therefore proving admissibility as evidence.
Litigation Strategy	Legal Analytics, ML Forecasting	Examines opposing counsel and judge conduct to guide case strategy.
Chatbots / Legal Assistants	LLMs, Conversational AI	Offers quick legal counsel or direction on common legal processes.
Time & Billing Automation	ML Time Tracking	Tracks and classifies billable hours from activity logs automatically.

3.2.4 Integrate AI into product development and innovation [13]

Combining Product Development Life Cycle (PDLC) with AI improves the effectiveness of IP planning processes. Manufacturers gain a substantial competitive advantage, as it enables them toachieve:

1. Designed for counterfeit protection, in new products
2. Significantly faster time to market
3. Quality, risk, compliance, and accessibility are addressed in parallel with designing, prototyping, and field testing.
4. Built-in design for repairability, a key requirement for compliance with regulations in the “Right to Repair” era. It involves designing products from the outset with ease of repair in mind, focusing on modularity, accessibility of components, and providing necessary information to consumers and third-party repairers.

The results achieved by Solinftec, a digital agriculture company in Brazil, demonstrate the efficacy of this consolidated approach to IP management [14].

How AI Tools help :

Artificial Intelligence boosts the capacity for accurate predictive analysis about compliance with data privacy, security, and bias through the use of machine learning models, hence facilitating the anticipation and response to future innovations and ensuring that intellectual property strategies remain aligned with market demands and company objectives. The incorporation of these instruments provides a thorough, all-encompassing, and sustainable strategy for intellectual property planning, enhancing organizations' resilience and competitiveness in a rapidly changing global environment.

4. AI-Driven Governance Layer

4.1 Current Legal and Regulatory Governance Framework for AI-based Solutions in India

India currently lacks a comprehensive standalone law specifically dedicated to artificial intelligence (AI). However, a multi-layered legal and regulatory framework governs AI-based solutions through a combination of existing laws, sectoral regulations, policy initiatives, and judicial precedents. Below is a breakdown of the current legal framework.

4.1.1Constitutional & Fundamental Rights Framework

a) **Right to Privacy (Article 21):** Recognised as a fundamental right in Justice K.S. Puttaswamy v. Union of India (2017) [15]. AI solutions must respect data privacy and personal liberty.
b) **Equality & Non-Discrimination (Articles 14 & 15):** AI algorithms must not lead to biased or discriminatory outcomes, especially in areas like credit scoring, recruitment, or policing.
c) **Key Statutory Laws:** These are outlined in Table 5.

Table 5: Key Statutory Laws Governing AI

Law	Applicability to AI
Information Technology Act, 2000	Governs digital operations, cybersecurity, and liability for computer-related offences; AI falls within its scope (Ref.: My Space Inc. vs. Super Cassettes Industries Ltd – upholds "safe harbour" provision for intermediaries under Sec. 79 of the Information Technology (IT) Act, 2000 [16]).
Indian Penal Code (IPC), 1860	Applicable in cases where AI-enabled tools cause harm or are used for fraud or defamation.

Law	Applicability to AI
Consumer Protection Act, 2019	AI chatbots, recommendation engines, and personalised ads are governed by product/service liability and misleading advertising provisions.
Copyright Act, 1957	Governs AI-generated content. Ownership of AI-generated works remains legally ambiguous.
Contract Act, 1872	Applies to AI-based smart contracts and automated digital agreements.
Personal Data Protection Bill (PDP) (proposed, now evolved into DPDP Act, 2023)	Governs AI usage involving personal data; mandates consent, purpose limitation, and accountability.
Digital Personal Data Protection Act, 2023 (DPDP Act)	The primary law governing data privacy impacts how AI systems collect, store, and process personal data. Compliance is critical.

4.1.2 Judicial and Quasi-Judicial Interventions

The courts have emphasised algorithmic accountability and the need for transparency in automated decision-making. For example, S Q Masood vs State Of Telangana [17]questioned the use of facial recognition technology without legislative backing.

4.1.3 Policy & Strategy Framework

India is actively developing a policy and strategy framework for AI, focusing on responsible development and deployment while aiming to become a global leader in AI. The key initiatives are outlined in Table 6 below.

Table 6: Policy & Strategy Framework for AI

Policy Document	Issuer	Key Focus
National Strategy for Artificial Intelligence #AIforAll (2018)	NITI Aayog	Focus on inclusive growth in healthcare, agriculture, education, smart cities, and smart mobility.
Responsible AI for All (2021)	NITI Aayog & World Economic Forum	Framework for responsible AI development in India.

Policy Document	Issuer	Key Focus
Digital India Act (Proposed, 2024)	MeitY	Will likely replace IT Act, 2000; expected to include governance of AI, deepfakes [18], algorithmic transparency, etc.

4.1.4 Emerging Guidelines

a) MeitY Advisory on Ethical AI (2021): Suggests principles like fairness, accountability, privacy, inclusivity, and transparency.
b) The Bureau of Indian Standards (BIS) is also developing standards for AI system safety and reliability.

4.1.5 Pending Legislation & Debates

a) The Digital India Act (draft expected by the end of 2025) islikely to bring binding rules on AI safety, audits, and sandboxing.
b) AI regulation consultation papers by various ministries are under discussion,but there is no binding law yet.

4.1.6 Data Privacy Concerns: Consent Management Platforms (CMP)

Most of the anti-counterfeit measures are dependent on consumer-initiated counterfeit detections – e.g., scanning QR codes on packaging and products. To ensure the legal validity of such consumer-initiated IP breaches, the anti-counterfeit solutions need to collect specific consumer information, including the consumer who reported the counterfeit product (e.g., PII data, image, video, etc.).
The DPDP Act and SPDI (Sensitive Personal Data or Information) Rules mandateconsent as essential for personal data (PII data, images, video). Many organisations use CMP, which ensures compliance withthe DPDP Act, 2023, by taking the following measures:

- Provide digital notice in multiple languages.
- Provides clear information about data collection practices and allows users to control their preferences,
- Log consent, withdrawal, and data access requests.
- Enable trusted data fiduciary platforms like Sahamati [19](for financial consent using the Account Aggregator model).
- Bias Detection in Algorithms (if AI is used to process personal data)
- Model Explainability Logs (especially for decisions affecting rights)
- Automated DPIA (Data Protection Impact Assessment) workflows

How AI Tools help :

- NLP parses and understands privacy policies, terms & conditions, and maps them to compliance frameworks.
- ML predicts risk of consent fatigue and recommends adaptive consent prompts.
- Computer Vision detects unauthorized data access patterns and flags it for consent violation.
- Process Automation and AI: Automates backend workflows like revoking consent

4.1.7 Compliance Checklist for using AI-driven solutions in Anti-Counterfeit Measures in India – Key Risks and Mitigation Strategy

The AI Compliance Checklist for India is provided in Table 7, which summarises the key requirements across the dimensions of privacy, fairness, transparency, safety, and accountability.Companies deploying AI to detect, track, and prevent counterfeit goods across supply chains, digital commerce, and physical product authentication should use these. It covers compliance from a legal, ethical, and technical perspective, with a focus on compliance requirements in India. If, for some risk components, there is no specific law that requires legal compliance, then relevant guidelines from policy-making agencies should be used—e.g., for ethical AI use and sectoral codes, one should follow NITI Aayog's principles that AI must avoid harm, bias, and data misuse.

Table 7: AI-driven Solutions' Compliance Checklist Key Risks and Mitigation Strategy

Risk component	Action to be taken	Risks mitigated
Legal & Ethical Assessment	Adhere to the DPDP Act, 2023, and SPDI Rules when processing personal data.	Non-compliance, unauthorised data use, legal liabilities.
Audit Bias & Fairness	MeitY Responsible AI guidelines: fairness, explainability, androbustness. Test AI outputs for bias.	Algorithmic bias, Blackbox model, reputational risk.
Human-in-the-Loop Review	Required under MeitY guidelines. Critical review and decision-making with the aid of legal professionals	Blindly following AI output, accountability gaps.

Risk component	Action to be taken	Risks mitigated
Auditability of AI decision-making	Required under MeitY guidelines. Keep records of AI decisions, logic and outputs for future audits.	Inability to defend decisions legally
Cybersecurity threats	The Indian Computer Emergency Response Team (CERT-In) mandates reporting within six hours of detection. Protect AI training data and implement a secure-by-design methodology; evaluate model weaknesses through adversarial testing.	Secure AI systems against cyberattacks. Only 24% of current generative AI projects are being secured [20]
AI hallucinations contribute to misinformation	MeitY Responsible AI guidelines: fairness, explainability, and robustness.Employ superior training data, meticulously assess AI models, and perpetually analyse and enhance them.	Propagation of misinformation via social media, exacerbating disinformation, tarnishing reputations, and perpetrating harassment or extortion against victims
Continuous Evaluation of Consumer Redress & Audit Trails	CPA 2019 requires the implementation of grievance mechanisms and the maintenance of AI decision logs. Regular monitoring of the alignment of AI performance accuracy and alignment with legal goals	Model decay, misalignment with regulations
Labelling & User Communication	Legal metrology + BIS rules: AI-generated trust labels (QR, RFID, holograms) must not mislead.Implement SOP for continuous monitoring and handling errors in labelling.	Avoid “deceptive marketing”. Delay in mitigation, client harm, and regulatory fines.

4.1.8 Handling Key Challenges

Adoption of AI-driven legal tech also faces a number of challenges [21], which call for appropriate action (Table 8).

Table 8: Key Challenges and Approach to Address Them

Challenge	Action to be taken	Issue addressed
Skill gap	Through the "Train the Trainer" programme, arrange hands-on training and continuous skill improvement without compromising the daily responsibilities of the legal team.	Mistrust of the quality of legal work and slow acceptance of AI-driven legal tech
Data Availability and Quality	Invest in data management technologies – such as data quality and the capability to handle and ingest data into a cloud data lake from all types of sources (text, structured data, ERP, SaaS, 3rd party data, unstructured data, streaming data, etc.). At the same time, implement a comprehensive data governance strategy to maintain data integrity over time.	Trustworthy, clean data from credible sources. AI models rely on high-quality data – this will eliminate poor data quality, severely undermining AI models, no matter how advanced they may be.
Initial cost	Adopt a phased investment approach for quality products and deliver more bang for your money before investing more.	Stay away from less expensive choices – prevent waste of time and money.
Client confidentiality	Make sure the instruments they employ comply with rules and have strong security measures	Be prepared for the trend to control the application of AI in legal work by many states [22]

5. Conclusions:

This research paper establishes the advantages of the adoption of a unique and effective IPR protection and anti-counterfeiting action framework, involving an integrated multi-layered approach: (a) AI-Driven Technology Layer, (b) AI-Driven Legal Tech

Layer and (c) AI-Driven Governance Layer. Furthermore, this innovative approach will aid in addressing emerging trends in the use of AI for IPR infringement and counterfeit protection, as outlined below.

5.1 AI and ML are anticipated to generate greater efficiencies and greater accuracy in the legal profession in the realms of IP and brand protection, though not without ethical and other risk-related concerns

Further disruption to the legal sector is inevitable as the growth of legal technology startups, and the venture capital investment in such entrepreneurial companies picks up pace. Technology is developing rapidly, so researchers, lawyers, and policy analysts must collaborate to capitalise on this new opportunity. They must maintain vigilance while adhering to ethical and legal codes of conduct. Investigations in these areas will be critically formative for the future of legal work in IP and brand security.

5.2 Emerging technology and "legal climate change" will lead to new business models [23]

According to a 2023 Goldman Sachs study, AI has the potential to replace 40% of legal industry workers and automate 44% of work tasks. Around the world, including India, we are increasingly observing the following trends:

5.2.1 A Rise in Flat Fee Billing

Since AI shortens the time needed for many legal office tasks, flat fees enable law firms to recognise the value of their services without being constrained by time-based billing. Additionally, billing cycles and payment collection are accelerated for law firms that use flat fees. Flat fee billing is becoming more common; compared to 2016, law firms are using it for 34% more cases.

5.2.2 Increasing Investment in Marketing and Tech

Law firms are increasing their marketing and technology expenditures steadily, according to the report. Since 2013, software expenditures have increased by an average of 20% annually. Revenue growth, which has been consistent at 9% annually, has been surpassed by this increase. A disproportionate increase in technology expenditures indicates that businesses are increasingly considering technology to be a critical component of their future operations.

5.2.3 Growth of entrepreneurship in the legal sector: A "legal climate change"

A "legal climate change" is now underway, where further disruption to the legal sector is expected as the growth of legal technology startups and the venture capital investment in such companies picks up pace. From 2018 to 2021, the venture capital invested in the legal industry has grown from $1 billion to $4 billion, with hundreds of new startups being launched. Many of these companies are less interested in selling or licensing directly to law firms but rather are looking at taking clients on as their own. The growth

of alternative service providers is predicted to grow significantly through 2027, with client expenditures growing from $12 billion to $85 billion.

5.3 Working across disciplines with subject matter experts, including legal professionals, ethicists, technologists, anti-counterfeit enforcement agencies and legislators, will be an essential step in this effort.

In an ever-changing environment, lawyers, policymakers, researchers, and educators must assemble to establish and document the role of artificial intelligence and machine learning in the practice of law. In conclusion, our task is not only to leverage these technologies fully but also to do so with extreme caution and vigilance in light of ethical considerations and the principles of justice central to the legal issue and its professionals.

5.4 Establishing jurisprudence about the proper use of AI will expedite adoption for IP and brand protection.

In the adjudicatory process, it is crucial for the legal sector to ensure the need to preserve the human component of justice while integrating AI. In Christian Louboutin SAS (Plaintiff) v. M/S The Shoe Boutique - Shutiq. (Defendant) [24],the Hon. Delhi High Court observed that "AI-generated data accuracy and dependability are still up in the air. Neither human intelligence nor the human component of the adjudication process can be replaced by AI at this point in technological development. The tool might, at most, be used for fundamental research or a preliminary understanding.Ethical guidelines and regulations should be established that govern AI algorithms in accordance with the principles of justice, impartiality, and accountability. Following the example set by the United States, Indian courts may implement mandatory disclosures about AI utilisation, which would entail identifying the AI tool, detailing its application, and indicating the precise sections that were composed or investigated with its assistance.

5.5 Adopt best practices for the implementation of AI-driven legal tech for IP and brand protection in compliance with existing and upcoming regulations

i. Conduct **pre-launch AI impact assessments** across jurisdictions.
ii. Build **explainability dashboards** for AI decisions: Log all AI decisions and keep records of how and why a product was flagged—useful for both legal defence and system improvement.
iii. **Human-in-the-loop:** Always involve human oversight for high-impact decisions like seller removal, customs seizure, or takedown notices.
iv. **Cross-functional compliance**: Work with legal, IT security, supply chain, and marketing teams to ensure AI-based anti-counterfeit tools do not introduce privacy, IP, or reputational risks.
v. Include **"AI-generated" notices on packaging** or digital twin interfaces to comply with labelling laws.

References:

1. Anand Saurav, (January 25, 2023), Live Mintbusiness publication, Almost 25-30% Products Sold in India Spurious with Counterfeiting: Report.
2. CorsearchInc. (Oct. 28, 2020), Corsearch Blog, Multi-Channel Brand Protection: Constructing a 3D Defence of Your IP
3. Clarivate ThinkForward (2024), Clarivate Whitepaper, Artificial Intelligence for the IP Legal Profession – Practical Approaches for Harnessing the Potential of AI (pp. 4-7)
4. ASPA and CRISIL Report, (January 2023), The State of Counterfeiting in India 2023
5. Community by NASSCOM Insights – Report (April 26, 2023), Unpacking India's IP Ecosystem – for an Innovation-Led Future
6. The Ministry of Electronics and IT (Meity) (February 27, 2025), Advisory Group, chaired by the Principal Scientific Advisor, Report on AI Governance Guidelines Development
7. Core-AI (Coalition for Responsible Evolution of AI), (February 27, 2025), Comments on the Sub-Committee's Report on AI Governance Guidelines
8. Gaur Vishal &Gaiha Abhinav, (May-June 2020), Harvard Business Review - Operations and Supply Chain Management, Building a Transparent Supply Chain
9. Certilogo S.p.A., (June 21, 2022) Certilogo Blog, How Technology Helps Brands to Fight Counterfeiting
10. VeritechInc. (October 15, 2024), VeritechBlog, How Secure Labels Protect Consumers from Counterfeit Products
11. Opentext Inc. (2024), Opentext Customer Story, Eversheds Sutherland Accelerates Case Analysis with End-To-End eDiscovery and Investigations Platform,
12. Anaqua Services, (June 14 2022), Anaqua Services - IP Business Management | Patent Management, Kyocera Document Solutions Inc. Selects Anaqua for Integrated IP Management
13. G. Chandra, H. Martin Harrysson, Singh Rikki & Chawla Aditi (February 10, 2025) McKinsey & Company, How an AI-Enabled Software Product Development Life Cycle Will Fuel Innovation
14. Xie Christina Xie, (October 18, 2024), AgNews, Robots in the Fields: How Solinftec Is Cultivating Brazil's AI-Powered Agricultural Revolution
15. The Supreme Court of India Judgement (August 24, 2017), Justice K.S.Puttaswamy (Retd) And Anr. vs Union Of India And Ors, AIR 2017 SUPREME COURT 4161

16. The Delhi High Court Judgement, (December 23, 2016), My Space Inc. (Appellant) vs. Super Cassettes Industries Ltd (Respondent) C.M. APPL.20174/2011, 13919 & 17996/2015
17. The Supreme Court of India Judgement (April 27, 2022), S. Q. Masood & Prs. (Appellant) v. State of Telangana (Respondent), Petition(s) for Special Leave to Appeal (C) No(s). 12926/202
18. The Delhi High Court Judgement, (September 20, 2023), Anil Kapoor (Plaintiff) v. Simple Life India & Ors. (Defendant), CS(COMM) 652/2023
19. Sahamati Foundation (2025), Account Aggregators Are the Future of Data Sharing
20. IBM Institute for Business Value, (2024), Research Insights, Securing Generative AI
21. Martin Kara (February 3, 2025), Naviant - Intelligent Automation, 9 Common Challenges to AI Adoption and How to Avoid Them
22. Norden Lawrence &Lerude Benjamin, (November 6, 2023), Brennan Centre for Justice at NYU Law, States Take the Lead on Regulating Artificial Intelligence
23. Langemo Bree, (May 23, 2024), American Bar Association (ABA), Transforming the Legal Profession Through Technology and Entrepreneurship,
24. The Delhi High Court Judgement, (August 22, 2023), Christian Louboutin SAS (Plaintiff) v. M/S The Shoe Boutique –Shutiq (Defendant) CS(COMM) 583/2023