JURISDICTIONAL ISSUES OF CYBERSPACE

Dr. Kumudha Rathna,
Department of Business Law,
The Tamil Nadu Dr. Ambedkar Law University.

Introduction

We are in the era of the digital world, as we all know that not even a single piece of work can be done without the help of technology, from recharging our mobile, paying electric bills, property tax, water tax, medical bills, daily grocery, bank transactions, from national to international online shopping, online education, remote works, travel ticket booking including bus, train, and flight all done online. Most of the transactions take place within a few seconds. With the help of technology, remote work can be done for companies located on the other side of the globe.

International trade became easy due to advancements in technological growth, interactive websites, and digital marketing have increased worldwide connectivity and opportunities. If we compare digital marketing with traditional marketing, without huge investment reaching customers is not so easy. Now the entire marketing strategy changed, start-ups can reach global customers without much investment, traditional marketing strategy became an additional investment but not mandatory investment, digital marketing became a boon for businesses. The one-time investment by the start-up is only on the electronic equipment such as computer, printer, internet, website, social media advertisement sponsors and digital marketing campaign and sponsors, renting huge workspace are minimized.

E-commerce became the center stage for a successful business. E-commerce is nothing but an interactive website that acts as an intermediary for Business-to-Business, and Business- to – customer, the logistic became easily trackable than before, people order products from all over the world including remote areas, the products are delivered within the time specified by the seller, and most importantly the e-commerce website provides enough support to fulfill customers rights and protection. E-commerce provides a platform for an entrepreneur to sell their products directly to customers without any retailers or intermediaries. In addition, these days Banks provide different and easy payment methods to enhance online transactions, secured transactions, and 24×7 customer services to promote digital transactions.

Further, because of the E-commerce websites, FDI became very easy, whether its multibranded or single branded government provides a concession for Foreign Direct Investment, mainly for E-commerce investment. The inflow of foreign investments plays a vital role in the country's economic rapid growth. People started to adopt the usage of the internet to enhance their daily life by minimizing unnecessary hurdles.

Understanding Cyberspace and Jurisdiction

Technology is like a weapon or a tool, it can be used in either way. Where there is a benefit there is a responsibility, nothing comes for free. So far, we saw the advantages of the technological revolution but there

is a disadvantage of using them because of the greed of few. Some of the major issues are the cybercrimes, online frauds, privacy issues, pornography, hate speech, rape threat, murder threat, online child abuse, online stalking, defamation, a threat to reputation and goodwill, data protection, system hacking threats, it clearly shows that there is a need for advanced technology in cyber cell and police station for the expeditious investigation, and there is a necessity to enhance the inadequate acts and rules. Among all the issues, Jurisdictional issues are one of the most challenging as cybercrime can be done from any part of the world. The technology growth made the entire globe fit inside our hands, but the question is how safe we are while handling those technologies. Are laws being uniform throughout the world! How far our rights and privacy are violated, what is the uniform solution for all the issues. How to overcome the jurisdiction issues. How to use the internet safely and securely! How much awareness do people have while using the internet! How to overcome the heinous crimes faced online?

Provisions

The jurisdictional issues in terms of e-commerce websites, domain names, trademarks, copyright and other intellectual property rights can be categorised broadly under two heads jurisdiction in Rem and Jurisdiction in personam. Jurisdiction in rem In terms of parties to the dispute involving the international bases of often leads to the statutory concerns. The foundational shift of jurisdiction in rem to jurisdiction in personam has been observed in World Wrestling Entertainment, Inc. v. M/s. Reshma Collection & Ors 2014 wherein a US based company was in dispute with a mumbai based company it was decided by Apex court that the jurisdictional issues in the cases involving e-commerce websites and attributes of intellectual property rights such as copyright and trademark etc. are to be dogged by the buyer's place of residence.[1]

Jurisdiction in internet domain has the Extra territorial aspect involved in it. "Lex loci delicti" can be understood in terms of the physical presence of the accused. This principle is relied upon by both national courts as well as courts Over the international platform in the developed nations like USA and other European countries etc. in USA minimum contact theory is considered as a sole criterion for determining the jurisdictional issues in case either of the party is from outside the territorial jurisdiction of the court involving a case under cyberspace.[2]

The US Supreme Court Has also placed its reliance over the rule considering the harm caused to the reputation of the plaintiff being the resident of the forum state. This rule is generally known by the name of 'Calder Effect Test.'[3] Under European legislation with effect of the Brussels convention the jurisdiction with respect to the commercial matters is regulated.[4]

In India jurisdictional issues in particular cases falls within the domain of code of civil procedure of 1908. Rolling down the eyes following the section 15 to 19 read with section 20 of the respective act enables the court of laws to adjudicate the matters wisely. These laws further add on to extract best out of the existing

[1] https://udrc.lkouniv.ac.in/Content
[2] Shoe Co. v. Washington, 326 U.S. 310 (1945).
[3] Calder v. Jones, 465 U.S. 783 (1984)
[4] Id.

provisions for the conflicting parties. In addition to this IT Act of 2000 comes into the limelight when the issues are related to internet and technology. This Act opens with the extension over the jurisdiction to which this act applies coupled with the provisions dealing with the commission of crimes in this affair of cyberspace outside India under section 1 and section 75 of the Act respectively. The amendment to the IT Act of 2000 has further change the perspectives of the crimes in the domain of cyber space across the borders of India pertaining to the Constitution of cyber appellate board under section 48 of the Act respectively, for the wise adjudication of the cases involving the concept of jurisdictional issues. Besides these Indian legislations also have particular act dealing with the specific sectors of Intellectual property Rights comprising Copyrights, Trademarks, Domain names, Data privacy etc.[5]

Issues, Remedies, And Jurisdiction

E-Commerce

Is nothing but selling and buying services, Goods, and products on the internet. Ecommerce includes both marketplace and inventory models but does not include individual sellers of goods and services. On 30th January 1997 UN has adopted the Model Law of Electronic Commerce adopted by the United Commission on International Trade Law and was recommended to be adopted by all countries, based on the said recommendation our country adopted and enacted The Information Technology Act, 2000, the moto is to enhance the E-commerce and to set uniformity of law applicable to substitute to the paper method of communication and storage of information.

As we can see, online contact issues are growing extremely fast. IT Act 2000 and (Amendment) 2009 provide a solution for several issues. For example, as per Section 10-A, any contract made in electronic means is valid and whoever discloses the information in breach of lawful contract will be punished under Section 72-A of the IT Act.

Data Privacy

Data privacy is the protection of personal, sensitive data from unauthorized use. These data are misused by way of selling that information to the dark web or to commercial companies for a huge amount of money, apart from that these data from a specific country can be used to create cyber terrorism, and so on. The main provisions that deal with Data Privacy are Section 43A and Section 72A of the Information Technology Act (2000). Section 43A explains the compensation for failure to protect data and Section 72A deals with punishment for disclosure of information in breach of a lawful contract, as per section the offender will be punished with imprisonment for a term which may extend to three years, or with fine which may extend to 5 lakh rupees, or with both. In most civil cases the agreement has the jurisdiction clause to provide a solution for all disputes.

[5] Id.

VKI v Amazon (2015)

In this case the court of justice of European union has decided the jurisdictional issue in the light of the rights of the consumers affected. The court held that in case of a conflict between the consumer and the company serving the interests of those consumer shall be resolved in the country wherein the interests of the consumers are being afflicted. In the present case, Amazon EU Sarl, is a company which is incorporated in Luxembourg. This said company conducted its sales in Austria. However the above stated company did not have any registered office in Austria. The company used to deal with the people through a website named as 'amazon.de'. However the standard terms and conditions of the country has allowed the Amazon to make the usage of the data of the consumers such as reviews feedbacks etc. for the better functioning of Amazon. The VKI, Consumer protection body, had applied in the Austrian court to grant an injunction against the usage of such data of the consumers under the shade of standard terms. As per the Brussels convention meant to deal with the jurisdictional issues guided the court of justice of European Union to be the suitable forum to decide the present matter.[6]

Analysis

In the present case the court of justice of European Union under the eclipse of Brussels convention attracted the jurisdiction in the present case. The court held that in case of a conflict between the consumer and the company serving the interests of those consumers shall be resolved in the country wherein the interests of the consumers are being afflicted.

Trademark And Domain Name

The domain name dispute, cybersquatting, and trademark issues will go parallel in most circumstances. We can say all three are interlinked. Domain names mainly refer to the website address. It is unique and cannot be shared between different sites. The registration process is on a first come first served basis, that is where the problem starts.

Cybersquatting is the term used when someone buys the domain name of a registered or well-known trademark, with the intention to sell it for profit. It generally refers to the practice of buying up domain names that use the names of existing businesses with the intent to sell the names for profit to those businesses.

The remedies for domain name disputes are to approach the court under the Trademark law of the country, the plaintiff can seek permanent/interim injunction or damages, to issue of takedown notice to the registrar along with a court order, to proceed with dispute resolution under UDRP/INDRP regarding registration of internet domain names, either to transfer the disputed domain name or takedown the website.

UDRP deals with a dispute arising out of the registration of any domain name, in UDRP proceedings the complainant selects the provider from the list of ICANN-approved providers who then form an administrative panel that administers the proceedings. The UDRP proceedings are governed by the UDRP policy, Rules of procedure, and the WIPO supplemental rules, most of the international disputes are solved in WIPO, the rules

[6] https://www.scl.org/articles/3730-vki-v-amazon-governing-law

over major factors such as whether the registered domain name is identical or confusingly similar to the trademark, whether the registrant has any legitimate rights or interests in the domain, whether the domain name was registered and used in bad faith, for what purpose the registrant using the domain for, whether there is any trace of habitual cybersquatting behavior, whether the domain name is used to disturb the business flow and to sell it fraudulently to the trademark holder.

Whereas disputes about (ccTLDs) are governed by the .IN Dispute resolution policy (INDRP) which is managed by the National Internet Exchange of India (NIXI), under the INDRP, the arbitrator must conduct the proceedings under the INDRP policy, rules of procedure, and the Arbitration and Conciliation Act, 1996, further it is to be noted that INDRP applicable only for .in registered domain name. Under the INDRP, the.IN registry will appoint an arbitrator from the list of arbitrators to conduct the proceedings. In order to decide whether to use UDRP or INDRP or to approach the courts, the first thing to note is to identify the defendant's domain name if it is registered by the.IN registry, it is preferable to initiate arbitration before INDRP tribunal, but if it is .com the UDRP to be approached, and even if the proceeding is pending, the complainant /plaintiff can seek additional reliefs by approaching the appropriate court of law.

Further, start-ups should buy all the relevant domain extensions so that their trademark will not be misused at a later point in time.

Trademark

Google Inc. v. Gulshan Khatri (2017)

In the present case, an American-based multinational technological company has sued the Indian-based company in terms of domain name. The respondent in the present case had been using a domain name googlee.com. On the other hand the petitioner had been using the domain name from the year 1997 as 'google.com.' The respondent had begun to make usage of the above stated domain name In the year 2007. This overt act of the respondent was creating confusion into the minds of general public at large. In addition to this, Respondents constant usage of the identical domain name was bringing down the goodwill and reputation of the petitioner into the eyes of the common mass. The petitioner had claimed that the domain name of the respondent was similar in both the terms conceptually as well as visually. The apex court in the present case had applied the principles embedded in the minimum contact theory. By virtue of the said theory the respondent in the present case was physically present in India they are for the jurisdictional issue for the present case was sought to be resolved in India. The apex court had adjudicated The present case into the favour of petitioner thereby restraining the respondent from using the domain name that is conceptually as well as visually identical to that of the petitioner causing the loss.[7]

Analysis

Indian apex court has sought a way to deal with the rising jurisdictional issues in the cyberspace. The main aim of the court of law is to bring the justice to the party whose rights has been violated by the wrongdoer. In

the present case the apex court had wisely laid down its foundation on the rules grounded by the developed countries like USA. This inclination of the Indian Courts towards the adaptation of the rulings in the field of cyber space will Take the nation up to the height of seven skies in the direction of development, making India from a developing country to a developed country.

Cyber Crime

Cybercrime is an unlawful act done with the help of computers and the internet. Some of the well-known Cybercrimes are Child pornography/ child sexually abusive material, Cyberbullying, Cyberstalking, Cyber grooming, Online job fraud, Online sextortion, Phishing, Sexting, SMS phishing, Sim swap scam, Debit/credit card fraud, Impersonation and identity theft, Phishing, Spamming, Ransomware, Virus, worms & trojans, Data breach, Denial of services /distributed dos, Website defacement, Cyber-squatting, Pharming, Crypto-jacking, Online drug trafficking, Espionage. We may question ourselves that since cyberspace is worldwide, the jurisdiction is the major issue, but the Information technology Act, 2000 provides protection to all victims, Section 75 of the IT Act applies for offenses or contraventions committed outside India irrespective of his nationality, therefore whether the crime is committed within India or outside India by Indian or Foreigner, the cybercriminals are subject to be punished under IT act, 2000.

Major IT And IPC Provisions[8]

- Offenses under I.T.Act: Tampering computer source documents (Sec.65) ComputerRelated Offences; Cyber Terrorism (Sec.66 F); Publication/transmission of obscene / sexually explicit act in electronic form (Sec. 67); Dishonestly receiving stolen computer resource or communication device (Sec.66B); Interception or Monitoring or decryption of Information (Sec.69); Un-authorized access/attempt to access to the protected computer system (Sec.70); Abetment to Commit Offences (Sec.84 B); Attempt to Commit Offences (Sec.84C); Computer-Related Offences (Sec.66). Identity Theft (Sec.66C); Cheating by personation by using computer resource (Sec.66D); Violation of Privacy (Sec.66E); Publishing or transmitting of material depicting children in the Sexually explicit act in electronic form (Sec.67B); Publishing or transmitting obscene material in Electronic Form; Publishing or transmitting of material containing sexually explicit act in electronic form (Sec.67A); Preservation and retention of information by intermediaries (Sec.67C).
- Offences under IPC (Involving Communication Devices as Medium/Target) r/w IT Act ; Abetment of Suicide (Online) (Sec.305/306 IPC); Cyber Stalking/ Bullying of Women/Children (Sec.354D IPC); Data theft (Sec.379 to 381); Fraud (Sec.420 r/w Sec.465,468-471 IPC) ;Cheating (Sec.420); Forgery (Sec.465, 468 & 471); Defamation/ Morphing (Sec.469 IPC r/w IPC and Indecent representation of women Act); Fake Profile (r/w IPC/SLL); Counterfeiting; Cyber Blackmailing/Threatening

(Sec.506,503,384 IPC r/w IPC/SLL); Fake News on Social Media (Sec. 505); Gambling Act (Online Gambling); Lotteries Act (Online Lotteries); Copy Right Act, 1957;

- Trade Marks Act, 1999. Other SLL(Special and Local Laws) Crimes; Fraud (Sec.420 r/w Sec.465,468-471 IPC); Credit Card/Debit Card; ATMs Online Banking Fraud OTP Frauds; Counterfeiting; Currency (Sec.489A to 489E); Stamps (Sec.255).

The legal remedy is to file an online complaint, the victim has to make an online submission on National Cyber Crime Reporting Portal: Helpline Number and Time 155260 (10:00 AM To 6:00 PM).

The cybercrime victim can also approach the cybercrime cell in their place of residence, if the cyber-crime cell is not available, the victim must file FIR in the nearest police station within 24 hours of the occurrence of the incident.

Conclusion

The term 'jurisdiction' refers to the court's ability to hear a particular case, it is either determined by pecuniary jurisdiction or territorial jurisdiction, but when it comes to cyberspace, there are no boundaries, the issue raised may be from any corner of the world, as the internet is worldwide. Several countries have enacted special laws to deal with internet issues.

While dealing with companies, most companies have added to their website terms and conditions requiring that any dispute must be addressed in a certain venue, the enforceability of these provisions varies based on the jurisdiction and facts, most companies have successfully incorporated and invoked such clauses for defending issues brought in foreign jurisdictions.

In Indian law, the IT act provides applicability to any offense or contravention committed outside the national boundaries, but still, we lack in procedural aspect, we are not trained enough to solve hundreds of complaints made every day, cyber cell, a police official and court are struggling to implement the law and to provide the victim with speedy redressal.

As far as cyber cell efficiency is concerned, we still have a long way to go. It's either inefficiency or political issues that prevent cybercrime victims from getting justice within a reasonable time.

If the issue is civil nature, even though the frustration is high, the victim can still survive in society without humiliation. As we all know that justice delayed is justice denied but denial of justice in cyberspace is much more heinous, the victim identity is circulated all over the internet without any protection without stringent action by the cyber cell, the victim gets affected physically, emotionally, and mentally, this may increase country suicidal rate due to humiliation. So, the solution is to make necessary changes in the technical advancement in the cyber cell, consumer redressal forums, and court proceedings while dealing with national and international cyber-crimes.

REFERENCES

1. Cyber Crime Portal
2. https://ncrb.gov.in/en
3. CII 2018 Volume 2.pdf (ncrb.gov.in)
4. Manupatra
5. SCC Online.