Cyber Crime and Challenges in Protection of Intellectual Property Law (IPR)

Dr. Nisha Kevaliya (Sharma)

Principal
Chameli devi Institute of Law
Indore, M.P.

***Abstract*-During the last two decades, digital technology, digitization of the economy and national security have opened up new possibilities. These possibilities have revolutionized the way businesses operated through integration and seamless transfer of information in real time. This , has created conditions for businesses alike, providing opportunities for startups and small companies to grow rapidly and challenges the existing ones. This change is most pronounced in the Indo-Pacific, where artificial intelligence (AI), block chain technology and cloud computing are expected to propel some of the region's biggest markets into digital leadership roles in the new 'Asian Century'. At the beginning of this millennium, this could not have been imagined**

The advent of quantum computing could render traditional encryption useless, giving cyber criminals access to business secrets such as encrypted data and sensitive information.

As the digital landscape changes with new innovative technology, many challenges have also arisen with it. Cyber attacks—ranging from persistent government-sponsored threats to opportunistic cybercriminals—can result in costly intellectual property and data thefts. Even a single person can become a serious threat to critical infrastructure, financial and logistic systems and national security, putting millions of people in trouble. These ever-present threats affect all industries include healthcare, energy, transportation and retail industries. These threats require constant vigilance, new safeguards, and imaginative re-evaluation.

Key words: **Cyber, cyber crimes, Cyber attacks, . Cyberspace, digitization, inventions, Right to Intellectual Property, management strategy, digital transformation, artificial intelligence, inventions. Achievements, e-commerce, cyber stalking, fraud, cyber bullying, phishing or spamming, IPR violations – copyrights, trademarks, trade secrets of businesses conducted online, hyperlinking Service mark, framing, practices, meta-tagging.**

INTRODUCTION

In ancient times, where the primitive man used to live by using the basic facilities of nature, whereas in today's present era, man has acquired all kind of facilities for the society through various inventions. All these inventions and achievements are the result of an individual efforts of a particular individual or collective efforts of an identified group of persons. A person, after his intense efforts, creates a new invention or idea, in fact, the original credit for that invention or idea should be given to him. But at present, many such examples have come to the fore where the real achievements of one person have been attributed to another person with their own name in a wrong way. The Right to Intellectual Property basically seeks to control similar irregularities and to provide the right to the competent person.

Every innovation in the technological field is fraught with dangers. Cyberspace has facilitated e-commerce on the one hand - connecting with friends and family, publishing literary works and sharing knowledge, but at the same time these personal data or copyright or patent data become vulnerable to various cyber attacks.

It is best to have an effective intellectual property management strategy for all e-businesses involved in the vast majority of cyberspace.

With the increasing penetration and digitization of the Internet, India's public and private sector is prone to cyber attacks, cyber crimes and incidents. Current geopolitical tensions with neighbouring countries such as China and Pakistan, coupled with the challenges of working from home due to the covid -19 pandemic, have led to a nearly 200% increase in all types of cyber crime and cyber incidents. These figures are of cyber attacks from government and non-government organizations in the public and private sectors in India.

Modern digitization of supply chain & logistics systems, technology-based solutions, cloud computing, AI and data analytics will also lead to an increase in cyber attacks. Conflicting interfaces, improper configuration, sensitivities of hardware & software and lack of procedures will also result in more cyber incidents and cyber crimes.

There are various laws nationally and internally in place to protect intellectual property against cyber threats, but it becomes the moral duty of the IPR owner to take all necessary protective measures to negate and mitigate illegal virtual attacks.

Right to Intellectual Property:

Intellectual property right is a right that gives full credit to the creator of an object or idea for the creation of that object or idea. From a social point of view, the right to intellectual property protects the personal interests of a creator in such a way that the goods produced by the creator and the use of those goods by various persons in the society are included in the information. Due to the difference of rights of the manufacturer giving credit for the creation encourages in various ways.

In general, industrial property and copyrights come under the right of intellectual property. But apart from this, there are many such rights which have been included in it as a principle. The right to intellectual property includes rights related to the following points - literary, artistic and scientific work; an artist's performance; Inventions made in various endeavor areas of man; scientific discovery; industrial design; Trade mark and service mark etc. On the basis of various points related to the right of intellectual property, the right of intellectual property can be divided into the following categories-

1. The right to intellectual property which is given on the basis of any invention and creative activities, it includes: patent, industrial design, copyright, right of plant breeder, layout or blueprint design of integrated circuit etc.
2. All those rights of intellectual property which provide information to a consumer It includes: trademarks and geographical indications.

Intellectual property rights -

Intellectual property rights protect original work in the fields of art, literature, photography, writing, painting, even choreography in written format audio and video files. IPR protects these works in both tangible and intangible form. Patents, copyrights, trademarks, trade secrets, industrial and layout designs, geographic indications are intellectual property rights for which legal remedies are also available for infringement online.

With technological advancements and innovations in the cyber world, the global markets have benefited copyright or patent owners. However, every good innovation has its disadvantages as IPR violation has become one of the major concerns due to the development of cyber technology. IPR and cyber laws go hand in hand and cannot be kept in separate compartments and online content needs to be protected.

The ever-increasing and evolving cyber crimes are not limited to cyber stalking, fraud, cyber bullying, phishing or spamming, but also IPR violations – copyrights, trademarks, trade secrets of businesses conducted online, illegal such as audio, video, hyperlinking Service mark, framing, by practices meta-tagging, and more.

Definition of cyber crime -

Cyber crime is a crime that involves a computer and a network Cyber crime involves the illegal use of modern tele-communications networks (Internet, mobile phones) to commit crimes against a person or group of persons, they can be harassed intentionally, can be damaged physically or mentally and damage can be caused to their reputation as well. Cyber crime can threaten the security and financial health of an individual or nation as whole.

Cyber crime is an illegal act, where a computer is used as a means or as a target or both. Cyber crime is a broad term, which can also be defined as:- "criminal activity where a computer or computer network is used as a means, target or site of criminal activity".

According to the United Nations Computer Crime Control and Prevention Manual, cyber crime is a crime that involves fraud, forgery and unauthorized access. Generally, "cyber crime" means a crime which is committed by means of a computer or communication device.

According to the European Cyber Crime Convention Council, cyber crime is a crime that is committed against data and copyright. In today's computer age as the technology is developing in the same way people associated with crime-world are also applying those techniques to carry out their work. Cybercrime is related to information technology or internet.

Cyber crime has become a worldwide and complex problem.

It is becoming more developed and changing with the gradual development of technology. This offense is basically in two forms - tampering with computer or mobile phone (Section 43, 66) and offense committed by computer or mobile phone or digital assistant (PDA) (Section 66-K to 66-F, 67, 67-A to 67-C)

The first recorded cyber crime in the computer world occurred in 1820 to discourage Joseph Marie Jaccard's employees from using the new technology used by their boss to investigate their weaving work.

International law for the protection of intellectual property in the field of cyber -

There are various international convention, treaties and agreements for the protection of intellectual property in cyberspace: The "Bern Convention (1886), the Madrid Agreement on the International Registration of Trademarks (1891), the Hague Agreement on the Registration of International Designs (1925), Rome Convention for Protection of Performers, Producers of Phonogram and Broadcasting Organizations (1961), Patent Cooperation Treaty (1970) Agreement on Trade-Related Aspects of Intellectual Property Rights (1994), World Intellectual Property Organization Copyright Treaty (1996), World Intellectual Property Organization Display and Phonogram Treaty (1996), and the Same Domain Name Dispute Resolution Policy(1999), Consolidation has international instruments governing intellectual property rights.

The Berne Convention (1886)protects IPR in literary and artistic works and provides for special provisions for developing countries.

The Rome Convention (1961) covers the creative works of authors and owners of physical indicators of intellectual property. It allows implementation at the domestic level by member states where the dispute is subject to adjudication by the International Court of Justice unless arbitration is resorted to.

TRIPS (1994) is a multilateral agreement on Intellectual Property that covers a wide range of intellectual rights such as copyright and related rights.

UDRP (1999) stands for the resolution of disputes over the registration and use of Internet domain names.

Intellectual property rights and law in India -

For protection, IPR in Indian soil, various constitutional, administrative and judicial regulations have been defined, be it copyright, patent, trademark or other IPR.

Legislation enacted to protect IPR-

In the year 1999, the government passed an important law based on international practices to protect intellectual property rights, the same are mentioned below-

The Patents (Amendment) Act, 1999, facilitates the establishment of a mailbox system for filing patents. It provides exclusive marketing rights for a time period of five years.

Trademark Bill, 1999.Copyright (Amendment) Act, 1999-

The Geographical Indications of Goods (Registration and Protection) Bill, 1999.

The Industrial Design Bill, 1999 replaced the Design Act, 1911.

The Patents (Second Amendment) Bill, 1999, to further amend the Patents Act, 1970 in pursuance of TRIPS.

Copyright act-

Section 51 of 1957, is expressly clear that the exclusive rights are vested in the copyright owner and anything to the contrary constitutes copyright infringement. Since there is no clear law prescribing the liability of an Internet Service Provider (ISP), section 51 can be interpreted in relation to the facility of server facilities for the storage of user data by ISPs at their business locations, and which is broadcasting services to earn profit through charges for advertisements. However, the other ingredients to be interpreted in this way are to be completed in a cumulative manner, these materials are 'knowledge' and 'due diligence' to hold the ISP liable for copyright infringement.

The Information Technology (Intermediary Guidelines) Rules 2021 and Section 79 of the IT Act, 2000 provide conditional protection from liability of online intermediaries, but at the same time are open to interpretation under any other civil or criminal act. The IT Act 2000 makes an intermediary non-responsive for any third-party content hosted on its site. The guidelines for 2021 include diligent approach to be followed by intermediaries to obtain protection or exemption under Section 79 of the IT Act, 2000. Therefore, it becomes important to have an initiative judicial interpretation based on the facts of each case.

Judicial position in cyber law and intellectual property dispute-

Cyberspace has no boundaries and intellectual property disputes have become a global concern with mixed infringements and cross-border disputes. Legal disputes for the prescription, adjudication and enforcement of law will come under the jurisdiction of the court or will not be of concern as there is no clear rule of law. A country as a sovereign power has the power to adopt a criminal law because an offensive was committed outside its borders, but which has effect within its territory. Courts can assume universal jurisdiction to prosecute cyber criminals, following international law.

Cyberspace has seen the development of various theories and legal concepts to address this concern of jurisdictional issues with respect to intellectual property infringement judgments. The most important of these are the minimum contact test, the impact test, and the sliding scale test or 'Zippo test' taken from US jurisdictions. The minimum contact test applies where one or both parties are outside the court's territorial jurisdiction but have contact with the state in which the court is located. The impact test applies in the jurisdiction of the court, the impact or injury of any cyber crime is experienced. The sliding test deals with individual jurisdiction over the interaction of commercial information on the Internet between non-resident operators.

Section 75 of the IT Act, 2000 applies to cyber crimes committed outside India if the offense involves a computer, computer system or computer network in India. Section 4 IPC, 1860 extends its jurisdiction to offenses committed at any place outside India by targeting any computer resource located in India. Courts in India can adjudicate against infringement of intellectual property in cyberspace and they protect intellectual property owners through judicial activism and effective jurisprudence.

Improving Cyber Security System in India: Challenges and Opportunities

The governance structure regarding cyber security in India is currently broken and they sometimes work without each other's knowledge. There is also a lack of coordinated and structured information sharing between the government and the private sector. India's new cyber security strategy can fill this gap by creating a centralized system of governance and facilitating coordination among government agencies.

It is also important that with better information exchange between government agencies, this system should be expanded to cover the private sector as well. Processes that seek to reduce security risks must be well defined and properly implemented.

AI, quantum computing, machine learning, the glut of IOT devices and the rise in digitization have only complicated the security infrastructure. Governments and companies will need to invest not only in hardware and software capability, but also in training the people working on such complex systems. There is no dearth of talent in India which can be harnessed to build a strong cyber infrastructure.

India has the potential to quickly become an attractive place for companies to set up manufacturing units. In this case, the Indian government has taken several steps to attract foreign investors such as incentives linked to production. Along with this, technical and infrastructure parks have also been set up for large manufacturing units in electronics and pharmaceuticals. The government has also announced the vision of a self-reliant India, which will require more investment not only in physical infrastructure but also in digital capability. The result of increased investment in the technology sector will raise questions over concerns about privacy and security of data generated through online services. Because of this, there is a need for legislation to control the flow of data.

With the spread of COVID-19 in India, new challenges have emerged in the security of online systems. Due to the lockdown imposed to prevent the spread of the epidemic, for the work companies had to depend on work from home. Work from home is now common place and the center of all activities these includes: education, work and financial transactions. The IT infrastructure, which was carefully designed to protect the online systems in offices, now has to handle the spread of employees and workplaces. In such a situation, it is not surprising that attacks on vulnerable systems have increased since the beginning of

the epidemic in India and the subsequent lockdown. The use of the app for contact tracing of covid-19 positive people has also increased the threat and encroachment on security.
About half (48 percent) of users faced a cyber threat between January and July 2020, based on the latest data from Kaspersky this means about 2 billion cases or 205 million malicious files. 25 percent more malicious files were identified daily compared to last year. That is, 4,28,000 new threats every day.
Not only people were targeted for cyber crime, but key sectors such as defence, health, processing and other sectors related to national security were also targeted. Cert-in, the nodal cyber security related in India, has issued several advisories since March 2020, warning people about phishing and malware attacks and also issued guidelines for protection against cyber incidents and attacks . The government has also recently advised the private sector to conduct security audits so that they can assess their infrastructure and human resource capacity to prevent attacks.
It is not uncommon in today's geopolitics for government-sponsored organizations to hide behind technology and security companies and use technology for ulterior motives. They engage in industrial espionage and theft of intellectual property, violate data privacy, and collectively monitor their public.

Cyber crime and Challenges in Protection of Intellectual Property Rights

Copyright Infringement "Copyright protection is granted to the owner of any published , artisticl, literary, theatrical or scientific work to prevent everyone else from using and profiting from that work in their own name." These copyright infringements includes: use without the permission of the owner, making and distributing copies of the Software and their unauthorized sale, and illegal copying from websites or blogs. Adding : Linking refers to directing the user of a website to another web page by clicking on at extort image without leaving the current page. This poses the reattached rights and interest soft he website owner and the owner may lose income easier latest the number of users visiting the websites. This can lead users to believe that the two websites are linked and under the same domain and ownership. In the Shetland Times, Ltd Vs Jonathan Wills and others, it was held to be an act of copyright the infringement under British law and an injunction was issued because the Shetland News should have been deeply linked to its embedded pages. The Shetland Times website, but they were also link eddo the Times' website. With digitization there is a threat to copyright to owner ship and rights on its own innovations it becomes easier to mold the various components of copy right elements in to various forms by the process of linking, in-linking and framing. No permission is required for this. Deep linking is challenging to manage as there are no clear laws at both the national and international level and this ambiguity becomes beneficial for cyber criminals who try to infringe copyright. Ensuring the smooth functioning of online resources and businesses needs to balance the rights of thecopyrightownerontheonehandandthefreeavailabilityofinformationontheother.ReadingSections14and51,the Indian Copyright Act,1957,alegalissuearises from which hit is not clear when the copy right ted work is be ingre produced. The ambiguity lies in the detection of copyright infringement, which his at the stage of deep link formation without disclaimer accessing a link that does not require any approval or at the time when a use ruses the link at will. Another challenge is within line links. Designed with Maps to navigate and fetch images from various sources on the browser visited by the user accessing the link, these images are copied by the end user who is unaware that he can downloaded them from different websites, is recovering. Like deep linking, the problem of infringement detection remains the same because this difficult to track down the exact stage of reproduction of copyrighted images. In line link creator is guilty of copyright infringement though not distributing it directly but giving way to facilitate making unauthorized copies of original website content, there by falling within the purview of Section14 of the CopyrightAct,1957.However,the end user does not have to know about or have knowledge of any copyright infringement and is thus protected.

- Framing:Framing is another challenge and becomes a legal issue and a matter of debate on the interpretation of derivation and adaptation under Section 14 of the Copyright Act, 1957. Framer only provides modalities for users to access copyrighted material that is retrieved from a website for the user's browser to access so that they are not held responsible for copying, transmitting or distributing copyrighted material. The question arises whether obtaining copyrighted material from a website and combining it with something else to create one's own will would amount to adaptation or interpretation under the law.

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

- Soft lifting - means sharing the program with an unauthorized person without a license agreement.
- Software Counterfeiting - Counterfeiting means creating fake copies of a software, copying the original and costing less than the original software. This includes providing boxes, CDs and manuals, all designed to look as close to the original as possible.
- Renting – This includes renting a copy of the software for temporary use without the permission of the copyright holder that violates the software's license agreement.

A. Cyber Squatting and Trademark Infringement:
The meaning of a trademark is a unique identifier mark that can be represented by a graph and the main idea is to distinguish one person's goods or services from others and may include the shape of the goods, their packaging and the combination of colors.

Cyber squatting is a cyber crime that involves copying a domain name in such a way that the resulting domain name may deceive users of the famous with the intention of making a profit from it. It is executed by the registration, sale or smuggling of a well-known domain name in order to capitalize on the goodwill of a popular domain name.
A domain name dispute arises when two or more people claim the right to register the same domain name when a previously registered trademark is registered by another person or organization that is not the owner of the registered trademark. All domain name registrars must follow the ICANN policy.
Meta tagging is a technique used to increase the number of users accessing a site by including a term in the keywords section so that search engines can pick up that term and direct users to the site, While the site has nothing to do with that term. This can result in trademark infringement when a website contains meta tags from other websites affecting their business.
There are a few conditions that need to be met for a domain name to be derogatory:

1. A domain name can be said to be derogatory if it gives users the impression of being similar to another popular trademark that is one registered and users mistakenly access a fake created with the malafide intention of benefitting users of the popular trademark domain.
2. The registrant has no legal right or interest in the domain name.
3. The registered domain name is being used incorrectly.

Conclusion-

With technological advancements and innovations, it becomes imperative to protect sensitive data and information and intellectual property online by resorting to strict legal measures. As new types of cyber crimes affecting intellectual property emerge, it has become necessary to enact new laws as traditional rules are not sufficient to provide justice as to protect or protect violators of intellectual property in the cyber world detection challenges are quite challenging. A secure environment is provided to import and export to protect IPR, for smooth travel and convenience of global trade and e-commerce and various businesses operating online. Newbie and updated technical practices like encryption, cryptography, digital signatures and digital watermarks are an absolute necessity for protecting copyrighted material. It is important to keep a record of all works owned by the IPR to identify the author, number or code associated with such works. It is not the only solution to take the path of legal settlement of the dispute, but it is very necessary on the part of the owners of copyright, patent, trademark and other intellectual property rights to take the initiative and take all necessary precautions to protect their works. The security for IPR should be updated with the existing technical measures.
Prime Minister Narendra Modi encouraged investment in blockchain technology during the India Ideas Summit in July 2020. He also allayed concerns that the initial opposition to cryptocurrencies did not mean that block chain was taboo. Now that India wants to attract investment from companies interested in different supply chains, it will need to digitize blockchain-secured logistics to remain competitive.
The digitization of supply chains and the use of blockchain technology will require individual countries to adopt laws that provide security in sync with the changing technological landscape. With the increasing role of technology in managing critical infrastructure, proper security arrangements have to be made to ensure that the benefits of digitization do not come at a cost.
At that time, protecting critical infrastructure from cyber attacks will be critical for growth and success. When India is trying to become a digital economy with emphasis on production.
Transparency has become essential for building trust and lasting partnerships at the business and diplomatic levels.In today's interconnected world, cyber security is not only about protecting hardware and software, but also protecting digital governance, economy and everyday life and the huge data it generates. If others are not convinced that they can trust you with their digital data, devices, networks and infrastructure, they will move to other locations or create barriers to mitigate any potential risk. Cyber security companies must adopt and demonstrate a commitment to transparency, including acknowledging the risks associated with creating source code or accessing processes for review by trusted third parties.

REFFERENCES:

https://www.legalserviceindia.com/legal/article-3233-intellectual-property-issues-in-cyberspace.html>

टलैंडटाइम्स लिमिटेड बनाम डॉ. जोनाथन विल्स और ज़ेटन्यूज़ लिमिटेड[1996] (सत्रकान्यायालय, एडिनबर्ग)।

बनर्जी, एस., 2021. साइबरस्पेस मेंबौद्धिक संपदा अधिकार कानून। [ब्लॉग] https://blog.ipleaders.in/ ,: <https://blog.ipleaders.in/intellectual-property-rights-law-in-cyberspace/>

लीगलसर्विसइंडियाडॉटकॉम। 2022. साइबरस्पेस में बौद्धिकसंपदा मुद्दे । [ऑनलाइन]

:[2]<https://www.legalserviceindia.com/legal/article-3233-intellectual-property-issues-in-cyberspace.html> [14 जून 2022 कोएक्सेसकियागया]।

Amit Yoran, “Australia’s Assistance And Access Bill Increases Risks Of Cyber Attacks”, FORBES, February 25, 2019.

Casey Newton, “India’s proposed internet regulations could threaten privacy everywhere”, THE VERGE, February 14, 202

"Digital India", MCKINSEY GLOBAL INSTITUTE, March 2019.

"India Cybersecurity Services Landscape- A Global Hub in the Making", DSCI, May 21, 2020 SuneethKatarki et al.,

"The Personal Data Protection Bill, 2019: Key Changes And Analysis," MONDAQ, January 6, 2020Rahul v Pisharody,

"Disha Bill: What are the highlights of Andhra Pradesh's new law?", THE INDIAN EXPRESS, December 14, 2019

"Will soon unveil a new cyber security policy: PM Modi", THE TIMES OF INDIA, August 15, 2020.