

## IPR Issues in Cyberspace: An Overview



Pooja, Assistant Professor  
advocatepoojarao@gmail.com  
Phone: +91-9899873049

### Abstract

The global economic development has been derived through Internet as a global medium. Internet provides new intellectual property rights and branding opportunities for conducting business globally and making it accessible to the consumers world-wide at affordable price. Again, it has also created new areas for various kinds of Intellectual Property Rights (IPR) infringement, disputes, cyber offences etc. In recent years, there has been much publicity about the unlawful distribution of intellectual property-protected music, films, art, photos, scripts, and software (content) on the Internet. These unauthorized downloads often violate national laws of copyright. Because of the ease with which digital files can be downloaded, unauthorized copying of content has been a major problem causing the loss of millions of dollars in revenue for the owners of these rights. The need of the hour is to do special efforts to fight such illegal activities to enhance the potential of IT sector in India. In order to keep the legal regime side by side with this change in the society, the Indian Parliament legislated the Information Technology Act, 2000. This paper attempts to provide an insight to the major issues being faced by India in the cyber space with respect to intellectual property rights and the recent laws to safeguard these rights thereto.

**Keywords:** Intellectual Property Rights, Data Protection, Information Technology Act, 2000, Software Piracy, Cyber Laws, Cyberspace

### Introduction

In the present era, Internet has come up as a global mean to drive global economic development. Internet provides new intellectual property rights and branding opportunities for spreading and conducting business globally and making it accessible to the consumers world-wide at affordable price. Again, it has also created new opportunities for various kinds of Intellectual Property Rights (IPR) infringement, disputes, cyber offences etc. India's growth in the internet space has been appreciable. India has made a huge growth in Information and Software Technology and is having compounded growth of more than 25% every year. However, the increasing use of Information Technology (IT), brings with it new challenges and threats like security threat, including data theft, piracy, hacking, identity theft, violation of intellectual property rights, etc. The need of the hour is to do special efforts to fight such illegal activities to enhance the potential of IT sector in India. In order to keep the legal regime side by side with this change in the society, the Indian

Parliament legislated the Information Technology Act, 2000.

### Intellectual Property Rights Over Internet

Most of the corporate Intellectual Properties are held in the digital form, Internet provides access of all the IPR resources at affordable price to public at large. However, infringement of IPR is also possible through internet, particularly; copying of Copyright material is very easy and simple. Internet is being termed as the world's biggest copying machine. In India there are specific legislations to deal with various kinds of IPR infringement however these legislations are not capable enough to deal with some of copyright violations in modern era. The Copyright Act, 1957 provides the prohibition to reproduce the copyrighted work in any material form including the storing of it in any medium by electronic means, by any unauthorized person but is not capable to deal with illegal duplication, importation, distribution and sale of pirated music as it becomes difficult to trace the location of information copied.

In the recent era, where the major function of internet is sharing of information among people, the peer-to-peer file sharing services provided by various websites, linking, deep linking, framing and other innovations which have changed the way people share information over the world wide web, have given rise to a legal controversy. While the users downloading software, music, computer games and other copyrighted material are held liable for direct copyright infringement, the service providers go scot free as the existing Copyright Act has no provision for making a service provider liable in such a situation. For tracking down copies of work that infringes IPRs, identifying the infringer and litigating in each concern jurisdiction, one has to spend a lifetime and fortune.

The Indian Copyright Act, 1957 and the IT Act, 2000 protects the computer software and other copyright issues over internet. While the Copyright Act grants protection to the computer program as it is granted to other forms of copyrighted work, the technological and complex nature of the computer programs calls for technically effective protection.

The Indian Copyright Act, 1957 protects computer software along with other forms of copyrighted work. The Copyright Act includes computer programs in literary works and gives the general exclusive rights provided to other literary works as well as it grants extraordinary exclusive rights to the owners of the computer programs like right to sell or offer for sale, and the right to give on commercial rental or offer for commercial rental. The Act has also exempted computer programs from 'fair dealing exception' (i.e., private use for research, criticism or review of that work or any other work) which is available in case of other copyright works.

The IT Act, 2000 provides for punishment for tampering with the 'source code' of a computer program but this protection applies to computer source codes 'which are required to be kept or maintained by law for the time being in force'. Hence, the protection accorded by the IT Act is only for 'source code' of computer programs of government agencies and the 'source code' of computer programs of private users still stand unprotected.

## Data Protection and Cybercrimes

Internet technology provides for storing a large number of personal Data. But this also creates a possibility of a threat to the privacy of a cyber consumer. With the increase in online service provider companies in India, misusing the personal data of a cyber consumer has become a major problem. However, we lack any specific legislation to protect the personal data of a person though to a little extent protection may be given under the Copyright Act, 1957. Countries like US and EU are having strict policies relating to privacy and protection of personal data. Moreover, it is very important for India, to promote the inflow of foreign investments and other business opportunities, to have specific data protection and privacy laws. Though, The Information Technology Act protects privacy rights of personnel only from government action and it is unclear if such protection can be extended to private actions as well.

The absence of data protection and privacy law has also been creating obstacles for Indian companies while dealing with the EU as the data protection directives require a very high level of protection. India needs to adapt to the changing needs of the time and provide for a comprehensive data protection regime which will not only help in gaining confidence in consumers but also increase the amount of business that Indian BPO service providers receive from the EU.

## Privacy Threats and Cybercrimes

This progress in technology has given a new shape to the various computer related crimes which runs through various territories thus creating jurisdictional issues all along the world. Some of the issues like identity theft, hacking, misuse of credit cards, leaking of critical information and frauds are mainly being faced by the Indian Cyber consumer. Some of these cyber offences are explained below:  
**Phishing and Pharming:** Phishing means to the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as password and credit card numbers. It may lead the user to disclose their personal data at their own will. Pharming means the fraudulent practice of directing internet users to a bogus website that mimics the appearance of a legitimate one, in order

to obtain personal information such as passwords, account numbers, etc.

**Cyber Stalking:** It is the repeated use of electronic communications to harass or frighten someone, for example by sending threatening emails. IT involves a person following a web-surfer through cyberspace in spite of the objections made by the later one, which could result into causing severe mental agony, stress and harassment to the person being stalked.

**Spamming:** Spamming means sending unsolicited bulk/commercial mails over the net which clogs the network and reduces the speed. IT Act does not have provisions on spamming.

**Credit Card Frauds:** Using credit card through internet, for making payment of goods or services, has opened major routes for frauds against the cyber consumers. While using credit card through internet, the transaction takes place CNP (Card Not Present), it provides the space for people stealing information of cards and misusing it for making a purchase. As the IT Act does not deal with credit card frauds, there exists a need express provision to be formulated for checking such activities.

## Domain Name Issues

With the advancement of e-commerce, the domain names have come to acquire the same value as a trademark or the business name of a company. The value attached to domain names makes it lucrative for cyber criminals to indulge in domain name infringements and the global nature and easier and inexpensive procedure for registering domain names further facilitates domain name infringements. When a person gets a domain name registered in bad faith, i.e., in order to make huge profits by registering a domain name corresponding to a trademark of another person, with intent to sell the domain name to the trademark owner at a higher price, such activities are known as cyber-squatting. The IT Act does not deal with the domain name issues. In India the domain name infringement cases are dealt with according to the trademark law. With most of the countries providing for specific legislations for combating and curbing cyber-squatting, India also needs to address the issue and formulate legal provisions against cyber-squatting. For settlement of Disputes, WIPO has introduced a new

mechanism called ICANN (Internet Corporation for Assigned Names and Numbers) for settlement of disputes relating to domain names. As the parties are given the right to file the case against the decision of ICANN in their respective jurisdictions, the decisions of ICANN are having only persuasive value for the domain users.

## Software Piracy

Software piracy refers to making unauthorized copies of computer software which are protected under the Copyright Act, 1957. Piracy can be of following types:

**Soft lifting:** this means that sharing a program with an unauthorized person without a licence agreement to use it.

**Software Counterfeiting:** Counterfeiting means producing fake copies of a software, imitating the original and is priced less than the original software. This involves providing the box, CDs, and manuals, all tailored to look as close to original as possible.

**Renting:** it involves someone renting a copy of software for temporary use, without the permission of the copyright holder which violates the license agreement of software.

## Cybersquatting and Trademark Infringement

Trademark means a unique identifier mark which can be represented by a graph and main idea is to differentiate the goods or services of one person from those of others and may include shape of goods, their packaging and combination of colours.

Cybersquatting is a cybercrime which involves imitation of a domain name in such a manner that the resultant domain name can dupe the users of the famous one with an intention to make profit out of that. This is executed by registering, selling, or trafficking of a famous domain name to encash a popular domain name's goodwill.

When two or more people claim over the right to register the same domain name then the domain name dispute arises when a trademark already registered is registered by another individual or organization who is not the owner of trademark that is registered. All domain name registrars must follow the ICANN's policy.

Meta tagging is a technique to increase the number of users accessing a site by including a word in the keyword section so that the search engine picks up

the word and direct the users to the site despite the site having nothing to do with that word. This may result in trademark infringement when a website contains meta tags of other websites thereby affecting their business.

**Information Technology (Intermediaries Guidelines) Rules 2021** and Section 79 IT Act, 2000 provide conditional safeguard from liability of the online intermediaries, but at the same time its open for interpretation under any other civil or criminal Act. IT Act 2000 makes an intermediary non-liaible for any third-party content hosted on its site. The 2021 Guidelines entail following of diligent approach by the intermediaries to avail protection or exemption under Section 79 IT Act, 2000. Therefore, it becomes crucial for initiative-taking judicial interpretation depending on the facts of each case.

**Jurisdictional Issues in IP Cases in Cyber Law**  
Cyberspace has no borders and Intellectual Property disputes have become a global concern with mixed infringements and cross border disputes. For prescription, adjudication, and enforcement of law the legal disputes will come under jurisdiction of a Court or not becomes a worrying concern as there is no clear-cut rule of law. A country as a sovereign power has powers to adopt a criminal law for to an offensive act was committed outside its borders may but which has an impact within its territory. Following the international law, Courts can assume universal jurisdiction to prosecute a cybercriminal.

Evolution of various of theories and legal concepts has been witnessed to deal with this much anxiety of jurisdictional issues with respect to adjudicating the infringements of intellectual property in cyberspace. The most significant of these are the Minimum Contacts Test, the Effects Test, and the Sliding Scale Test or 'Zippo Test' taken from US Courts. The Minimum contacts test is applicable where one or both parties are out of territorial jurisdiction of the Court but there is a contact with the State in which the Court is located. The Effects test is applicable at the territory of the Court the effects or injury of any cyber-crime is experienced. The Sliding Test is related to personal jurisdiction regarding the interactions with commercial information over the internet between the non-resident operators.

**Section 75 IT Act, 2000** is applicable to cybercrimes committed outside India if the offence involving a computer, computer system, or computer network placed in India.

**Section 4 IPC, 1860** extends its jurisdiction to offences committed in any place outside India targeting a computer resource located in India. The courts in India can adjudicate against the intellectual property infringements in cyberspace and they protect the intellectual property owners by means of judicial activism and effective jurisprudence.

## Conclusion

The Indian Information Technology Act provides India to build a technological advanced society and keeping in pace with the rest of the world by providing a legal framework within which such society can flourish. While the Indian Government feels the need for a law on this and has taken its first step in regulating the cybercrimes by legislating the IT Act 2000, the legal regime on Information Technology in India is still in its developing stage. There exist numerous loopholes and grey areas in the Act which need to be considered. There are numerous unprecedented issues due to advance technological development that do not find express solution in the existing Act. The issues relating to intellectual property rights on internet, spamming, cybersquatting, cyber stalking, credit card frauds, data protection and privacy on the net need to be addressed. Following the footsteps of other developed countries like United States and EU which have adopted effective legislations for data protection and privacy, Indian Government is also in the process of formulating laws to tighten its legal regime over the issues relating to data protection and privacy to support its offshore credibility. Following the modern ways of cybercrimes, the government has taken in to account the violation of data protection norms and drafted Information Technology Amendment Act 2008 addressing issues relating to electronic contracts, breach of confidentiality and privacy, child pornography, e-commerce frauds like Phishing, identity theft, sending offensive mails, in order to bring a comprehensive legislation to protect the rights of the individuals. This will help the country go a long way in making Internet and

# International Journal of Professional Development

**Vol.10, No.1, Jan-June2021**

**ISSN: 2277-517X (Print), 2279-06599(Online)**

cyber space safer, people friendly and commercially more reliable.

## References

1. <http://www.oznetlaw.net/factsheets/databaseprotection>
2. I.T. Act, 2000
3. Indian Copyright Act, 1957
4. <http://www.linfo.org/database.html>
5. Macmillan & Co. Ltd Vs Cooper, 1924; 40 TLR 186
6. Jain, Pankaj & Rai, Pandey Sangeet CPT Laws, 2005
7. Declaration of W.I.P.O (Stockholm, July 14th, 1967)
8. Sec.106 (3) of the American Copyright Act, 1988
9. <http://www.bitlaw.com/source/17usc/102.html>
10. James M.Jordan III Copyright in an Electronic Age
11. <http://www.copyright.gov/legislation/hr2281.pdf>

[www.ijpd.co.in](http://www.ijpd.co.in)