Team Code: TC218

Name of the Author: Arti Yadav

Name of College: Lloyd Law College, Greater Noida

Email: 1516artiyadav@gmail.com

Contact number: 9457490353

Introduction

The rapid growth of the internet and digital technologies has transformed the way we live, work and communicate. The internet has developed into a vital resource for people, organizations, and the government, providing a multitude of chances for creativity and social and economic progress. But along with this expansion has come a rise in cybercrime, including identity theft, phishing, hacking, online harassment, and other malevolent actions.

The emergence of cybercrime in India has raised serious concerns, as numerous organizations and individuals have been targeted by these nefarious actions. According to the Indian Computer Emergency Response Team's study. Phishing attempts have been responsible for a large portion of the nation's recent cybercrime cases.

The case of Nasscom vs Ajay Sood and Ors.[1] is a significant one in the realm of Indian cyber laws. This case involves allegations of phishing and cybercrime activities. Nasscom is India's leading software association, the National Association of Software and Service Company, a non-profit trade association of Internet Technology (IT) and Business Process Outsourcing (BPO) industry, sued Ajay Sood and three other defendants. Through this case commentary, we will examine the facts of the case, arguments, legal issues, court's ruling and implications of the case, highlighting its significance in establishing the groundwork for cyberspace and Intellectual Property Law in India.

Brief Background and Facts

The term "phishing" was originally introduced to the public in 1992 by the AOHell Program, which was founded by a Pennsylvanian youth in the 1990s with the goal of getting into America Online accounts (AOL). Targeting huge numbers of people in password-stealing techniques was made easier by the hacking program. The prominent software association of India, "Nasscom," was deceitfully impersonated in the current case of Nasscom vs. Ajay Sood and Ors. Here, the Delhi High Court examined the definition and context of the term "phishing." The defendant was accused of creating a website, "www.nasscom.co.in", that was misleadingly similar to Nasscom's official website, "www.nasscom.in.". This website was created to defraud people and obtain unfair advantages. In order to stop the defendants or anyone else working on their behalf from spreading false emails purporting to be from the plaintiff that use the trademark "Nasscom" or any other confusingly similar mark in connection with goods or services, the plaintiff sought a permanent injunction under Order 23 Rule 3 CPC. It was discovered throughout the inquiry that the defendant, who was sending fraudulent emails using the Nasscom domain name, was using false identities created at the employee's directions in order to evade detection and repercussions.

A commission was dispatched to look into the defendant's property, and after recovering two hard drives from the defendant's house, it was determined that these drives were the origin of all those fake emails. From these hard drives, the offending emails were found.

[1] National Association Of Software And Service Company v. Ajay Sood And Ors. 119(2005) DLT596 (2005) (India)

In the case of Yahoo! Inc. vs. Akash Arora[2], Yahoo! Sued Akash Arora over the use of the domain name "yahooindia.com," which was like Yahoo's trademark. The court ruled in the favour of Yahoo and passed restraining order against Akash Arora. It was the time when the common law concept of passing off was applied to a domain name for the first time in India, it became evident that cybersquatting, the practice of registering domain names that closely resemble well-known brands would not be allowed under Indian law. This case played a significant role because it examined whether the current trademark laws might be expanded to cover online domain names and digital brands. An important precedent for digital trademark protection in India was established by this decision.

Issue (s)

1. Whether Ajay Sood and others were guilty of phishing and cybercrime activities.

2. Whether the defendant's actions constituted a violation of the Information Technology Act and caused harm to NASSCOM's reputation.

3. Whether the use of a deceptively similar domain name constitute passing off or cybersquatting.

4. Whether the principle of trademark law apply to the internet and digital space.

Decision

Hon'ble Justice Pradeep Nandrajog (Delhi High Court) rendered the decision in the case of Nasscom vs. Ajay Sood and Ors. on 23.03.2005. The petitioner argued that the defendant is fraudulently sending emails to a certain number of targeted persons posing as Nasscom to extract personal data of such persons which can later be used for head-hunting. The defendant in response capitalized on the loophole of lack of legislation defining and penalizing internet fraud, sub dividing into specific category of phishing.

Even though there is no specific legislation in India that penalizes phishing, the court ruled in this case that it is an illegal act and for the first time defined it as "misrepresentation made in the course of trade leading to confusion as to the source and origin of the e-mail causing immense harm not only to the misused but also to those whose information has been misused."

It was held that that the usage of the website 'www.nasscom.co.in' constituted passing off, as it could mislead the public into believing that the emails were sent by Nasscom only. This confusion could harm Nasscom's image and can damage its reputation. It affirmed that domain names could be considered trademarks, and using them without authorization could amount to passing off and infringement. After this case, domain

names began to be seen as digital assets that should be protected by intellectual property law in India. The foundation for upcoming issues pertaining to digital brand protection was established by this decision. The court further stated, by way of an example, that common phishing scams involves individuals posing as

[2] Yahoo!, Inc. v. Akash Arora & Anr. 78(1999) DLT 285

representatives of online banks and stealing money from e-banking accounts in order to obtain their personal banking information.

The Delhi High Court established a major precedent in the field of online fraud by defining phishing and classifying it as a fraudulent act, despite the lack of legislation that define and penalize phishing. The court considered the broader consequences of Ajay Sood's conduct and held him accountable for the harm caused to Nasscom and the IT-BPO industry

In addition, the court issued an ex-parte ad-interim injunction prohibiting the defendant from using any of the plaintiff's pirated software and ordered the defendant to reimburse the plaintiff a total of Rs. 1.6 million in monetary damages. Additionally, the court mandated that the plaintiff, who would be the rightful owner of the hard disks, receive the disks that were taken from the defendant's property.

Analysis

Robert Louis B Stevenson in his article titled "Plugging the Phishing Hole": Legislation v. Technology[3]; dated 17.03.2005 discusses the necessity of an act that, if passed, would prohibit sending phishing emails, and add two new crimes to the existing federal code. First, the act would criminalize sending phising emails regardless of whether recipients actually suffered any damages, and second it would criminalize creating phishing websites regardless of whether website visitors actually suffered any damages.

Therefore, this act if passed would be extremely important since it makes it illegal to create a phishing website, regardless of whether or not any visitors actually experienced any harm.

Ajay Sood and Ors. v. Nasscom is regarded as a landmark case that introduced "Phishing" to the domestic legal system. The court brought the conduct of phishing under Indian law even in the lack of specific legislation. It demonstrates the confidence that owners of intellectual property have in the ability and willingness of the Indian legal system to protect citizens' intangible property rights and makes it abundantly evident to them that they can conduct business in India without compromising their rights. The court also took into account the broader ramifications of Ajay Sood's actions, holding him accountable not just for the direct harm caused to people, but also for the harm made to Nasscom and the IT-BPO industry. Additionally, an ex-parte ad-interim injunction order was passed granting relief to the extent of 1.6 million rupees to the Plaintiff.

Similar arguments were raised in the 2005 case of Microsoft Corporation vs. Yogesh Papat[4], which claimed that the defendant's conduct had left the plaintiff's copyright in the stolen software uncontested. As a result, the court held the defendant liable for software infringement and causing the plaintiff to incur financial losses. As a result, the defendant was ordered to compensate the plaintiff, and an injunction was imposed to prevent the defendant from conducting business in a manner that would hurt the plaintiff's reputation. Similarly, in the 2005 case of Autodesk, Inc. And Anr. vs. Mr. Prashant Deshmukh[5], on March 9, 2011, the Delhi High Court

[3]Robert Louis B. Stevenson, Plugging the Phishing Hole: Legislation v. Technology, (Mar. 17, 2005) (https://scholarship.law.duke.edu/dltr/vol4/iss1/5/)
[4] Microsoft Corporation v. Mr. Yogesh Papat and Anr. 118(2005) DLT580 (2005) (India)
[5] Autodesk, Inc. & Another vs Mr. Prashant Deshmukh & Others CS(OS) No. 1755/2003 (2003) (India)

granted the plaintiff a permanent injunction against the defendant for copyright and registered trademark infringement. In the case of Sporta Technologies Pvt. Ltd. and Anr. vs. John Doe and Ors.[6]on November 30, 2023, where the plaintiff claimed that the defendants created fake websites using the plaintiff's domain name, causing harm to the plaintiff's reputation, the Delhi High Court ruled in favour of the plaintiff and granted an ex-parte injunction order prohibiting the defendants from creating and sharing fake websites.

India is among the 195 nations that are members of INTERPOL. It is the biggest international police organization in the world which promotes crime prevention and police cooperation on a global scale. Being a part of Interpol helps India fight cybercrime as it provides it access to a vast database of criminal data and facilitates communication and cooperation between Indian authorities and foreign law enforcement. Additionally, it aids in locating and apprehending cybercriminals who flee to other nations. To assist cybersecurity audits and simulated exercises through CERT-In and ensure the ongoing readiness of businesses and crucial sectors of the nation, India has also created a cyber crisis management plan that would allow it to respond to cyber incidents.

Many members of the Commonwealth are affected by inadequate digital capacity, thereby making such countries prone to cyber threats and attacks from malicious cyber actors. Globally, malware attacks increased to 358 per cent in 2020 compared to 2019. Globally cyberattacks also increased by 125 percent through 2021. The cost of cybercrime is estimated to grow from US$3 Trillion in 2015 to US$ 6 Trillion by the year 2025. According to the United Nations Conference on Trade and Development worldwide resource, 80 percent of the United Nation member countries have cybercrime legislation, 5 percent with draft legislation, 13 per cent with no legislation and 1 per cent with no cybercrime data.

As a result, with the advent of the digital era, cybercrime has grown rapidly and is having a huge impact in nations such as India, where literacy rates remain low despite recent improvements. Some of the most frequent types of cybercrime include phishing scams, internet fraud, online Intellectual Property Violation (IPR), identity theft, and online harassment and bullying. Phishing is one of these cybercrimes that does not have a legal framework; therefore, a regulation that may control non-personally identifiable data is necessary to prevent cybercrime and guarantee that businesses safeguard their assets.

The Information Technology Act, 2000[7] covers few cybercrimes which includes hacking, publishing pornographic electronic content, damaging computer source code, breaching protected systems, and publishing a fake digital signature certificate in specific contexts or for fraudulent purposes which was further amended to The Information Technology Act of 2008[8] to introduce other cybercrimes besides these. Despite the amendment there still exists a lacuna in the laws due to the rapid growth of Internet Technology.

Therefore, it is evident that while there is a lack of appropriate legal and regulatory framework to control cybercrimes like phishing, citizens also need to be made aware of the dangers of phishing and how to avoid

[6] Sporta Technologies Pvt. Ltd., And Anr. v. John Doe and Others CS(COMM) 842/2023 (2023) (India)
[7] The Information Technology Act (India), 2000
[8] The Information Technology Act(India), 2008

becoming targets of attacks, as the growing use of cloud services has made it simpler for phishers to launch attacks. Additionally, the court also played a proactive role in defending intangible property rights and made it clear that one should have faith in the legal system's capacity. As observed in the current case of Nasscom vs. Ajay Sood and others, the case accomplishes two significant goals-

First one being that the practice of 'phishing' is now placed within the purview of Indian legal framework, despite the absence of a specific statute and secondly, it debunks the misconception that there is no "damage culture" in India for the infringement of Intellectual Property Rights. Both goals were earlier considered to be impossible but now are bolstering the faith of the citizens that the judicial system is willing and can protect the Intangible Property Rights and now Intellectual Property owners can do business freely without sacrificing their Intellectual Property Rights.

Most often developed countries like the United State and United Kingdom become the target for cyberattacks. Phishing is a global phenomenon, and therefore various organisations of the world must be proactive in tracking the phishing trends in their region. In order to comply with data privacy policies, European businesses and organizations have been investing in cyber security measures since the General Data Protection Regulation (GDPR) came into effect in 2018.

Different nations have different sets of laws and regulations to protect their nation from cyberattacks as in Europe, where members of the European Union have heightened sensibilities towards cyber security and privacy, which are engrained in European Union laws.

There is a need of an appropriate legal framework, because in the absence of one, cybercrime will erode the fundamental trust and confidence in Information Communications Technologies (ICTs which is necessary to accomplish the Sustainable Development Goals (SDGs) and advancing the Commonwealth’s values of democracy rights, human rights, rule of law and good governance.

Conclusion

The case of Nasscom vs. Ajay Sood and Ors. represents a critical turning point in the India’s battle against cybercrime. Notwithstanding the lack of formal legislation, this historic ruling has defined phishing and placed it under Indian law. The court's ruling has made it abundantly evident to owners of intellectual property that they can do business in India without jeopardizing their rights.

For companies and individuals functioning in India's digital environment, the case has broader ramifications. It underlines the need of safeguarding Intellectual Property Rights and the necessity of an all-encompassing legal framework to prevent cybercrime. The ruling also demonstrates how capable and prepared the Indian legal system is to protect Intangible Property Rights.

Ultimately, the case of Nasscom vs. Ajay Sood and Ors. establishes a significant precedent in the battle against cybercrime, enhancing trust in Indian judicial system and its capacity to defend Intellectual Property Rights in the digital era.