International Journal of Research in Engineering, Science and Management
Volume-1, Issue-9, September-2018
www.ijresm.com | ISSN (Online): 2581-5782

Flaws in E-Contracts and E-Commerce: Better Implementation of Cyber Laws in India

H. P. Purvik
Student, Department of Law, Christ University, Bengaluru, India

***Abstract*—This paper presents the flaws in e-contracts and e-commerce and will explain the better implementation of cyber laws in India.**

***Index Terms*—e-contracts, e-commerce, cyber laws**

I. Introduction

Concept of E-Contract

E-Contract is an aid to drafting and negotiating successful contracts for consumer and business e-commerce and related services. It is designed to assist people in formulating and implementing commercial contracts policies within e-businesses. It contains model contracts for the sale of products and supply of digital products and services to both consumers and businesses.

An electronic or digital contract is an agreement "drafted" and "signed" in an electronic form. An electronic agreement can be drafted in the similar manner in which a normal hard copy agreement is drafted. For example, an agreement is drafted on our computer and was sent to a business associate via e-mail. The business associate, in turn, e-mails it back to us with an electronic signature indicating acceptance. An e-contract can also be in the form of a "Click to Agree" contract, commonly used with downloaded software: The user clicks an "I Agree" button on a page containing the terms of the software license before the transaction can be completed. Since a traditional ink signature isn't possible on an electronic contract, people use several different ways to indicate their electronic signatures, like typing the signer's name into the signature area, pasting in a scanned version of the signer's signature or clicking an "I Accept" button and many more.

A. Types of E-Contracts

E-Contracts can be categorized into two types i.e. web-wrap agreements and shrink-wrap agreements. A person witnesses these e-contracts everyday but is unaware of the legal intricacies connected to it. Web-wrap agreements are basically web based agreements which requires assent of the party by way of clicking the "I agree" or "I accept" button e.g. E-bay user agreement, Citibank terms and conditions, etc. Whereas Shrink-wrap agreements are those which are accepted by a user when a software is installed.

The traditional paper based contract law has rules that apply to matters such as jurisdiction, validity, formation of contract, modifications to contracts. In the world of online trading these are all issues that arise in online contracts and is a challenge to the traditional concepts of contract law.

An example of an electronic contract that went horribly wrong occurred in 2002 when Eastman Kodak placed a camera for sale on its United Kingdom website for £100 instead of £329. Before Kodak could rectify the error, thousands of orders had already been placed. The company was faced with an option of honoring the contracts or face a lawsuit by the disgruntled customers. Initially Kodak said that it was a mistake and they would not fill the orders. One of their arguments was that the orders were simply bids to accept its offer for sale but it was not a cogent argument as the company accepted the orders and thereby formed an online contract. In the end Kodak was left with little choice but to honor the contracts. The total cost to Kodak was enormous and Kodak shrugged off the question whether customers would have won the lawsuit by saying that trade on the internet is a grey area.

B. Legality of E-Contract

The first issue that arises is to ensure that online contracts are legally enforceable. Before the advent of the internet contracts were normally concluded either in writing or by oral agreement. The United Nations Convention on Contracts for the International Sale of Goods (1980) The United Nations Commission on International Trade Law realized that the growth of electronic commerce required it to take steps to recognize that contracts can be validly concluded by using the internet. The steps taken by the UNCITRAL had to ensure that users of E-Commerce should be able to electronically sign the contracts to ensure their enforceability.

The UNCITRAL therefore adopted the Model Law on Electronic Commerce and in article 16 of the UNCITRAL Model Law on Electronic Commerce formally recognition is provided for the legality of an online electronic contract. The UNCITRAL Model Law on Electronic Commerce requires that States ensure that such contracts are legally binding on the parties. Article 7 of the UNCITRAL Model Law on Electronic Commerce further confirms that electronic signatures are recognized.

The United States adopted the UNCITRAL Model Law by the adoption of the Uniform Electronic Transactions Act and the Electronic Signatures in Global and National Commerce

Act (E-Sign).

The EU also adopted the UNCITRAL Model Law. The adoption took place by way of the adoption of the Directive on Electronic Signatures and the Ecommerce Directive. The question of validity of an electronic signature will come to the force once proof of the signature is required.

C. E-Commerce

E-Commerce – 'the new communication technology' is the latest way of doing business. IT has given the opportunity to expand their markets to include anyone in the world but it has also massively affected and changed the way business is done today. While businesses can derive the advantage of going global at a cheaper cost, consumers also benefit from the freedom to choose for a variety of sellers. Since then, ecommerce has evolved to make products easier to discover and purchase through online retailers and marketplaces. Independent freelancers, small businesses, and large corporations have all benefited from ecommerce, which enables them to sell their goods and services at a scale that was not possible with traditional offline retail.

Despite its numerous advantages, however, e-commerce comes with its set of pitfalls. Internet being the backbone of the e-commerce revolutions, there are significant risks attached to conducting business over the internet.

D. Flaws in E-commerce

E-commerce growth comes with downsides as well. Perhaps the most noteworthy area of concern is the growth in online security breaches, fraud and other forms of electronic malfeasance. Direct e-commerce fraud rates have decreased significantly over the last several years, in part due to major investments in security and fraud prevention.

However, fraud still costs e-commerce merchants billions in losses. Loss estimates vary, but conservative estimates put e-commerce fraud losses at $3 billion. Most of these losses have their origin in compromised card data, either through data breaches (online and offline) or other forms of cardholder data theft.

In spite of online security investments, e-commerce merchants remain vulnerable to fraud committed using stolen information compromised in data breaches, highlighting a unique challenge to tighten security both in the physical and electronic environments. This becomes even more important given the nascent mobile commerce industry, which introduces additional security challenges. These security problems come with significant hard dollar costs, as well as harder-to-quantify costs to consumer confidence and brand reputation.

A data breach is a confirmed incident in which sensitive, confidential or otherwise protected data has been accessed and/or disclosed in an unauthorized fashion. Data breaches may involve personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property.

Common data breach exposures include personal information, such as credit card numbers, Social Security numbers and healthcare histories, as well as corporate information, such as customer lists, manufacturing processes and software source code. If anyone who is not specifically authorized to do so views such data, the organization charged with protecting that information is said to have suffered a data breach.

E. Notable Data Breaches

There have been several major data breaches of both large enterprises and government agencies in recent years. In 2013, retail giant Target Corporation disclosed it had suffered a major data breach that exposed customer names and credit card information. The company initially announced that 40 million customers were affected by the breach but later raised that number to 110 million. An internal investigation into the matter revealed the initial intrusion point was a third-party business partner that had been breached; the threat actors then used the business partner's credentials to access Target's network and then spread point-of-sale (POS) malware to the company's POS systems. The Target data breach led to several lawsuits from customers, state governments and credit card companies, which resulted in the company paying tens of millions of dollars in legal settlements. In addition, the company's CEO and CIO both resigned in the wake of the breach.

The cyber laws that govern the e-commerce transactions are not very clear and vary from country to country. These legal issues prevent people from entering into electronic contracts.

Cyber law is important because it touches almost all aspects of transactions and activities and on involving the internet, World Wide Web and cyberspace. Every action and reaction in cyberspace has some legal and cyber legal angles.

Cyber Crime is not defined in Information Technology Act 2000 nor in the National Cyber Security Policy 2013 nor in any other regulation in India. In fact, it cannot be too. Crime or offence has been dealt with elaborately listing various acts and the punishments for each, under the Indian Penal Code, 1860 and quite a few other legislations too. Hence, to define cyber-crime, one can say, it is just a combination of crime and computer. To put it in simple terms 'any offence or crime in which a computer is used is a cyber-crime'. Interestingly even a petty offence like stealing or pick pocket can be brought within the broader purview of cybercrime if the basic data or aid to such an offence is a computer or an information stored in a computer used (or misused) by the fraudster. The I.T. Act defines a computer, computer network, data, information and all other necessary ingredients that form part of a cybercrime.

In a cyber-crime, computer or the data itself the target or the object of offence or a tool in committing some other offence, providing the necessary inputs for that offence. All such acts of crime will come under the broader definition of cyber-crime.

Cyber law encompasses laws relating to:

- Cyber crimes
- Electronic and digital signatures

- Intellectual property
- Data protection and privacy

F. Need for Cyber Law

In today's techno-savvy environment, the world is becoming more and more digitally sophisticated and so are the crimes. Internet was initially developed as a research and information sharing tool and was in an unregulated manner. As the time passed by it became more transactional with e-business, e-commerce, e-governance and e-procurement etc. All legal issues related to internet crime are dealt with through cyber laws. As the number of internet users is on the rise, the need for cyber laws and their application has also gathered great momentum.

In today's highly digitalized world, almost everyone is affected by cyber law. For example:

- Almost all transactions in shares are in demat form.
- Almost all companies extensively depend upon their computer networks and keep their valuable data in electronic form.
- Government forms including income tax returns, company law forms etc. are now filled in electronic form.
- Consumers are increasingly using credit/debit cards for shopping.
- Most people are using email, phones and SMS messages for communication.
- Cybercrime cases such as online banking frauds, online share trading fraud, source code theft, credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, pornography etc. are becoming common.
- Digital signatures and e-contracts are fast replacing conventional method of transacting business.

A major program has been initiated on development of cyber forensics specifically cyber forensic tools, setting up of infrastructure for investigation and training of the users, particularly police and judicial officers in use of this tool to collect and analyze the digital evidence and present them in Court.

Indian Computer Emergency Response Team (CERT-In) and Centre for Development of Advanced Computing (CDAC) are involved in providing basic and advanced training of Law Enforcement Agencies, Forensic labs and judiciary on the procedures and methodology of collecting, analyzing and presenting digital evidence.

G. Cyber Laws in India

In India, cyber laws are contained in the Information Technology Act, 2000 ("IT Act") which came into force on October 17, 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government.

India has an extremely detailed and well-defined legal system in place. Numerous laws have been enacted and implemented and the foremost amongst them is the Constitution of India. We have inter alia, amongst others, the Indian Penal Code, the Indian Evidence Act 1872, the Reserve Bank of India Act, 1934, the Companies Act, and so on. However, the arrival of internet signaled the beginning of the rise of new and complex legal issues. It may be pertinent to mention that all the existing laws in place in India were enacted way back keeping in mind the relevant political, social, economic, and cultural scenario of that relevant time. Nobody then could really visualize about the Internet. Despite the vivid insight of our master draftsmen the requirements of cyberspace could hardly ever be anticipated. As such, the coming of the Internet led to the emergence of numerous tricky legal issues and glitches which required the enactment of Cyber laws.

The existing laws of India, even with the most compassionate and liberal interpretation could not be interpreted in the light of the emergency cyberspace, to include all aspects relating to different activities in cyberspace. In fact, the practical experience and the wisdom of judgement found that it shall not be without major threats and pitfalls, if the existing laws were to be interpreted in the scenario of emerging cyberspace, without enacting new cyber laws. Hence, the need for enactment of relevant cyber laws.

None of the existing laws gave any legal validity or sanction to the activities in Cyberspace. For example, the Net is used by a large majority of users for email. Yet till today, email id not "legal" in our country. There is no law in the country, which gives legal validity, and sanction to email. Courts and judiciary in our country have been reluctant to grant judicial recognition to the legality of email in the absence of any specific law having been enacted by the Parliament. As such the need has arisen for Cyber law.

Internet requires an enabling and supportive legal substructure in tune with the times. This legal infrastructure can only be given by the enactment of the relevant Cyber laws as the traditional laws have failed to grant the same. E-commerce, the biggest future of Internet, can only be possible if necessary legal infrastructure compliments the same to enable its pulsating growth.

All these and other varied considerations created a conductive atmosphere for the need for enacting relevant cyber laws in India.

H. Jurisdiction

If a crime is committed on a computer or computer network in India by a person resident outside India, then can the offence be tried by the Courts in India?

According to Section 1(2) of Information Technology Act, 2000, the Act extends to the whole of India and also applies to any offence or contravention committed outside India by any person. Further Section 75 of the I.T. Act, 2000 also mentions about the applicability of the Act for any offence or contravention committed outside India. According to this section, the Act will apply to an offence contravention

committed outside India by any person, if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

A Police officer not below the rank of Deputy Superintendent of Police should only investigate any offence under this Act. (Sec. 78 of I.T Act, 2000)

Without a duly signed extradition treaty or a multilateral cooperation arrangement, trial of such offences and conviction is a difficult proposition.

I. Intermediaries

Section 79 deals with the immunity available to intermediaries. The Information Technology (Intermediaries guidelines) Rules, 2011 governs the duties of the intermediaries.

"Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet device providers, web hosting service providers, search engines, online payment sites, online auction sites, online market places and cyber cafes.

Intermediary will not be liable for any third party information, data or communication link hosted by him. It will apply only if:

- The function of the intermediary is limited to providing access to a communiqué system over which information made available by third parties is communicated or temporarily stored or hosted.
- The intermediary does not initiate the transmission or select the receiver of the transmission and select or modify the information contained in the transmission.
- The intermediary observes due diligence while discharging his duties.

The intermediary will be held liable if he collaborated or assisted or aided or persuaded whether by intimidations or promise or otherwise in the commission of the unlawful act. He will also be liable if upon receiving actual knowledge or on being notified that any information, data or communication link residing in or connected to a computer resource controlled by it is being used to commit an unlawful act and it fails to expeditiously remove or disable access to that material.

II. Conclusion

A. A solution to the problem with the moment of contract and jurisdiction can be removed by all countries adopting the same regulations relating to their online contracting and thereby creating a common law that will apply in all instances. Such a move will promote much more certainty in electronic contracts as all parties will know exactly what their entitlements and responsibilities are in such contracts.

To sum up, though a crime free society is perfect and exists only in illusion, it should be constant attempt of rules to keep the criminalities lowest. Especially in a society that is dependent more and more on technology, crime based on electronic law-breaking are bound to increase and the law makers have to go the extra mile compared to the impostors, to keep them at bay. Technology is always a double-edged sword and can be used for both the purposes – good or bad. Steganography, Trojan Horse, scavenging (and even Dos or Don'ts) are all technologies and per se not crimes, but falling into the wrong hands with an illicit intent who are out to exploit them or misuse them, they come into the array of cyber-crime and become punishable offences. Hence, it should be the tenacious efforts of rulers and law makers to ensure that technology grows in a healthy manner and is used for legal and ethical business growth and not for committing crimes.

References

[1] https://www.lawctopus.com/academike/legal-issues-involved-e contracts/
[2] http://www.legalserviceindia.com/article/l350-E-contracts-&-issues-involved-in-its-formation.html
[3] https://www.theregister.co.uk/2002/01/09/kodak_discount_camera_fiasco/
[4] https://www.lawteacher.net/free-law-essays/commercial-law/potential-problems-using-electronic-contracts-commercial-law-essay.php
[5] https://www.shopify.com/encyclopedia/what-is-ecommerce
[6] https://www.pymnts.com/company-profile/2011/data-breaches-and-ecommerce-is-there-promise-in-new-prevention-options/
[7] https://searchsecurity.techtarget.com/definition/data-breach
[8] http://www.cyberlawsindia.net/internetfraud.html
[9] https://blog.ipleaders.in/need-know-cyber-laws-india/