Journal of Intellectual Property Rights
Vol 29, November 2024, pp 500-506
DOI: 10.56042/jipr.v29i6.4806

Digital Forensics for Safeguarding Intellectual Property Rights: A Study in the Context of Indian IPR Laws

Chitrakara Hegde[1], S Chakravarthy Naik[2†] and Lammata Ashish Kumar[3]

[1]Department of Science, Alliance University, Bengaluru — 562 106, India

[2]Department of Law, Alliance University, Bengaluru — 562 106, India

[3]Vignan Institute of Law, Vignan's University (VFSTR), Guntur — 522 213, India

Received: 11th August 2023; revised: 22nd February 2024

The protection of intellectual property rights in the digital realm is of utmost importance, particularly in developing countries like India. This paper conducts a thorough investigation into the role of digital forensics in preserving and enforcing intellectual property rights, specifically within the Indian context. Through an extensive review of relevant literature, we identify gaps in current research and propose a comprehensive methodology for examining and addressing intellectual property infringements in the digital domain. The paper incorporates certain examples and cases where digital forensics may be used to counter infringement. By exploring the intersection of digital forensics and intellectual property rights in India, this study contributes valuable insights to the existing body of knowledge, offering practical implications for policymakers, law enforcement agencies, and intellectual property rights holders operating in similar contexts.

Keywords: IPR, Cyber Laws, Digital Forensic, Hypothetical Cases

According to Ken Zatyko, former director of the US defense computer forensics laboratory digital forensics digital forensics can be defined as "The application of computer science and investigative procedures for a legal purpose, involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible expert presentation."[1] Digital forensic and intellectual property rights (IPR) are both crucial apparatuses in today's digital age. Digital forensic plays a significant role in investigating and analysing digital evidence to uncover cybercrimes and protect individuals and organizations from cyber related threats. It helps in identifying and gathering crucial information, such as data breaches, hacking incidents, or intellectual property theft. On the other hand, intellectual property rights safeguard the creations of the human mind, encouraging innovation, creativity, and economic growth. Digital forensic is instrumental in enforcing these rights by uncovering unauthorized use or infringement of intellectual property, allowing for legal action to protect the interests of inventors, artists, and businesses.[2] Together, these disciplines ensure a secure digital environment, foster innovation, and safeguard the rights of intellectual property owners.The development of DF and IPR is of utmost importance within the Indian context, as the country witnesses a significant surge in technological advancements and digitization.[3] Developing country like India with expansion of digital landscape, the risks associated with cybercrimes and the unauthorized use of intellectual property is huge, hence there is critical demand to recognize the digital forensic and IPR protection, leading to the establishment of specialized forensic laboratories and the formulation of legal frameworks to address emerging challenges. By examining the evolution of digital forensic practices in India, including advancements in techniques such as computer forensic, mobile forensics, network forensics, and cloud forensics, this study seeks to provide insights into the growth and effectiveness of digital forensic investigations.[4] Additionally, it explores the legal framework surrounding intellectual property rights, including laws and regulations governing copyrights, trademarks, and patents. Understanding the legal landscape is crucial in comprehending the framework that protects the rights of concerned individual. The challenges faced in the domain of DF and IPR protection in India cannot be overlooked. Limited resources, rapidly evolving technologies, and the need

†Corresponding author: Email: Chakravarthynayak@gmail.com

for capacity building pose significant obstacles. In India many initiatives have been started such as the establishment of specialized intellectual property courts, the promotion of awareness campaigns, and collaborations with international agencies have shown promise in enhancing digital forensic practices and IPR enforcement.[5]

From the achievement report of the office of the controller general of patents, designs &trademarks (CGPDTM), government of India gives insight into the number of patents, trademarks, copyrights, and design filed and granted/registered in India between 2014 and 2019 showed significant growth. The report indicates a substantial increase in the grant of patents by 317%, registration of trademarks by 607%, registration of copyrights by 346%, and registration of designs by 71%.[6] Figure 1 highlight the increasing importance of IPR protection in India.

Cyber Laws, IPR and Digital Forensics

The convergence of Indian cyber laws, IPR, and digital forensics creates a comprehensive approach to safeguarding intellectual property rights. When IPR violations occur in the digital space, digital forensics helps in preserving evidence, conducting forensic analysis, and presenting factual findings in legal proceedings. It assists in determining the extent of infringement, identifying the responsible parties, and proving the intention behind the illicit activities. Digital forensic techniques such as data carving, deleted file retrieval, chat history analysis, metadata analysis, network forensics, and file identification contribute to the identification of counterfeit products, pirated software, unauthorized distribution of copyrighted material, and other IPR infringements. The results of digital forensic investigations hold great value in court, providing irrefutable evidence and aiding in the successful prosecution of offenders.

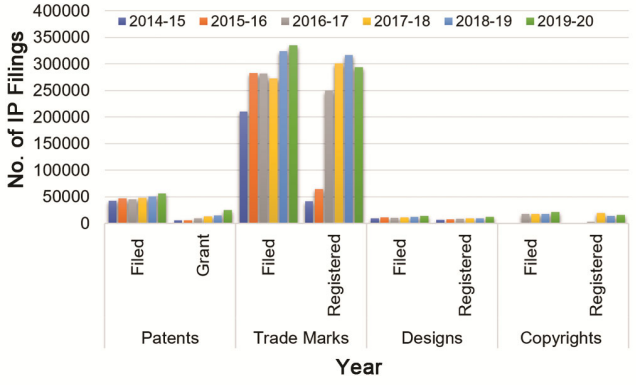

Fig. 1 — IP filing data in India

Intellectual property rights are like any other property right which protects and safeguard original inventor hard work. Post independence the Indian patent Act conceived on 1970[7] and amended in the year 1995, 1999, 2002 and 2005. The rules under this act known as patent rules further amended many times 2005, 2006, 2012, 2013, 2014, 2015, 2016, 2017 and 2019 in order to make this rule compatible, robust with changing technology, research methodology and international trend requirement. With effect from 1January 1995 India became member of WTO (World Trade Organization) and became party to the Trade-Related Aspects of Intellectual Property Rights (TRIPS). With advancement of technology, today India is the one of the major places of internet users. The 2022 report on internet in India by internet and mobile association of India (IAMAI)[8] says that there are 759 million (2022) internet users and it may reach up to 900 million by 2025. It can be argued that a large number of people in India utilize various devices such as desktop computers, laptops, and mobile smartphones to access the internet. As they engage with these devices, they rely on a multitude of software, apps applications. Additionally, they often use USB flash drives (pen drives) to store their search results. This signifies that a significant portion of the Indian population is now actively involved in the digital realm. Given this scenario, there is a growing need to address the diverse requirements of these individuals. Extensive research is being conducted on software development, application design, computer accessories, and advancements in Android phone technology. It is crucial to safeguard the intellectual property of inventors involved in these areas to ensure the progress and protection of their innovations.

Considering above facts,we can say that digital forensic plays important role in protecting IPR. Let us understand this further with an example,suppose a company suspects a software theft or infringement, then digital forensic experts image the hard drive of the suspected infringer's computer, capturing a complete snapshot of its contents followed by data analysis to identify any signs of software theft or infringement. This may involve examining files, metadata, logs, and other digital artifacts. Based on the forensic findings, appropriate remedial actions can be taken, such as removing unauthorized copies, securing intellectual property, and initiating legal proceedings against the infringing party. Action plan can be represented in following ways as shown in Fig. 2.

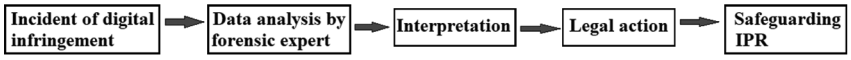

Fig. 2 —Action plan for safeguarding IPR through digital forensics

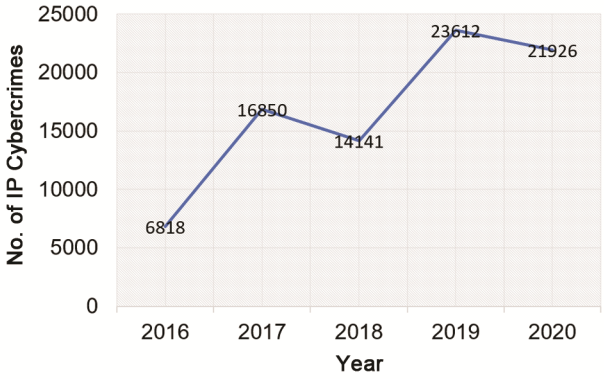

Fig. 3 — Cybercrime cases registered related to computer-based offences

Cybercrime and IPR

In India the mid-1990s, there was a notable acceleration in globalization and computerization, resulting in an escalating number of nations digitizing their governance systems and witnessing a substantial expansion in e-commerce. Prior to this era, the majority of international trade and transactions relied on physical documents transmitted via postal services or telex. Evidence and records predominantly existed in the form of tangible paper documents or other hard copies. However, with the increasing prevalence of electronic communication and the rapid adoption of email, there arose a pressing and imperative need to acknowledge the legal validity of electronic records, encompassing data stored in computers or attached external storage devices. With above background Government of India enacted IT Act, 2000 (information technology Act) which main objective being issues on legal recognition of electronic documents, legal recognition of digital signatures, offenses and contraventions and justice dispensation systems for cybercrimes. Though this act clearly not defines cybercrime in a simpler term we can say any offence or crime in which a computer is used is a cybercrime. As per the record of National Crime Record Bureau all over India total cybercrime cases registered which related to computer-based offences for the five years from 2016 to 2020 are shown in following Fig. 3.[9]

Digital forensics [10] plays a crucial role in the realm of justice, serving as a formidable weapon to safeguard intellectual property rights such as patents, copyrights, and trademarks (Table 1). In India, the incidence of cybercrime[11] has witnessed a significant surge, making it imperative to explore hypothetical scenarios where expertise in digital forensic investigation can aid in resolving these issues effectively.

In *Microsoft Corporation* v *Yogesh Papat and Anr.,*[22] the Delhi High Court observed that there has been infringement of Trademark and Copyright over certain softwares like MS-DOS, Microsoft Office, Microsoft Windows. The basis for this judgment is the digital forensics. Though there is no specific reference to this term at that time, but it can be observed that the methodology involved is inherent to the digital forensics. The evidence conclusively determined the piracy of the hard disks by the defendants. It was proved that defendants engaged in software piracyand thereby uploading those softwares on the hard disk of the sold computers without proper authorization or consent from the plaintiffs.

Media Houses like T-series have filed numerous lawsuits against uploading of its copyrighted and licensed content on YouTube, social media platforms, etc. These media companies employ digital forensic technologies to identify the infringing content, unauthorized uploading, and gathering evidence against the infringers.[23]

In 2017, there was a major cyber attack on HBO's Game of Thrones series where an episode was leaked online by the hackers. HBO employed cyber security firms to encounter this issue through digital forensics.[24] These cases show the importance of digital forensics as digital space is expanding, and the commission of crimes have found new ways to breach the internet world.

Artificial Intelligence, Digital Forensics and Intellectual Property Rights

The development of Artificial Intelligence has revolutionized Intellectual Property Rights. Deployment of Artificial Intelligence technologies have been used for catena of areas like IP management, examining potential infringements, searching prior art, patent filing, drafting patent applications, technology transfer, licensing. Conducting IP due diligence through AI is assuming significance in many corporations.

Artificial Intelligence can be employed in digital forensics to identify the actually infringing

Table 1 — IPR Offenses and Digital Forensic Solutions

IPR offenses	Hypothetical case explanation	Applicable Law/Rule in India	How digital forensic expert can help
Copyrights	A renowned music company filed a lawsuit alleging copyright infringement against an individual involved in the unauthorized sale of copyrighted sound recordings	Copyright Act,[12] 1957, Section 51	A digital forensic expert possessing specialized tools and techniques can play a vital role in recovering data from the defendant's digital devices. They can examine metadata linked to the unauthorized sound recordings to determine their origin and trace the channels through which they were distributed. If the unauthorized sales occurred online, the digital forensic expert can investigate the network infrastructure, internet protocols, and online platforms involved. By tracking the digital footprints left by the defendant, including IP addresses, email accounts, and online payment gateways, they can establish connections and unveil the defendant's online activities[13]
Copyrights	A renowned technology corporation initiated legal proceedings against an individual, alleging the sale of pirated copies of software owned by the corporation.	Copyright Act, 1957, Section 65 A[14]	Forensic expert can investigate the network infrastructure, internet protocols, and online transactions involved to track the from where software ordinally belonging [15]
Copyrights	A well-established software development company, XYZ Software, created and copyrighted a mobile application that gained substantial popularity in the market. However, they discovered that certain individuals were illicitly distributing and selling unauthorized copies of their copyrighted mobile software	Copyright Act, 1957, Section 58	By using advanced mobile forensic toolkit expert can get original place of software
Design	ABC Semiconductors, a semiconductor design company, registered a unique and innovative layout design for an integrated circuit However, XYZ Electronics, a competitor in the semiconductor industry, began manufacturing and selling integrated circuits that bore a striking resemblance to the registered layout design of ABC Semiconductors. XYZ Electronics did not obtain the necessary authorization or license from ABC Semiconductors to use or replicate their layout design.	Indian Semiconductor Integrated Circuits Layout Design Act, 2000, Section 18[16,17]	To comprehend and evaluate the original circuit layout design and identify instances of infringement, Specialized electronic design automation (EDA) software and forensic tools for circuit design analysis play a crucial role. These tools are purpose-built for conducting in-depth examinations and analyses of circuit designs[18]
Design	'Z'a semiconductor design company, created an innovative and unique layout design for a cutting-edge semiconductor chip. Successfully registered their layout design under the provisions of the Indian Semiconductor Integrated Circuits Layout Design Act, 2000. Another company namely 'X Electronics', replicated and manufactured identical semiconductor chips using Z semiconductor designs' registered layout design without obtaining proper authorization or a license	Indian Semiconductor Integrated Circuits Layout Design Act, 2000, Section 62	Digital forensic expert can conduct comparative analysis of two design and examination of Metadata, such as creation dates, modification history, or embedded information, can provide insights into the origin and unauthorized usage of the layout design. This information can help establish a connection between X Electronics and the infringement[19]

(*Contd.*)

Table 1 — IPR Offenses and Digital Forensic Solutions (*Contd*.)

IPR offenses	Hypothetical case explanation	Applicable Law/Rule in India	How digital forensic expert can help
Trademark	A well-known beverage company in India 'XYZ' that specializes in providing various bottled drinks, including a popular orange fruit beverage, decided to expand its business internationally. As part of their expansion strategy, the Defendant entered into an agreement with another global beverage corporation 'ABC'. Under the terms of the agreement, the 'XYZ' gave exclusive rights to the ABC for formulation, intellectual property, and know-how associated with their orange fruit drink for the Indian market. Now ABC company started exporting orange fruit drink under same name. XYZ company believe these actions constituted trademark infringement.	Section 134 The Trademarks Act, 1999[20]	If the ABC company is using the same name for their orange fruit drink, the expert can analyze the website to determine if it mimics the design, layout, or content of the XYZ company's website, which could strengthen the trademark infringement claim. The expert can conduct a comprehensive investigation into the online presence of the ABC company to identify any other instances of trademark infringement or unauthorized use of intellectual property. This may include searching for similar products or advertisements in other markets or online platforms[21]
Trademark	A news agency makes/distribute online news content through its registered website aby.com and its rival company make similar business through its website abby.com. now aby.com agency alleges trademark infringement on abby.com	Section 11 of The Trademarks Act, 1999	The expert would conduct network forensics, which involves examining network traffic and communication data related to the websites. This may include analyzing server logs, network packets, and any other available network records.Using specialized tools and techniques, the expert would identify the IP addresses associated with aby.com and abby.com. This can be done by examining DNS (Domain Name System) records, WHOIS information, or by directly interacting with the websites' servers. The expert would trace the identified IP addresses to their physical locations or hosting providers. This can involve gathering information from Internet Service Providers (ISPs) and other relevant entities to determine the geographical locations or hosting infrastructure of the websites.

components of patents, copyrights, trademarks, and other forms of IP. Due to the technological advancements, IP has become more operative in cyber space opening it to various risks. Use of basic technologies is already evident in identifying IP risks and infringement, but the manual process takes time and the loss is already borne by the owners. Artificial Intelligence can significantly reduce the time of assessing the method of violation and identifying the infringers through robust investigating mechanisms and evidence accumulation.

A case to case-based reasoning approach is employed by Artificial Intelligence through data mining so as to find out the minute of infringing components. The aim of Artificial Intelligence in infringement analysis is to dwell into exploring IP infringement data sets and application of data mining and machine learning algorithms to the allegedly infringing data. Data processing complexities demands more technological interference than human intervention. The data processing analysis is catalysed by Artificial Intelligence through logical reasoning(artificial) which may be always checked by human experts for any possible errors and arrive on a decision in a timely manner.

In most of the Intellectual Property infringements especially copyrights and patents, there is a pattern of infringements. Artificial Intelligence can be best used for identifying patter recognition of infringements on the dependent data sets.

The proliferation of data is challenging the legal enforcement as infringers have acclimatised to the digital environment. Distributed systems and network where digital operations are operated at different

places (different networks), VPN etc have become more challenging. With the meagre human force, it is difficult to identify these networks unless the physical location of the infringers is found. Ontologies induced AI and expert AI systems can reduce these difficulties for blocking the infringers.

On the other hand, Artificial Intelligence can be widely used in pre-grant procedures of Intellectual Property. In the stages of classification of applications, prior art searches, trademark searches etc, Artificial Intelligence becomes handy to due humongous applications flowing into IP offices all-over the world. In 2021, 3,401,100 patent application, 18,182,300 trademark applications, 1,515,200 industrial design applications were filed.[25]Recognizing the need World Intellectual Property Organization (WIPO) developed AI technologies to handle trademarks, patents, etc. WIPO employed an AI empowered image search tool to identify the similarities of the marks of new application with the existing registered marks.[26] Similarly for patents classification under International Patent Classification system, it deployed an automatic patent classification tool which uses neural network technology (IPCCAT-neural).[27]International Patent Classification classifies the patents and utility models on the basis of a hierarchical classification of language independent symbols. There are classified as per various technologies the patent or utility model may belong to. So, IPCCAT-neural is an AI tool that helps efficiently classify into main and sub-group levels through automatic text classification into categories. It is a trained system based on neural networks technology which can predict patent classification. Additionally, it can also predict the output of classification even if the input languages are English, French, Chinese, Arabic, Portuguese, etc. This is a major development in the field of patent procedures.[28] WIPO also uses a state of art technology which is neural machine translation (WIPO-Translate). It is a patent translation tool employed by WIPO to which helps the user to translate words or sentences that are technical in nature. The significant feature of this tool is the accuracy of the translation of patent phrases given by Neural Machine Translation as it is trained by Big Data.[29]Employing AI tools like these would invariably save time and efforts of examiners, conduct comprehensive prior-art searches, drafting and analysis. There would be transformative shift in the conventional IP management to AI based management of IP both for the authorities as well as the applicants and owners of intellectual property.

Conclusion

The strides of digital forensics and Intellectual Property have converging significance in the light of evolving technological frontiers. The paper explored the complex relationship shedding light on different facets of IPR and digital forensics.There is an inseparable connection between the legal landscape, Intellectual Property protection and the various tools and mechanisms of cyber forensics. For every digital presence of patent, copyright, trademark and other forms of IP, there is an equal scope of violation of the rights which needs to be addressed by digital forensic assisting in detection, preservation, analysis of evidence at different stages of legal procedures. Few primary limitations include lack of specific provisions with reference to digital forensics as infringements are dealt in a generalised approach in Copyrights Act, 1957, Patent Act, 1970, etc. Specific provisions involving digital forensics in legal enforcement coupled with capacity building and training programmes for concerned officials would strengthen and safeguard IPR in its truest sense. This is very much necessary due to the advanced presence of cyber criminals committing IP thefts, direct infringements of various IP. The data driven world has paved the way for Artificial Intelligence to be best used for protecting Intellectual Property. Diversified techniques like pattern recognition, ontologies, data mining, etc have will enable the enforcement agencies to ably counter IP infringements. It is indeed motivating to see international organisations like WIPO deploying Artificial Intelligence based technologies to deal with pre-grant registration procedures. The same is advised to Indian IP agencies to employ due to rising IP applications being filed by individuals, corporations and especially start-ups. Additionally, the tech companies should develop their inhouse cyber attack prevention mechanisms by employing Digital forensic specialists. Though, most of companies are having their own cyber security wings but a dedicated mechanism would invariably help them to prevent any kind of possible infringements that may occur as digital space is vulnerable to cyber-attacks.

Higher Educational institutions, research organisations, etc, should be leveraged to develop such digital forensic technologies which would help the IP and other enforcement agencies to tackle the

ever-growing issue of online infringements. Establishment of Centres for Digital Forensic Technology Development, collaborating with universities Foreign as well as Indian by formation of Working Groups, organizing training programmes within the institutions and technology-oriented industries would catalyse the transition of usage of conventional forensics to advanced digital forensics.

References

1 Zatyko K, Commentary: Defining digital forensics, *Forensic Magazine*, 2007.

2 Piquero N, Causes and prevention of intellectual property crime,*Trends in Organized Crime*, 8 (2005) 40.

3 Rani S, Digital India: Unleashing prosperity, *Indian Journal of Applied Research*, 6 (4) (2016) 187.

4 Cyber Forensics: Law and Practice in India, https://blog.ipleaders.in/ cyber-forensics-law-and-practice-in-india/ (accessed on 7 July 2023).

5 Bhat R S, Innovation, and intellectual property rights law-an overview of the Indian law, *IIMB Management Review,* 30 (1) (2018) 51.

6 Contact Us, Intellectual Property India, Government of India, ipindia.gov.in (accessed on 15 July 2023).

7 History of Indian Patent System, Intellectual Property India, Government of India,ipindia.gov.in (accessed on 15 July 2023).

8 Internet and Mobile Association of India (IAMAI), https://www.iamai.in/ (accessed on 20 July 2023).

9 Crime in India Table Contents, National Crime Records Bureau, ncrb.gov.in (accessed on 20 July 2023).

10 Costantini S, De Gasperis G & Olivieri R, Forensics and digital investigations meet artificial intelligence, *Annals of Mathematics and Artificial Intelligence,* 86 (2019) 193.

11 Patil J, Cyber laws in India: An overview, *Indian Journal of Law and Legal Research*, 4 (1) (2022) 1391.

12 Alankrita M, A Reflection upon the digital copyright laws in India, *Journal of Intellectual Property Rights*, 25 (2020) 5.

13 Rachana YP & Satish RD, Network forensic investigation protocol to identify true origin of cyber crime, *Journal of King Saud University - Computer and Information Sciences*, 34 (5)(2022) 2031.

14 Sufiya A, Fair dealing in Indian Copyright Law, *Journal of Intellectual Property Rights*, 26 (2021) 96.

15 Kim H, Kim E, Kang S & Kim HK, Network Forensic Evidence Generation and Verification Scheme (NFEGVS), *Telecommunication Systems*, 60 (2) (2015) 261.

16 SICLDR: Semiconductor Integrated Circuits Layout Design Registry.

17 Saurabh B, The Semiconductor Integrated Circuit Layout Design Act 2000 in India and the mischief of freedom of infringement, *Journal of Intellectual Property Law & Practice*, 10 (5) (2015) 378.

18 Paul R, Interpol review of digital evidence for 2019-2022, *Forensic Science International: Synergy,* 6 (2023) 100313.

19 Jeremy L, Daniel N, Charles TH, Karthik R & Jane G,The role of metadata in reproducible computational research,*Patterns,* 2 (9) (2021) 100322.

20 Sidharth C & Garima P, Legal position of naked licensing in trademarks: A comparative legal study between India and the US, *Journal of Intellectual Property Rights*, 27 (2022) 16.

21 Van Baar RB, Van Beek HMA&Van Eijk EJ, Digital Forensics as a Service: A game changer,*Digital Investigation,* 11(1) (2014) S54.

22 118(2005) DLT 580.

23 Indian Express, https://indianexpress.com/article/cities/delhi/t-series-copyright-infringement-case-delhi-hc-restrains-goldmines-telefilms-uploading-songs-14-films-8883555/ (accessed on 9 February 2024).

24 Cisomag, https://cisomag.com/hbo-targeted-major-security-hack/ (accessed on 10 February 2024).

25 WIPO IP Statistics Data Center, https://www3.wipo.int/ipstats/key-search/search-result?type=KEY&key=201 (accessed on 5 August 2023).

26 Global Brand Database,https://branddb.wipo.int/en/similarlogo?strategy=concept&sort=score%20desc&rows=60&asStructure=%7B%22boolean%22:%22AND%22,%22bricks%22:%5B%5D%7D&_=1691470854764 (accessed on 5 August 2023).

27 WIPO, https://www.wipo.int/classifications/en/news/ipc/2019/news_0006.html (accessed on 10 February 2024).

28 WIPO, https://ipcpub.wipo.int/?notion=search&version=20230101&symbol=none&menulang=en&lang=en&viewmode=f&fipcpc=no&showdeleted=yes&indexes=no&headings=yes&notes=yes&direction=o2n&initial=A&cwid=none&tree=no&searchmode=ipccat (accessed on 5 August 2023).

29 WIPO Translate – Breaking Language Barriers with AI, https://www.wipo.int/wipo-translate/en/ (accessed on 6 August 2023).