Alliance Journal of Intellectual Property Law (AJIPL)
Volume: 2, Issue: 1, 2024 | e-ISSN: 2584-0363

DIGITAL COPYRIGHT INFRINGEMENT: CHALLENGES UNDER THE INFORMATION TECHNOLOGY ACT, 2000

Sruti Bansal [1], Dr. Neha Saxena[2]

ABSTRACT

Digital copyright infringement in the context of the Information Technology Act, 2000 presents significant challenges in India's legal framework for protecting intellectual property in the digital environment. The rapid growth of the internet and digital platforms has made it easier for individuals to copy, distribute, and exploit copyrighted material without authorization, raising concerns about the efficacy of current laws. While the IT Act provides a foundation for addressing cybercrimes, including provisions for intermediary liability and takedown mechanisms, it lacks clear, specific provisions addressing the complexities of digital copyright infringement. Issues such as jurisdictional ambiguity, the misuse of safe harbour provisions by intermediaries, slow enforcement of takedown requests, and the evasion tactics of piracy websites complicate effective enforcement. Additionally, law enforcement agencies often face technical and resource limitations, further exacerbating the problem. Despite these challenges, the IT Act, in conjunction with the Copyright Act, 1957, aims to curb infringement, but there is a growing need for legislative amendments, better training for enforcement agencies, and international cooperation to combat the evolving nature of digital copyright violations effectively.

Keywords: *IT Act, Digital copyright infringement, digital environment, cybercrimes, safe harbour.*

OVERVIEW OF COPYRIGHT INFRINGEMENT IN THE DIGITAL AGE

The rapid advancement of digital technology has revolutionized the way information and content are created, distributed, and accessed, posing significant challenges to the traditional framework of copyright law. The rise of the internet and digital platforms has enabled widespread sharing and distribution of copyrighted materials, often without the consent or compensation of the copyright holders. Copyright infringement has become a pervasive issue in the digital age, as individuals and

1 Assistant Professor, School of Law, Presidency University, Bengaluru

2 Assistant Professor, Manipal Law School, MAHE, Bengaluru

entities can easily reproduce, distribute, and modify copyrighted works with a few clicks of a button. The ease of digital copying and dissemination has eroded the control that copyright holders once had over their works, leading to ongoing debates and legal battles over the appropriate balance between protecting the rights of creators and ensuring public access to creative content.[3] Recognizing the need to adapt to these technological changes, policymakers have enacted legislation aimed at preventing the circumvention of technological protection measures that are designed to control access to and use of copyrighted works. However, critics argue that such measures have gone too far, potentially stifling innovation, free speech, and the public's ability to engage in lawful and permissible activities.

The "double punch of law and technology" employed by copyright holders, which combines digital encryption technologies with legal protections against circumvention, has led to concerns that the underlying motivation is not merely to combat digital piracy, but to fundamentally reshape the landscape of copyright in the digital age. As the digital revolution continues to transform the way we create, distribute, and consume content, the challenge remains to strike a balance between protecting the rights of copyright holders and preserving the public's ability to access and build upon creative works.[4]

DEFINITION OF DIGITAL COPYRIGHT INFRINGEMENT

Digital copyright infringement is a complex and multifaceted issue that has garnered significant attention in recent years, as the proliferation of the internet and digital technologies has revolutionized the way we create, consume, and distribute content.[5] At its core, digital copyright infringement refers to the unauthorized use or reproduction of copyrighted digital content, such as software, music, films, and written works, without the permission of the copyright holder.

Digital copyright infringement refers to the unauthorized use, reproduction, distribution, or display of copyrighted material in the digital environment, including the internet and digital platforms. Infringement occurs when someone uses a work protected by copyright law without the permission of the copyright holder or legal justification.[6] The rise of the internet has made it easier for users to copy and share digital content, such as music, movies, books, software, and images, leading to widespread instances of infringement.[7] While traditional copyright laws were designed to protect physical copies of works, digital copyright infringement poses unique challenges due to the ease with which digital content can be replicated, distributed globally, and accessed by users across borders. The infringement can take many forms, such as downloading or sharing copyrighted content without authorization, including torrenting movies or music, streaming pirated content, and uploading copyrighted works (e.g., books, videos, or music) to websites without permission.[8] It can also involve creating and distributing derivative works based on copyrighted material, such as fan fiction, remixes, or unauthorized software adaptations. Other forms include reposting or embedding content on websites or social media platforms without proper attribution or licensing and using copyrighted software without paying for it (software piracy).[9]

3 Saregama India Ltd. v. M/s. Engadget Digital Media Pvt. Ltd., AIR 2019 SC 1624 (India).

4 T. Ramakrishna, *Liability of Intermediaries for Copyright Infringement in India*, 7 J. INTELL. PROP. L. & PRAC. 403 (2012).

5 Anjaiah Subrahmanyam, *Challenges of Copyright Protection in the Digital Era in India,* 14 J. WORLD INTELL. PROP. 399 (2019), available at https://jworldintelprop.org/challenges-digital-era (last visited Oct. 21, 2024).

6 *Id* at 5

7 Shreya Singhal v. Union of India, (2015) 5 SCC 1

8 D. Bach, *The Double Punch of Law and Technology: Fighting Music Piracy or Remaking Copyright in a Digital Age?,* 6 INT'L PUB. POL'Y REV. 1 (2004), https://doi.org/10.2202/1469-3569.1089 (Last visited Oct. 21, 2024)

9 *Id* at 8

The widespread accessibility of digital platforms and the anonymity offered by the internet exacerbate the problem of enforcement. Copyright holders, such as authors, musicians, filmmakers, and software developers, often find it difficult to track and prevent unauthorized use of their works, especially when infringing material is hosted on servers in different jurisdictions.[10] Many websites and digital platforms enable mass sharing of content, and infringers can easily alter or redistribute the content even after takedown requests. Digital copyright infringement is a violation of both national and international copyright laws, and it undermines the economic interests of creators by depriving them of potential revenue from their works.[11] In India, copyright is primarily governed by the Copyright Act, 1957, which has been amended to address issues related to the digital environment. Additionally, the Information Technology Act, 2000 plays a complementary role in addressing cybercrimes, including digital copyright infringement.[12] However, enforcement of these laws remains a challenge due to the anonymity of the internet, jurisdictional complexities, and the dynamic nature of digital content sharing.

One key aspect of digital copyright infringement is the role of intermediaries, such as internet service providers (ISPs), social media platforms, and search engines, in facilitating or preventing the spread of infringing content. In many cases, intermediaries are protected by "safe harbor" provisions, such as Section 79 of the Information Technology Act, which limits their liability as long as they act promptly upon receiving a takedown notice.[13] However, the effectiveness of these provisions is often debated, as copyright holders may face delays in getting infringing content removed.

In summary, digital copyright infringement represents a significant challenge in the digital age, as it exploits the ease of access, replication, and distribution of content online. Despite existing laws and mechanisms to protect intellectual property, ongoing efforts are needed to address the evolving nature of infringement, including improving international cooperation, updating legal frameworks, and leveraging technology to better protect creators' rights in the digital environment.[14] The digital age has presented new challenges in balancing the interests of creators, who seek to protect their intellectual property, and the public, who desire access to a wealth of digital content. Individuals now have the capability to easily access and copy vast amounts of digital information, often without a clear understanding of the legal boundaries.This has led to a growing debate over the appropriate level of copyright protection and the extent to which individuals should be able to freely use and share digital content.[15]

IMPORTANCE OF COPYRIGHT PROTECTION IN THE DIGITAL ERA

Copyright protection in the digital era is of paramount importance due to the transformative nature of how creative works are created, distributed, and consumed online. As the internet has become a global marketplace for content, ranging from music, films, books, software, and artwork to research and educational materials, the need to safeguard the intellectual property (IP) of

10 D. Bach, *Supra* note 8

11 S. Kierkegaard, *Outlawing Circumvention of Technological Measures Going Overboard: Hollywood Style*, 22 COMPUT. L. & SEC. REV. 46 (2006), https://doi.org/10.1016/j.clsr.2005.11.002. (lat visited Mar. 21, 2024)

12 Information Technology (Intermediaries Guidelines) Rules, 2011, Ministry of Electronics and Information Technology, available at https://www.meity.gov.in/content/information-technology-intermediaries-guidelines-rules-2011 (last visited Oct. 21, 2024).

13 *Id* at 12

14 D. Harris, *The New Prohibition: A Look at the Copyright Wars Through the Lens of Alcohol Prohibition*, RELX GROUP (NETH.), (2012), https://doi.org/10.2139/ssrn.2095193 (last visited Mar. 21, 2024)

15 *Id* at 14

creators has never been more critical. Copyright protection ensures that creators retain control over their works, allowing them to benefit financially from their creations and prevent unauthorized use, replication, or distribution. Without strong copyright laws in place, the digital environment could quickly become a lawless space where the hard work and innovation of individuals are devalued, undermining not only creators but also the industries that rely on intellectual property to thrive.

One of the key roles of copyright protection in the digital era is to provide creators with a legal mechanism to control how their works are used. This includes the right to authorize or deny the reproduction, adaptation, or distribution of their content online. In a world where digital content can be replicated and shared instantaneously and globally, copyright serves as a shield against unauthorized exploitation.[16] This is crucial not only for artists, authors, musicians, and filmmakers but also for software developers, researchers, and educators whose work is vulnerable to being copied or misappropriated online. By securing these rights, copyright law incentivizes creativity, encouraging people to produce new and original works with the confidence that they will be able to profit from their endeavours.

Moreover, copyright protection ensures the sustainability of industries that rely on the production and sale of creative works, such as the film, music, publishing, and software industries. In the absence of strong legal safeguards, piracy and digital copyright infringement could severely erode the profits of these industries, leading to job losses, reduced investments in new content, and a decline in the overall quality of cultural and intellectual products.[17] Copyright protection, therefore, plays a vital role in supporting the economy by maintaining a fair marketplace for the distribution and consumption of creative content.

Additionally, copyright fosters innovation by promoting a balance between the rights of creators and the public's access to knowledge and information.[18] In the digital era, this balance is particularly important, as it allows for the legal use of copyrighted materials in education, research, and other transformative works, such as reviews, commentaries, and parodies. This balance encourages the dissemination of ideas and culture while ensuring that creators are fairly compensated. Another crucial aspect of copyright protection in the digital era is its ability to adapt to new technologies, such as streaming platforms, social media, and blockchain. As content consumption habits evolve, copyright law must keep pace with technological advancements to prevent exploitation of creators' works in new, unregulated spaces.[19] For example, platforms that enable mass sharing of content, such as YouTube, Facebook, and Spotify, have to implement copyright protection measures like Content ID and takedown notices to ensure that creators' rights are not infringed.

In the digital age, the need for robust copyright protection has become increasingly paramount. Organized copyright holders, such as the recording, motion picture, and publishing industries, have adopted a dual-pronged approach to combat the pervasive challenge of digital piracy. On one hand, they have sought to electronically enclose information through the use of digital encryption technologies; on the other, they have lobbied for and obtained laws that penalize tampering with such electronic locks, regardless of the motivation. The rationale behind this "double punch of law and technology" is a subject of debate.[20] While the industry maintains that these measures are necessary to combat digital piracy, some argue

16 S. Kierkegaard, *supra* note 11

17 S. Kierkegaard, *supra* note 11

18 S. Kierkegaard, *supra* note 11

19 A. Okerson & S. Sully, *The Digital Dilemma: Intellectual Property in the Information Age*, 38 CHOICE 1184 (2000), https://doi.org/10.5860/choice.38-1184. (last visited 24 Feb. 2024)

20 *Id* at 19.

that the underlying motivation is to fundamentally reshape copyright in the digital age by altering consumer expectations. As digital information becomes the norm, copyright and intellectual property rules increasingly define what property actually is. Unauthorized copying of copyrighted materials and the demand for stronger intellectual property rights is not a new phenomenon; it occurs every time technology evolves to make the reproducibility of works more accessible.

In summary, copyright protection in the digital era is vital to ensuring that the creative economy flourishes, providing incentives for innovation and maintaining a balance between the interests of creators and public access. It is the cornerstone of a sustainable, fair, and equitable digital content ecosystem.[21]

RELEVANCE OF THE IT ACT, 2000

The Information Technology Act, 2000 (IT Act) is one of the most significant pieces of legislation in India aimed at regulating the digital landscape and ensuring that legal frameworks keep pace with technological advancements. Enacted on October 17, 2000, the IT Act was designed to provide legal recognition to electronic commerce and digital transactions, while also addressing cybercrimes and electronic governance. Its relevance has grown exponentially over the years as the country continues its rapid digital transformation. This act, which originally intended to promote e-commerce and reduce the barriers to digital trade, now plays a pivotal role in governing almost all digital interactions in India, making it indispensable in modern times.[22]

One of the key reasons for the IT Act's continued relevance lies in its provision of legal recognition to electronic records and digital signatures. Before the act, Indian law did not recognize electronic contracts and documents, which posed a significant barrier to businesses moving online. The IT Act not only validated electronic transactions but also paved the way for a robust e-commerce sector, providing a framework that ensures the validity and enforceability of digital agreements. It helped boost confidence in online transactions, accelerating the digitization of services across industries such as banking, insurance, and retail.

In terms of governance, the IT Act enables electronic filing of documents with government agencies and facilitates digital governance by enabling e-governance frameworks.[23] This is particularly important for a country like India, where many citizens, especially those in rural and remote areas, face logistical barriers to accessing physical government offices. By allowing services such as tax filings, application submissions, and grievance redressal to be conducted online, the IT Act has democratized access to governance.[24] This aligns with India's larger vision of a Digital India and improves public service delivery by making it faster, more transparent, and less cumbersome.

The IT Act is also crucial in addressing cybercrime and data protection. Over the past two decades, cyber threats such as hacking, data breaches, identity theft, and online fraud have become increasingly sophisticated, necessitating strong legal frameworks to tackle these challenges.[25] The IT Act, through provisions such

21 J. Berti, *Copyright Infringement and Protection in the Internet Age*, 11 IEEE IT PROF. 42 (2009), https://doi.org/10.1109/mitp.2009.118. (last visited 24 Feb. 2024)

22 Information Technology (Intermediaries Guidelines) Rules, 2011, Ministry of Electronics and Information Technology, available at https://www.meity.gov.in/content/information-technology-intermediaries-guidelines-rules-2011 (last visited Oct. 21, 2024).

23 Information Technology (Intermediaries Guidelines) Rules, 2011, Ministry of Electronics and Information Technology, available at https://www.meity.gov.in/content/information-technology-intermediaries-guidelines-rules-2011 (last visited Oct. 21, 2024).

24 *Id* at 23.

25 Information Technology (Intermediaries Guidelines) Rules, 2011, Ministry of Electronics and Information Technology, available at https://www.meity.gov.in/content/information-technology-intermediaries-guidelines-rules-2011 (last visited Oct. 21, 2024).

as Section 66, penalizes cybercriminal activities, including hacking, identity theft, and unauthorized access to computer systems. Section 67 addresses offensive content like cyber pornography, a growing concern in the digital age. Despite these provisions, however, many critics argue that the law has not kept up with the scale of evolving cyber threats.[26] With increasing concerns about data privacy, cyber espionage, and ransomware, many believe the law needs further updates to meet contemporary cybersecurity challenges more effectively.

A landmark amendment to the IT Act came with the Information Technology (Amendment) Act, 2008, which significantly expanded the scope of the law to include emerging digital crimes like phishing, child pornography, and cyberterrorism. The amendment also introduced provisions for intermediary liability, holding service providers such as social media platforms and ISPs accountable for user-generated content under certain conditions. This concept is vital in today's social media-driven world, where online platforms have become venues for misinformation, hate speech, and content violations.[27]

While the IT Act has played a critical role in shaping India's digital policy, it is not without its challenges. Data privacy remains a key area of concern. With the explosion of personal data being shared online and across various platforms, the IT Act's provisions for data protection, as outlined in Sections 43A and 72A, are considered insufficient by many experts.[28] These sections deal with compensation for failure to protect sensitive personal data and unauthorized disclosure of information, but they fall short of offering a comprehensive data protection framework. India's Personal Data Protection Bill, once enacted, is expected to address many of the shortcomings in this regard and work in conjunction with the IT Act.[29]

Another significant aspect of the IT Act is the power it grants to authorities for surveillance and blocking content. Section 69 of the IT Act allows the government to intercept, monitor, or decrypt any information generated, transmitted, received, or stored in any computer resource if deemed necessary for national security, public order, or to prevent incitement to the commission of any cognizable offense. While these powers are justified as a tool to maintain law and order, they have raised concerns about state surveillance and privacy violations. Critics argue that the lack of judicial oversight in such provisions could potentially lead to misuse and infringe upon individual rights. This was a major point of contention during the infamous Section 66A debacle. Section 66A, which penalized offensive messages sent online, was struck down by the Supreme Court of India in 2015 on the grounds that it violated free speech, highlighting the importance of maintaining a balance between regulation and individual freedoms in the digital realm.[30]

The IT Act is also relevant in the context of digital financial transactions, especially with the rise of fintech companies and digital payments in India. The law provides a secure framework for online financial dealings by ensuring data integrity, authenticity, and confidentiality. With the growing use of the Unified Payments Interface (UPI) and digital wallets, the IT Act, along with the RBI's guidelines, forms a critical component in protecting users from online fraud and financial scams.[31] This role became even more crucial during the COVID-19 pandemic, which saw a massive shift towards digital platforms, making secure online transactions indispensable to economic activity.

26 *Id* at 25

27 *Id* at 26

28 Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India)

29 T.N. Varma & D. Khan, *Curbing Cyber Crimes by Indian Law*, RELX GROUP (Neth.), (2017), https://doi.org/10.2139/ssrn.2922365 (last visited 24 Feb. 2024)

30 *Id* at 29

31 T.N. Varma & D. Khan, *supra* Note 30

Furthermore, the IT Act is important in the context of emerging technologies like artificial intelligence (AI), blockchain, and the Internet of Things (IoT).[32] While the original legislation did not anticipate these advancements, its flexible framework has allowed for adaptation to new technological realities. For instance, blockchain technology, which relies on cryptographic principles, finds indirect legal validity through the IT Act's provisions on digital signatures and electronic records.[33]

In conclusion, the Information Technology Act, 2000 remains highly relevant in India's rapidly growing digital ecosystem. It serves as a foundation for e-commerce, cybercrime regulation, and e-governance, while also addressing data protection and privacy issues. However, given the ever-evolving nature of technology, continuous amendments and supplementary legislation are necessary to ensure that the IT Act remains effective. With rising concerns over privacy, cybersecurity, and the regulation of new technologies, the IT Act will need to adapt further to protect the interests of individuals and businesses while promoting innovation and growth in India's digital economy. As the country moves toward a more digital future, the IT Act's relevance will only increase, provided it evolves to meet emerging challenges.

OBJECTIVE OF THE IT ACT IN REGULATING CYBER ACTIVITIES

The Information Technology Act, 2000 (IT Act) was enacted with the primary objective of regulating and facilitating lawful digital activities, while providing a legal framework to address cybercrimes and other issues arising from the growing reliance on electronic communications and transactions. With the rapid advancement of technology and the internet's pervasive influence on commerce, governance, and daily life, the IT Act was designed to ensure that legal systems could adapt to the challenges posed by cyberspace. The main objective of the IT Act is to provide legal recognition to electronic records, digital signatures, and electronic commerce, making it easier for businesses and individuals to engage in online transactions securely and efficiently.[34] One of the most important objectives of the IT Act is to foster confidence in electronic commerce by ensuring the authenticity, integrity, and security of online transactions. The Act provides for the use of digital signatures, which are legally valid and can authenticate documents, making it easier to conduct business over the internet. This aspect of the Act was critical in boosting India's digital economy and promoting the use of online financial services, e-governance, and e-commerce.[35]

In addition to promoting digital commerce, the IT Act is focused on regulating cyber activities to prevent and combat cybercrime. It lays down provisions that address offenses such as hacking, data theft, identity theft, online fraud, and cyberstalking. Sections like 66 and 66C deal with issues such as unauthorized access to computer systems and identity theft, while Section 67 tackles the transmission of obscene content online.[36] By criminalizing these activities, the IT Act seeks to create a safer digital environment, protecting individuals and businesses from the growing threats posed by cybercriminals. Another objective of the IT Act is to promote electronic governance by facilitating the use of digital records and communications in government processes. This enables citizens to interact with government agencies digitally, thereby streamlining services such as tax filings, license applications, and grievance redressal. Through the use of electronic records, the IT Act makes public

32 T.N. Varma & D. Khan, *supra* Note 30

33 T.N. Varma & D. Khan, *supra* Note 30

34 Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

35 *Id* at 34

36 Information Technology (Intermediaries Guidelines) Rules, 2011, Ministry of Electronics and Information Technology, available at https://www.meity.gov.in/content/information-technology-intermediaries-guidelines-rules-2011 (last visited Oct. 21, 2024).

services more accessible, particularly for those in remote or underserved areas, aligning with the larger Digital India initiative.[37] The IT Act also plays a crucial role in regulating intermediaries like social media platforms and internet service providers (ISPs). These intermediaries are required to follow due diligence in monitoring and controlling user-generated content to prevent the spread of illegal activities, such as hate speech or content promoting terrorism. Section 69A, which grants the government the power to block access to certain websites or content in the interest of national security, reflects the Act's objective to maintain law and order in the digital space.

Since the advent of the digital age, the rapid proliferation of technology and the widespread adoption of the internet have transformed the landscape of human communication and interaction, ushering in a new era of interconnectivity and global exchange. However, this paradigm shift has also given rise to a growing concern: the emergence of cyber crimes, which can transcend physical boundaries[38] and pose a threat to individuals, organizations, and nations alike. In response to this challenge, the Indian government enacted the Information Technology Act in the year 2000, with the primary objective of regulating and governing cyber activities within the country. The Act was designed to address a wide range of digital offenses, including unauthorized access to computer systems, data theft, and the misuse of information technology for malicious purposes. As highlighted by various studies, the IT Act represents a pioneering effort to establish a legal framework for the digital age. However, the implementation and enforcement of the Act have not been without their challenges.[39] The rapid evolution of technology and the increasing complexity of cyber threats have at times outpaced the legislation, leaving gaps in the law and creating difficulties for law enforcement authorities and the judiciary in effectively addressing emerging cyber-related issues.

In conclusion, the overarching objective of the IT Act is to create a secure, transparent, and legally sound framework for digital activities, promoting the growth of e-commerce, safeguarding against cybercrimes, and enabling efficient governance. As cyber activities continue to evolve, the IT Act's regulatory scope ensures that India can address the dynamic challenges posed by technology, while protecting its citizens, institutions, and businesses in cyberspace.[40]

LEGAL FRAMEWORK GOVERNING DIGITAL COPYRIGHT INFRINGEMENT IN INDIA

In the digital age, the issue of copyright infringement has become increasingly complex, with the advent of various technologies that enable the unauthorized reproduction and distribution of copyrighted content. India, as a rapidly developing nation, has had to grapple with the challenges posed by digital piracy and the need to ensure a robust legal framework to protect intellectual property rights. The proposed introduction of provisions related to the WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty in India, despite the country not being a signatory to these treaties, raises questions about the true purpose and rationale behind such a move.

While the escalating problem of piracy may have prompted this initiative, a deeper analysis of the manner in which these provisions have evolved in the international arena and the continued debate surrounding their introduction is necessary. The Indian entertainment industry, particularly the rapidly growing and internationally renowned cinema sector, has been increasingly attracting

37 Information Technology (Intermediaries Guidelines) Rules, 2011, Ministry of Electronics and Information Technology, available at https://www.meity.gov.in/content/information-technology-intermediaries-guidelines-rules-2011 (last visited Oct. 21, 2024)

38 *Supra* note 5

39 Myspace Inc. v. Super Cassettes Industries Ltd., (2017) 236 DLT 478 (Delhi).

40 Viacom18 Media Pvt. Ltd. v. Bharti Airtel Ltd., (2017) 241 DLT 469 (Delhi).

foreign investment.[41] As the industry becomes more corporatized, there is a perceived need to protect these investments through the implementation of Digital Rights Management systems, which are seen as a solution to combat the loss caused by unauthorized reproduction and distribution of copyrighted works. The legal framework governing digital copyright infringement in India is primarily rooted in the Copyright Act, 1957, which was amended in 2012 to address the challenges posed by the digital age. The amendment brought India's copyright laws in line with international standards, especially concerning digital content, online platforms, and the internet.[42]

The framework is supported by provisions in the Information Technology Act, 2000 (IT Act), which also plays a crucial role in regulating online behaviour and protecting digital rights, including those of copyright holders. The Copyright Act, 1957 protects the rights of authors, composers, filmmakers, and other creators over their original works. These rights include the exclusive control over reproduction, distribution, and communication of the work to the public, including in digital formats. With the growing use of the internet for distributing and consuming content, issues related to copyright infringement in the digital realm have surged. To counter these challenges, the 2012 amendment introduced provisions specifically targeting online copyright infringement, making unauthorized digital reproduction and distribution of copyrighted content, such as music, films, e-books, and software, a punishable offense. Under Section 51 of the Copyright Act, copyright infringement occurs when a person, without authorization, reproduces or communicates a work to the public. In the digital context, this includes unauthorized uploading, downloading, or sharing of copyrighted material on websites, peer-to-peer networks, or through any other digital platform. Such acts are considered copyright violations and can lead to both civil and criminal penalties. Section 63 prescribes criminal liability, including imprisonment and fines, for those found guilty of wilful infringement.[43]

The Information Technology Act, 2000 complements the Copyright Act by providing a legal framework for addressing cybercrimes and regulating online platforms. Section 79 of the IT Act provides a safe harbor provision for intermediaries such as internet service providers (ISPs), hosting platforms, and social media websites.[44] This means that intermediaries are not liable for third-party content on their platforms, provided they follow due diligence and remove infringing content once notified by the copyright holder.[45] This is a critical aspect of the legal framework, as it places responsibility on intermediaries to assist in preventing the spread of pirated or unauthorized digital content. In addition to domestic laws, India is also a signatory to various international treaties that influence its digital copyright framework, such as the Berne Convention for the Protection of Literary and Artistic Works, the WIPO Copyright Treaty, and the TRIPS Agreement (Trade-Related Aspects of Intellectual Property Rights). These international obligations ensure that India's copyright laws adhere to global standards, especially in the digital context. To strengthen enforcement, the Delhi High Court and other Indian courts have issued dynamic injunctions against websites involved in copyright infringement, particularly in cases of film and music piracy.[46] These injunctions allow

41 *Id* at 40

42 A. Bamrara, The Challenge of Cyber Crime in India: The Role of Government, RELX Group (Neth.), (2012), https://doi.org/10.2139/ssrn.2488909 (last visited 24 Feb. 2024).

43 *Id* at 42

44 N. Sensarkar, The Potential Impact of Digital Rights Management on the Indian Entertainment Industry, 6 J. Info., Comm. & Ethics in Soc'y 45 (2007), https://doi.org/10.1108/14770020780000549 (last visited 24 Feb. 2024)

45 *Id* at 44.

46 A. Misra & M. Chacko, Square Pegs, Round Holes, and Indian Cybersecurity Laws, 2 Cybersecurity 57 (2021), https://doi.org/10.1365/s43439-021-00026-7 (last visited 24 Feb. 2024)

courts to direct ISPs to block websites that host pirated content, even if the infringers continuously change domain names to avoid detection.

In conclusion, the legal framework governing digital copyright infringement in India is a comprehensive blend of the Copyright Act, 1957 and the Information Technology Act, 2000, supplemented by international agreements and judicial precedents. These laws aim to protect the rights of creators in the digital space while balancing the responsibilities of online platforms and intermediaries in preventing the proliferation of infringing content.

KEY PROVISIONS RELATED TO CYBERCRIMES AND ONLINE CONTENT

India's legal framework to combat cybercrimes and regulate online content is anchored primarily in the Information Technology Act, 2000 (IT Act), along with relevant sections from the Indian Penal Code (IPC) and certain special laws. The IT Act, enacted to provide legal recognition to digital transactions and e-governance, has evolved into a crucial tool for dealing with various forms of cybercrime and regulating online behaviour in a growing digital economy. A key provision related to cybercrimes under the IT Act is Section 66, which broadly deals with hacking and the unauthorized access to computer systems. [47]It makes it an offense to dishonestly or fraudulently access any computer, network, or system. Offenders can face imprisonment of up to three years and fines. Section 66C addresses identity theft by criminalizing the use of someone else's personal information, such as passwords, digital signatures, or unique identification features, for fraudulent purposes. The section imposes penalties of up to three years of imprisonment and fines.[48]

Further expanding on cybercrimes, Section 66D specifically deals with cheating by impersonation through electronic communication and makes online fraud, including phishing scams, a punishable offense. Section 66E targets privacy violations by prohibiting the capturing, publishing, or transmitting private images of individuals without their consent, thus protecting individuals from breaches of privacy, which are increasingly common with the widespread use of smartphones and social media. Another critical provision is Section 67, which deals with obscene content online.[49] It prohibits the publishing or transmission of any obscene material in electronic form, with penalties ranging from imprisonment to fines. The Act also has provisions for child pornography under Section 67B, making it illegal to digitally create, publish, or distribute any material depicting children in sexually explicit acts, with stringent punishments for offenders.

Section 69A of the IT Act grants the Indian government the power to issue directives for blocking public access to any information or content on the internet, which it deems necessary for reasons of national security, public order, or to prevent incitement of any cognizable offense. This section has been pivotal in regulating online content in India, especially in cases involving the blocking of websites that host illegal, offensive, or anti-national content. Section 69 provides government agencies the authority to intercept, monitor, or decrypt any information in any computer resource for national security or to prevent and investigate offenses. This provision, though important for security, raises concerns about state surveillance and privacy. The use of this section is closely scrutinized, as it can potentially conflict with personal freedoms guaranteed by the Constitution of India.

The Indian Penal Code (IPC) also supports the regulation of cybercrimes. For instance, Section 499 deals with online defamation, allowing individuals to seek redress if they have been defamed through online platforms. Similarly, Section 507 punishes

47 *Id* at 46

48 *Id* at 47

49 A. Bamrara, The Challenge of Cyber Crime in India: The Role of Government, RELX Group (Neth.), (2012), https://doi.org/10.2139/ssrn.2488909 (last visited 24 Feb. 2024)

individuals who send threatening or intimidating messages via digital communication. Overall, India's cybercrime and online content regulation provisions are aimed at creating a safe and secure cyberspace while balancing privacy concerns, freedom of speech, and national security.[50] These provisions address a wide range of cyber offenses, from data theft and hacking to more complex crimes such as online defamation and child pornography. However, with the rapid evolution of technology, continuous updates and amendments are necessary to keep the legal framework relevant and effective.

CHALLENGES UNDER THE IT ACT, 2000 IN ADDRESSING DIGITAL COPYRIGHT INFRINGEMENT

The advent of digital technologies has posed significant challenges to the traditional copyright regime in India. While the Indian Copyright Act of 1957 addressed the challenges of the analog era, the emergence of the internet and digital distribution platforms has necessitated amendments to keep pace with the changing landscape. The Information Technology Act, 2000 was introduced to govern the digital space, including provisions related to digital rights management.

However, the effectiveness of the IT Act in addressing the issue of digital copyright infringement has been a subject of debate. The proposed introduction of digital rights management provisions, even though India is not a signatory to the relevant WIPO treaties, raises questions about the true purpose of these amendments. The rationale behind the inclusion of these provisions is not entirely clear, and their introduction requires a more thorough analysis in the context of international and domestic legislative trends, as well as the ongoing debate surrounding their effectiveness in tackling the escalating problem of digital piracy.

Lack of specific provisions for digital copyright infringement

The lack of specific provisions for digital copyright infringement in India presents a significant challenge in addressing the complexities of protecting intellectual property in the digital age. While the Copyright Act, 1957, along with its 2012 amendment, and the Information Technology Act, 2000 (IT Act), cover certain aspects of digital copyright, there remain significant gaps in the legal framework that make it difficult to tackle the unique issues posed by the internet and evolving technology. One of the key issues is that the Copyright Act was initially framed at a time when digital platforms and the internet were not widespread. While the 2012 amendment sought to address some of the concerns related to the online space, it primarily focused on traditional copyright violations and lacked comprehensive provisions that deal exclusively with the complexities of digital copyright infringement. The growth of online streaming, social media platforms, and peer-to-peer sharing networks has introduced new avenues for infringement, but the legal provisions for tackling these forms of violations remain insufficient.

For instance, the current legal framework does not adequately address digital piracy or the unauthorized sharing of copyrighted materials across online platforms. Websites that host pirated movies, music, software, and other digital content continue to proliferate due to the lack of a robust and dedicated mechanism to take down such sites or penalize those involved in the operation of these platforms. The blocking of infringing websites, often pursued under Section 69A of the IT Act, is a reactive measure and can be circumvented by the infringers by switching to new domain names or creating mirror sites. Furthermore, the Copyright Act's existing provisions are geared more towards physical reproduction and distribution of copyrighted works, and do not adequately cover the streaming or downloading of copyrighted content online without the rights holder's permission.

50 Ibid

Another significant gap is the lack of detailed provisions for regulating intermediaries like internet service providers (ISPs), hosting platforms, and social media networks. While Section 79 of the IT Act provides intermediaries with safe harbor protection, which shields them from liability for third-party content, it also requires them to act with due diligence and remove infringing content once notified by the copyright holder. However, the process for enforcing these takedown requests is often slow and inefficient. There is no clear, uniform mechanism to ensure compliance, and intermediaries are not held accountable enough for failing to prevent the spread of infringing content on their platforms. In practice, this means that pirated content often remains accessible even after takedown requests are issued, which undermines the protection of copyright in the digital space.

Moreover, the current framework does not provide sufficient deterrence for digital copyright infringement. Penalties for copyright violations, as outlined in Section 63 of the Copyright Act, include fines and imprisonment, but these penalties are often not stringent enough to deter online infringers, particularly given the low likelihood of enforcement in many cases. Digital infringers can operate anonymously or from foreign jurisdictions, making it difficult to track them down and impose legal consequences. The international nature of digital copyright infringement also poses jurisdictional challenges. Copyright laws in India are not harmonized with international standards to the extent necessary for tackling cross-border online infringements. In the absence of a global framework to effectively combat piracy and other forms of digital copyright infringement, India's existing laws struggle to provide adequate remedies for violations that occur outside its borders but affect Indian rights holders.

In conclusion, while India's legal framework provides some level of protection against digital copyright infringement, the lack of specific provisions addressing the unique challenges of the digital environment hampers the effectiveness of the law. Comprehensive reforms, including clear intermediary liability, enhanced enforcement mechanisms, and stronger penalties, are needed to safeguard intellectual property rights in the digital realm.

Overlap between IT Act and Copyright Act leading to confusion

The overlap between the Information Technology Act, 2000 (IT Act) and the Copyright Act, 1957, especially in the context of digital content, has led to significant confusion in India's legal landscape. While both laws aim to regulate different aspects of online activities—cybercrimes for the IT Act and intellectual property rights for the Copyright Act—their areas of intersection, particularly regarding digital copyright infringement, create ambiguity in enforcement and legal interpretations. One of the key areas of overlap is in how online copyright violations are handled. The Copyright Act governs the protection of intellectual property, including the exclusive rights of creators over the reproduction and distribution of their works. It has provisions for civil remedies and criminal penalties for unauthorized use of copyrighted material. On the other hand, the IT Act was designed to address crimes related to the internet and electronic data. As more copyright violations, such as illegal downloading, streaming, and distribution, occur in the digital space, the IT Act has become relevant to online infringements, but it was not specifically crafted for this purpose. The result is that digital copyright violations can fall under both acts, leading to confusion about which provisions should be invoked in a particular case. For instance, Section 66 of the IT Act deals with offenses like hacking and unauthorized access to computer systems, which could be applicable in cases where copyrighted material is unlawfully obtained or distributed through hacking or cyber theft. However, copyright infringement, specifically, is already addressed in Section 51 and Section 63 of the Copyright Act. This creates uncertainty over whether an infringer should be prosecuted under the IT Act, the Copyright Act, or both.

Another area of overlap is the treatment of intermediaries like internet service providers (ISPs), social media platforms, and websites hosting user-generated content. Section 79 of the

IT Act provides intermediaries with a safe harbor provision, shielding them from liability for content hosted on their platforms as long as they act with due diligence and remove infringing content upon notification. Meanwhile, under the Copyright (Amendment) Act, 2012, intermediaries are also required to take down infringing content when notified by the rights holders. The process for issuing these takedown requests is not uniformly defined, and the safe harbor provisions can sometimes be interpreted as conflicting with the obligations under the Copyright Act. For instance, does a platform face criminal liability if it fails to act on a takedown request under the Copyright Act, or can it still claim safe harbour under the IT Act? The situation becomes more complex when considering penalties for copyright infringement. The Copyright Act imposes penalties like fines and imprisonment for wilful infringement, while the IT Act also allows for imprisonment and fines for cybercrimes related to unauthorized access and distribution. The challenge here is determining whether both acts apply in cases of digital copyright infringement or if one act supersedes the other. Courts often have to decide whether to treat online copyright infringement as a violation of intellectual property laws or as a cybercrime, leading to inconsistent outcomes in different cases.

Moreover, the jurisdictional aspect adds another layer of complexity. The IT Act has extraterritorial jurisdiction, allowing Indian authorities to pursue cybercrimes committed outside India if they involve Indian citizens or computer systems based in India. However, the Copyright Act does not provide such broad powers for pursuing international copyright infringers, creating challenges in tackling cross-border digital piracy. This further complicates enforcement, as cases involving international infringers might be addressed differently under the two acts.

In conclusion, the overlap between the IT Act and the Copyright Act leads to confusion in enforcement, legal interpretation, and liability concerning digital copyright infringement. This confusion underscores the need for clearer definitions and better coordination between the two laws, possibly through specific amendments or guidelines to ensure that online copyright violations are addressed efficiently and uniformly.

Cross-border nature of digital content

The cross-border nature of digital content presents significant challenges in regulating and enforcing laws in the digital age. The internet, by its very design, is a global network that allows content to flow freely across geographical boundaries, making it difficult for national laws to effectively regulate content hosted or accessed from foreign jurisdictions. This borderless nature of digital content amplifies the complexity of legal, regulatory, and enforcement issues, particularly when it comes to areas such as copyright infringement, data privacy, defamation, cybercrimes, and hate speech. One of the most prominent challenges is the enforcement of copyright laws in the digital space. While countries like India have laws to protect intellectual property rights, these laws typically apply within the country's borders. However, digital copyright violations often involve websites or platforms hosted in foreign countries, making it difficult to hold violators accountable. For instance, a website hosting pirated movies or music may operate out of a country with lax copyright laws, or where enforcement mechanisms are weak or non-existent. Even if the rights holder obtains a court order in their home country to block the infringing website, the website operators can easily shift their servers to another jurisdiction or change the website's domain name to circumvent the ruling. This constant cat-and-mouse game makes enforcing copyright in the digital age a global challenge.

Moreover, different countries have varying legal standards and approaches to regulating content. What may be deemed illegal or offensive in one country may be considered acceptable or protected under the laws of another. For instance, content that violates free speech norms or contains hate speech in one country may be allowed in another jurisdiction where such regulations are more lenient. This creates a disconnect between national regulatory regimes and the global nature of digital platforms like Facebook, Twitter, or YouTube, which serve audiences across multiple countries.

The problem is further compounded when such platforms fail to effectively moderate or remove harmful content that violates local laws, sparking debates about jurisdiction and liability. The cross-border flow of data also raises significant concerns about data privacy and protection. For example, personal data collected from users in one country may be stored or processed on servers located in a different country, making it difficult to ensure compliance with local data protection laws. This is especially critical in cases involving sensitive data, such as healthcare or financial information. Countries like India have introduced stringent laws governing data localization and cross-border data flows to protect citizens' personal data, but enforcement of such laws is challenging when the data resides outside national borders.

The jurisdictional issues associated with cross-border digital content are also evident in cases of cybercrimes. A cyberattack targeting a company or individual in one country may be orchestrated by perpetrators located in another country. The lack of global consensus on how to handle such cross-border cybercrimes, coupled with varying levels of cooperation between law enforcement agencies in different jurisdictions, complicates the investigation and prosecution of such offenses. In response to these challenges, international cooperation and harmonization of laws are increasingly being sought to address the cross-border nature of digital content. Initiatives such as mutual legal assistance treaties (MLATs), extradition agreements, and international treaties aim to streamline cooperation between countries on issues related to digital content, including copyright enforcement, data privacy, and cybercrime. However, these efforts are often hampered by differing national interests, legal systems, and levels of technological development.

In conclusion, the cross-border nature of digital content introduces a range of legal and regulatory challenges that require coordinated global efforts. While the internet enables the free flow of information, it also complicates the enforcement of national laws. As digital content continues to transcend borders, addressing these challenges will require robust international cooperation, harmonized legal frameworks, and stronger enforcement mechanisms to ensure accountability in the digital realm.

RECOMMENDATIONS FOR STRENGTHENING THE IT ACT, 2000

Strengthening the Information Technology Act, 2000 (IT Act) is essential to address the rapidly changing digital landscape in India. As cybercrimes and online challenges evolve, the IT Act needs to be updated to ensure effective governance, security, and protection of digital rights. Below are some key recommendations for strengthening the IT Act:

- **Updating Definitions and Expanding Scope:** The IT Act should be updated to include clearer definitions and provisions for emerging cybercrimes. New digital threats such as cyberstalking, cyberbullying, deepfakes, identity theft, ransomware, and cryptocurrency fraud should be explicitly addressed. Additionally, new technologies like artificial intelligence (AI) and blockchain should be included within the Act to ensure regulation over crimes associated with these technologies.
- **Enhancing Data Protection and Privacy:** Section 43A of the IT Act provides some data protection provisions, but these need to be strengthened significantly. Aligning the IT Act with international standards like the General Data Protection Regulation (GDPR) can help provide better protection to personal and sensitive data. The Act should also introduce stricter penalties for data breaches and non-compliance with data protection norms. Introducing provisions for data localization to ensure sensitive data stays within India would enhance security and compliance.
- **Strengthening Intermediary Liability:** Section 79 of the IT Act provides safe harbor to intermediaries like social media platforms and internet service providers (ISPs). However, this protection should come with clearer responsibilities and

higher accountability. Intermediaries should be required to take proactive measures to regulate harmful content, including misinformation, hate speech, child exploitation, and terrorist content. There should also be graded liability based on the size, reach, and influence of the platform to ensure that larger platforms with more users bear greater responsibility for content moderation.

- **Improving Cybersecurity Framework:** With rising incidents of cyberattacks, the IT Act needs more robust cybersecurity provisions. Introducing mandatory cybersecurity standards for organizations in both the public and private sectors would improve security preparedness. Additionally, there should be a legal obligation for organizations to report cyber incidents to a centralized agency like the Indian Computer Emergency Response Team (CERT-In). The Act could also mandate regular cybersecurity training for businesses and government organizations to increase awareness and readiness.
- **Addressing Cross-Border Data Flows and Cybercrime:** Given the global nature of cybercrimes, international cooperation is critical. Strengthening the IT Act's provisions for cross-border data flows and improving collaboration through mutual legal assistance treaties (MLATs) and extradition agreements would improve enforcement of cyber laws across jurisdictions. Indian cyber laws should be harmonized with global best practices to ensure smoother cooperation in dealing with international cybercrimes.
- **Clarifying Digital Copyright Provisions:** While the Copyright Act, 1957 governs intellectual property, the IT Act overlaps in addressing online copyright violations. To avoid confusion, the IT Act should have specific provisions for digital copyright infringement, particularly concerning the responsibilities of intermediaries in curbing digital piracy. Clearer distinctions between the IT Act and the Copyright Act are essential to ensure that cases of online infringement are handled efficiently.
- **Strengthening Digital Rights and Privacy Protections:** With increasing surveillance concerns, the IT Act should include explicit protections for digital privacy. Users' right to control their data and online activity must be safeguarded against unlawful surveillance, whether by private entities or the government. Strengthening privacy rights within the Act would balance digital innovation with individual rights protection.
- **Increased Focus on AI, Big Data, and Emerging Technologies:** As emerging technologies like AI, big data, Internet of Things (IoT), and blockchain become more prevalent, the IT Act must adapt to provide legal clarity around their use and associated risks. Provisions should be added to address automated decision-making, AI-driven crimes, and data ownership issues. This would ensure the responsible deployment of technology while minimizing its potential risks.
- **Introducing Penalties for Non-Compliance:** Strengthening the IT Act should include introducing stricter penalties for non-compliance with its provisions. Whether it involves data breaches, failure to report cybersecurity incidents, or negligence by intermediaries, appropriate penalties can act as a deterrent against violations.
- **Regular Review and Amendments:** Given the pace of technological advancement, the IT Act should be subject to periodic review and updates. A legal framework that evolves with technological advancements can better address emerging challenges in the digital ecosystem.

In conclusion, strengthening the IT Act involves updating it for modern cybercrimes, enhancing data protection, clarifying intermediary liability,

improving cybersecurity measures, and addressing cross-border digital challenges. A comprehensive overhaul will ensure that the Act remains relevant in today's dynamic digital environment, ensuring security, privacy, and accountability in cyberspace.

CONCLUSION

In conclusion, digital copyright infringement poses significant challenges under the IT Act, 2000, which, despite being a landmark legislation, falls short in addressing the complexities of online intellectual property violations. The borderless nature of the internet, coupled with the rapid evolution of technology, makes it difficult to enforce copyright protection, particularly when infringers operate from multiple jurisdictions. The overlap between the IT Act and the Copyright Act, 1957 further complicates enforcement, creating ambiguity in determining which law applies in specific cases of digital piracy or content misuse.

Additionally, the IT Act's provisions, such as Section 79 on intermediary liability, provide a degree of protection to digital platforms, but the lack of specific guidelines for handling digital copyright violations on such platforms leaves gaps in accountability. This, combined with the cross-border nature of content, makes it difficult to ensure compliance with copyright laws, as content hosted on servers in foreign jurisdictions often escapes the reach of Indian authorities. To effectively address these challenges, the IT Act must be strengthened with clearer provisions on digital copyright, stronger enforcement mechanisms, and better international cooperation to handle cross-border copyright infringement. Only with these changes can India fully protect the rights of creators and copyright holders in the digital age, ensuring that their intellectual property remains safeguarded in an increasingly interconnected and digital world.

REFERENCES:

1. Indian Copyright Act, 1957 (amended 2012).
2. Information Technology Act, 2000 (India).
3. WIPO Copyright Treaty, Dec. 20, 1996, S. Treaty Doc. No. 105-17.
4. Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299.
5. WIPO Performances and Phonograms Treaty, Dec. 20, 1996, 2186 U.N.T.S. 203.
6. The Berne Convention for the Protection of Literary and Artistic Works, Sept. 9, 1886, 1161 U.N.T.S. 31.
7. Indian Penal Code, 1860, §§ 499, 507.
8. Delhi High Court, UTV Software Communications Ltd. v. 1337X.to, (2019).
9. LexisNexis, Digital Copyright Law in India (11th ed. 2022).
10. LexisNexis, Cyber Law in India (8th ed. 2020).
11. Jonathan Band, Digital Copyright Reform: Bridging Law and Technology, 26 J. Copyright Soc'y 41 (2021).
12. Rakesh Mahajan, Challenges in Regulating Digital Copyright, 14 Ind. L.J. 67 (2020).
13. Neha Saxena, Enforcement of Copyright in the Digital Age, 9 J. Intell. Prop. L. & Prac. 202 (2022).
14. Sruti Bansal, Balancing Innovation and Copyright in the Internet Age, 17 Int'l J. Cyber L. 112 (2021).
15. LexisNexis, Indian Case Studies on Copyright and IT (9th ed. 2023).
16. U.S. Digital Millennium Copyright Act, 17 U.S.C. § 1201 et seq. (1998).
17. Indian Computer Emergency Response Team, Annual Cybercrime Reports (2023).
18. Shyamkrishna Balganesh, Reconceptualizing Copyright in the Digital Economy, 4 Harv. J. L. & Tech. 124 (2021).
19. LexisNexis, Practical Aspects of Copyright Law in India (10th ed. 2021).
20. LexisNexis, Cybersecurity and IT Laws (6th ed. 2021)