ISSN 2249-4421 UGC Approved Journal No. 42016

STUDENT JOURNAL

A Journal of Amity Law School, Delhi
(A Peer Reviewed Journal)

Volume 6 DECEMBER, 2017

STUDENT JOURNAL SOCIETY

ISSN 2249-4421 UGC Approved Journal No. 42016

ALSD Student Journal: A Journal of Amity Law School, Delhi
(Peer-Reviewed Journal)

Volume 6 2017

Published and Distributed by
ALSD Student Journal

ALSD Student Journal is published annually.

ISSN: 2249-4421

Disclaimer:
Views expressed in the ALSD Student Journal are those of the contributors. The Editors and ALSD do not necessarily subscribe the views expressed by the contributors. The Editors and ALSD disclaim all liability and responsibility for any error or omission in this publication. In the case of binding defect, misprint, missing pages etc., the publisher's liability is limited to replacement of the defective copy.

All enquiries regarding the journal should be addressed to:
Editor,
ALSD Student Journal
(An Institution of the Ritnand Balved Educational Foundation)
(Affiliated to Guru Gobind Singh Indraprastha University, New Delhi)
F-1 Block, Sector 125, ALSD Student Journal University Campus
Noida-201313 (U.P.) Tel: 0120-4392681
E-mail : alsdelhi@amity.edu Website: www.amity.edu/als

Printed at
K. S. Enterprises
28/8, Street No. 15, 60 Feet Road, Vishwas Nagar,
Shahdara, New Delhi - 110032
Phone : 011-22570110, Mobile : 8800553000
E-mail : k.s.enterprises1957@gmail.com, k.s.enterprises1958@gmail.com

ALSD Student Journal

A Journal of Amity Law School, Delhi
(Peer-Reviewed Journal)

ISSN 2249-4421
Volume 6
2017

CONTENTS

ABOUT AMITY LAW SCHOOL

The School has been consistently ranked as one of the Top Law Schools in the Country since 2006. In the survey of the India's Best Law Colleges by India Today (THE INDIA TODAY NIELSON SURVEY), the National Magazine, Amity Law School Delhi(ALSD) bagged 4th rank in India in 2017 moving up in ranks from Rank 11 in the same in 2016. In THE WEEK (HANSA RESEARCH SURVEY) ALSD was ranked at 12th in 2016 and 11th in 2015. THE OUTLOOK (OUTLOOK GFK MODE SURVEY), ALSD was ranked 10th in 2016.

The Amity Law School, Delhi(ALSD) has the distinction of being the first Law School in Delhi to start a 5-year integrated LL.B (H) programme in 1999. The School was established under the Ritnand Balved Education Foundation (RBEF) to achieve world-class legal education in the country. Dr. Ashok K. Chauhan, the Founder President of the Law School is a great philanthropist and a man of extraordinary vision. This great vision has been translated into practical reality through the establishment of various educational institutions including the Amity Law School. His vision for the Law School is to provide excellence in legal education and to produce quality lawyers with good moral principles and great human values. The President RBEF, Dr. Atul Chauhan has been providing dynamic leadership intervention in strengthening the vision of the Founder President. Presently the academic values are being inculcated by Prof. (Dr.) D. K. Bandyopadhyay, (Former Vice-chancellor, GGSIPU) Chairman, Amity Law Schools.

Amity Law School Delhi has been granted affiliation by the Guru Gobind Singh Indraprastha University, Delhi for running a 5-year Integrated LL.B (H) programme and the affiliation has been approved by the Bar Council of India. The programme is designed to incorporate teaching methods for realizing holistic legal education.

The programme offered by Amity Law School Delhi seeks to promote multi-disciplinary analysis of the socio-legal problems by designing/pursuing/giving effect toits course-structure and teaching methods to realize these objectives. The methods of teaching in the Law School include lecture, discussions, case law analysis, moot court training, project assignment and placement programmes. In addition, the School organizes seminars on contemporary legal issues, conducts clinical courses and train students in legal research and legal writing. By the time a student completes the 5-year programme he/she will be fully equipped with the required theoretical knowledge and practical experience in the field of law to become a full-fledged responsible member of the legal profession.

VALIDITY OF E-CONTRACTS

Ankit Purohi[*] and Sanyukta Saxena[**]

Meaning and Definition of E-Contract

Introduction

The advancement in the technology has revolutionized the human life. Now a days significance of pioneering technologies can be seen in every facet of life. The recent amelioration of Information technology, Telecommunications and Computer technology has caused the computer networks to gain immense popularity amongst the masses. These computer networks facilitate electronic trading across the globe. Electronic trading embodiesuse of computer network to enter into contract between two human trading partners and also includes such contracts which are contracted between two legal entities (legal persona) together with the help of a computer program which acts as an agent although it has no conscious of its own and also acts as an Initiator.

What is E-Commerce and E-Contract?

Electronic Commerce (or E-Commerce) is the business conducted over computer networks. The phrase 'E-commerce' can be defined as 'commerce conducted in digital form or an electronic platform' or 'selling or buying goods and services on the Internet'[1]. E-commerce now serves as an integral part of the economic infrastructure. Companies are now drawn towards facilitating their transactions over the web by targeting every owner of a computer linked to the computer network. Electronic contracts can be executed by such technologies as funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data interchange (EDI), inventory management systems and automated data collection systems. Present day electronic commerce is found to typically use the World Wide Web (www) at least once in the entire transaction's life-cycle, and it may encompass a wider range of technologies such as e-mail, mobile devices and telephones as well.

* 1ST YEAR LL.M. STUDENT, DEPARTMENT OF LAWS, PANJAB UNIVERSITY.

** 5th YEAR B.A. LL.B. (HONS.) STUDENT, AMITY LAW SCHOOL, DELHI.

1 Fangfei Wang, F. (2010). Law of electronic commercial transactions.1st ed. Routledge, p.5.

Contemporary electronic commerce involves everything ranging from ordering 'digital' content for immediate online consumption, to ordering conventional goods and services, to "meta services" to facilitate other type of electronic commerce.

Business-to-business transactions play a vital tole in e-commerce market in a way wherein big corporations and financial institutions exchange financial data with the medium of internet to facilitate domestic as well as international business, however a large portion of revenue is generated from business to consumer transactions which provides consumers with varied multiple benefits like availability of goods at lower cost, wider choiees and doors step delivery options which saves time and energy. People have the freedom to purchase goods with a click of the mouse button without having to move out of house.

An E-contract is a contract modelled, executed and enacted by a software system. The business transaction administered by e-contracts is automated by the computer programs. E-contracts can be mapped to inter-related programs, which have to be specified carefully to satisfy the contract requirements. Such contracts are not capable of handling complex relationship that arises between the parties to an e-contract. E-contract is any kind of contract formed during the course of e-commerce by interaction of two or more individuals using electronic means such as e-mail, the interaction of an individual with an electronic agent, such as computer program, or the interaction of two electronic agents that are programmed to recognize the existence of a contract.[2]

Essentials of an Offline Contract

Indian Contract Act, 1872 concerns itself with the law relating to contracts in India. The act is based on the principles of English Common Law. The act deals with the circumstances in which promises made by the parties to a contract shall be legally binding on them.

Meaning and Definition

The definition of Contract is given under Section 2(h)[3], which provides *"a contract is an agreement enforceable by law"*.

Therefore the definition of contract can be divided in to two elements: An agreement and its enforceability by law.

1. An agreement is defined u/s 2 (e) as *"every promise and every set of promises, forming consideration for each other"*. Promise is the acceptance of proposal. Thus

2 Morakhia, S. (2018). *E Contracts and Issues Involved.* [online] Academia.edu. http://www.academia.edu/8719077/E_Contracts_and_Issues_Involved.

3 The Indian Contract Act, 1872.

an accepted proposal becomes an agreement. Therefore, in order to form an agreement there must be a proposal or an offer by one party and its acceptance by other party.

2. The second part of the definition deals with enforceability by law. An agreement is enforceable u/s 10 if it is made by competent parties, out of their free consent and for lawful object and consideration. Thus all contracts are agreements but all agreements are not necessarily contracts.[4]

Essential Elements of a Valid Contract

Section 10 of the Act[5] envisages, *"All agreements are contracts if they are made by free consent of parties, competent to contract, for a lawful consideration and with a lawful object and are not hereby expressly declared to be void"*. The essential ingredients of a valid contract are[6]:

1. *Agreement*

To constitute a contract there must be an agreement. There must be two parties to an agreement, i.e. one party making an offer (offeror) and the other party accepting the offer (offeree). The terms of the offer must be definite and acceptance must be absolute and unconditional. The acceptance must be according to the mode prescribed and must be communicated to the offeror.

2. *Offer / Proposal*

An offer is a proposal by one person, whereby he expresses his willingness to enter into a contractual obligation in- return for a promise, act or forbearance. Section 2(a) defines proposal or offer as *"when one person signifies to another his willingness to do or abstain from doing anything with a view to obtaining the assent of that other to such act or abstinence, he is said to make a proposal."*

3. *Consensus-ad-idem (Meeting of Minds)*[7]

To constitute a valid contract, there must be meeting of minds i.e. consensus-ad-idem

4. *Intention to create legal relationship*

The two parties enter into an agreement, there must be an intention by both parties to legally bind the other as a result of such agreement. Thus, agreements of social or household nature are not contracts.

4 www.lawnn.com.

5 The Indian Contract Act, 1872.

6 ibid.

7 www.educonz.com.

5. *Capacity of Parties (Competence):*

The parties to the agreement must be capable of entering into a valid contract. According to Section 11, every person is competent to contract if he or she,

1. is of the age of majority;
2. is of sound mind; and
3. is not disqualified from contracting by any law to which he is subject.

6. *Lawful Consideration*

An agreement to form a valid contract should be supported by consideration Consideration means "something in return" (quid pro quo). It can be cash, kind, an act or abstinence. It can be past, present or future. However, consideration should be real and lawful.

7. *Free Consent*

To constitute a valid contract there must be free and genuine consent of the parties to the contract. It should not be obtained by misrepresentation, fraud, coercion, undue influence or mistake.

8. *Lawful Object*

The object of the agreement must not be illegal or unlawful. Section 23: According to Section 23, the consideration or object of an agreement is lawful, unless-

- it is of such nature that, if permitted it would defeat the provisions of any law or is fraudulent; or
- it involves or implies, injury to the person or property of another; or
- the court regards it as immoral, or opposed to public policy.

9. *Agreement not declared void or illegal*

Agreements which have been expressly declared void or illegal by law are not enforceable at law; hence does not constitute a valid contract.

10. *Certainty and possibility of performance*

The terms of agreement must be certain and not vague. If it is not possible to ascertain the meaning of the agreement, it is not enforceable at law. Also, agreements to do impossible acts cannot be enforced.

II. Legal Formalities

A contract may be oral or in writing If, however, the law requires for a particular contract, it should comply with all the legal formalities as to writing, registration and attestation.[8]

Formation of E-Contract

E-contracts functions on the same Principles and remedies of traditional contract.Technological advancement has revolutionized the conventional paper based contracts to online contracts.Business activities are now shifting from paper based contracts to online contracts, leading to the emergence of a new set of contracts, called, "electronic contracts".[9] The simple understanding of the word suggests that the word means a contract formed electronically.Electronic commerce can be defined as "Electronic buying and selling on the internet and includes all the activities that a firm performs or selling and buying services and products using computers and communication technologies"[10].

The following legal requirements can be summarised upon legal contracts:

1. Clear identification of contracting parties.
2. Clear indication of the subject of the contract.
3. Clear indication of the time period of validity.
4. The contract must have valid signatures of the involved parties certifying their acceptance of the liabilities laid down in the contract. The date on which the contracts validity commences has to be mentioned as well.
5. Clause of Non-Repudiation which means that under no circumstances will the content of the contract be changed once such contract has been signed.

Need for E-Contract

The need for quick, efficient and time saving mode of contracting is the basic premise for the need of an E-contract in the 21st century. The obstacles of distance and queuing up can be easily tackled by parties entering into a contract over the internet. In the electronic age, the whole transaction can be completed in seconds, with both parties simply affixing their digital signatures to an electronic copy of the contract.

8 Available at www.referabbleknowledge.over.blog.com.

9 Electronic Contracts and the Law in India, Asian School of Cyber Law.

10 JogaRao, S. (2005). Computer contracts & information technology law. 2nd ed. New Delhi: Wadhwa and Company, p.182.

An electronic contract aims to[11]:

- To create a secured atmosphere of transacting online with alternative mode to paper and writing.
- To create an electronic documentation system which will safeguard the contracting parties on par with the traditional mode of contracts.
- To create statutory status monitoring/verifying authorities for such electronic transactions.
- To check frauds, intentional and unintentional transactions to promote and build confidence in genuine online transactions.
- To create necessary legal structure to oversee such transactions to establish standard rules and regulations for smooth functioning of online transaction.
- To make Digital Signature legally valid and incorporating the same with the existing legal regime of contracts, sale of goods, evidence and consumer acts.

Legal Validity of E-Contracts in India

India has an internet user base of over 100 million users. The penetration of e-commerce is low compared to markets like the United States and the United Kingdom but is growing at a much faster rate with a large number of new entrants. The industry consensus is that growth is at an inflection point with key drivers being:

- Increasing broadband Internet and 3G penetration.
- Rising standards of living and a burgeoning, upwardly mobile middle class with high disposable incomes.
- Availability of much wider product range compared to what is available at brick and mortar retailers.
- Busy lifestyles, urban traffic congestion and lack of time for offline shopping.
- Lower prices compared to brick and mortar retail driven by disintermediation and reduced inventory and real estate costs.
- Increased usage of online classified sites, with more consumers buying and selling second-hand goods.
- Evolution of the online marketplace model with sites like ebay, Infibeam and Tradus.

11 : Rastogi, S. (2013). Insights into e-contracts in India.

E-commerce websites are Internet intermediaries within the meaning of IT Act, 2000. "Intermediary", with tespect 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 service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places, and cyber cafes. The IT (Intermediaries Guidelines) Rules of 2011 regulate the functioning of e-commerce websites. Cyber law due diligence is the main aspect that all e-commerce site owners should comply with.

The conventional law relating to contracts i.e. The Indian Contract Act of 1872 is not equipped to address all the issues that arise in electronic contracts. The Information Technology Act solves some of the peculiar issues that arise in the formation and authentication of electronic contracts.Chapter IV of the Information Technology Act, 2000 i.e. sections 11, 12 and 13 covers the aspects of Attributiou, Acknowledgment and Dispatch of Electronic Records. According to Sec.10A of the IT Act, 2000, a communication or contract shouldn't be denied or declared void merely because it's in electronic form. It thereby acknowledges the legal validity of e-contracts.

Section10A of the act[12] confers legal validity and enforceability on contracts formed through electronic means. This provision was inserted to clarify and strengthen the legal principle enshrined in section 4 of IT Act, 2000 that *Electronic documents are at par with traditional documents and e-contracts are legally recognized and acceptable in law.* Force of law will build the netizens confidence in e-commerce activities thus facilitating its growth.

Correspondence with Article 11 of Model Law on E-commerce adopted by UNCITRAL

- The UNCITRAL Model Law on Electronic Commerce[13] instead of defining an E-Contract, it, merely states that " a contract can be made by exchanging data messages and when a data message is used in the formation of a contract, the validity of such contract should not be denied."[14]
- A transaction formed by electronic messages in which the messages of one or both parties will uot be reviewed by an individual as a routine step in forming of the contract.

12 IT Amendment Act,2008.

13 Model law 1999.

14 UNICITRAL Model Law on E-Commerce, 1996 Article II.

The Information Technology Act, 2000, defines 'data' as a representation of information, knowledge, facts, concepts or instructions which are prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or a computer network, and may on any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.[15]

According to UNCITRAL Model Law, 'data messages' means ' information generated, sent, received or stored by electronic, optical or similar means including, but not limited to Electronic Data Interchange(EDI), electronic mail, telegram, telex or telecopy.[16]

Forms of E-Contract

Electronic contracts can be executed by two ways:

1. First is through the exchange of Electronic Mail (e-mail).
2. Second, is through the use of World Wide Web (or Website), which can be further classified as -
    - Click Wrap
    - Browse Wrap
    - Shrink Wrap

- ***Electronic Mail***

  Electronic mail also called as "e-mail", is used as a method of exchanging digital messages across the internet or other computer networks across the globe. It means the transmission of messages over communication networks.

  Anyone interested in communicating business details through e-mail must have an e-mail address for which he has to register himself with the Internet Service Provider(ISP) who runs a constantly accessible mail server. Once the registration is complete by filling up the form which is electronically available, an electronic mail box(inbox) along with the address is allocated to the user. The person wishing to send an offer to another will type the desired contents of the offer on his system with an e-mail address of a party to whom he intends to send the offer which is to be mentioned in the address column.

15 S.2(o) of Information Technology Act, 2000.

16 UNCITRAL Model Law on E-Commerce, 1996, Article 2 (a).

The message then is electronically transmitted by pressing the 'send' button to the service provider of the sender and is then forwarded to the recipient's provider who puts it in the recipient's mailbox whereit is saved. Placing e-mail in the recipient's mailbox does not enable him to know the contents of the message. Similarly, the sender does not know whether the recipient has received the message[17].An email contract is read by each contracting party, rather than processed automatically by an information system. It can assume any form which the parties are willing to accept.

- *Click Wrap Contracts*

Also called as "click through" agreement or "click wrap license". In common parlance, these are the agreements that we generally stumble upon while surfing the internet such as "I AGREE" to the terms or "I DISAGREE" to the above conditions. Click Wrap agreements allows the user to be well versed with the terms and conditions of the agreement before accepting it. The enforceability of the click wrap is through the act of "clicking" the "accept" button thereby giving his assent without any requirement of signature and without any opportunity to amend the conditions. These type of contracts are extensively used on the Internet, for either granting permission to access a site or downloading of a software or selling something online by way of a website. The case of click wrap agreement is different from that of other contracts because these contracts are executed instantaneously "The main difference between click wrap contracts and emails is that the communication between web clients and servers, unlike e-mails is instantaneous". In case of Click Wrap agreement, a party posts terms on its website pursuant to which it offers to sell goods or services. To buy these goods, the purchaser is required to indicate his assent to be bound by the terms of the offer, by his conduct i.e. typically the act of clicking on a button stating "I agree". Once the purchaser indicates his assent to be bound, the contract is formed on the posted terms, and the sale is consummated No paper record is created nor is the signature of the purchaser required. The product cannot be obtained or used unless and until the icon is clicked.

A web-wrap license is considered as an Internet contract that asks the user to accept the terms of the license by clicking a "yes" or "no" button before or after seeing the complete agreement. A "yes" gives the user complete access to the website. A "no" prevents the user from gaining access to all or some of the information on the site. This is also known as a click-wrap license.

17 Ahmad, F. (2005). Cyber law in India. Delhi: New Era Law publications.

Types of Click-Wrap Agreements: -

Click wrap agreements are of two types:-

- Type and Click: In this case user must type "accept" or other specified words in an onscreen box and then click "submit" or similar button to indicate acceptance of contractual terms. Without such action, the user cannot proceed to access the targeted Web site, download the desired software, or purchase the desired product or service.
- Icon Clicking: In this case the user must click on an "ok", "I agree", or similar icon to signal acceptance of the terms. Access is denied unless the button is clicked. A user indicates rejection by clicking "cancel" or closing the window.

They are "take it or leave it" agreements in which the user is not made aware of the terms of contract until late in the transaction (just before the use of the product) which is different from a traditional written contract.[18].

- ***Browse Wrap***

  In a browse wrap agreement, the terms and conditions of use for a website or other downloadable product are posted on the website as a hyperlink, at the bottom of the screen. Browse wrap agreement do not appear on the screen. The user is also not compelled to accept or reject the terms as a condition of proceeding with further computer operations. Browse wrap agreement does not require the express manifestation of assent. Rather, a website user purportedly gives his assent by simply using the product.

  There is uncertainty of enforceability with browse wrap agreements because is it unclear whether the person using the website has actually accepted the terms of the agreement or not. The courts[19] have held the validity of a Browse Wrap agreement. It is primarily based on whether the user of website had actual or constructive notice of the terms and conditions prior to using the website or the product.

- ***Shrink Wrap***

  'Shrink Wrap contract' refers to license agreements or other terms and conditions of a contractual nature. Such terms or license agreements can only be read and accepted by the customer after opening the product. In this the

18 Lemly, M. (2006). Software and internet law, page 382. [online] Berkely Law. http://www.law.berkely.edu/5638.html

19 *Hubbert v Dell Corp* [2005] (Appellate Court of Illinois,Fifth District.).

20 Raghvendra S Shrivastava, Online contracts.

people agree to the terms by using the software which they have already purchased. When software is licensed, it is packed in such a way that a note is attached at the top of the packaging which contains the terms and conditions for the use of such software. Once the package is opened by the user, the user is deemed to have read such conditions and will be bound by them.[20]

The term Shrink wrap describes the plastic wrapping which is used to cover software boxes but that does not mean that such contracts are limited to software industry only. The license is contained inside a plastic shrink wrapped box containing the software. The logic behind this is that by breaking the seal i.e. pulling off the plastic wrap, the user agrees to the terms of the license. Thus, a Shrink Wrap license can be defined as an unsigned agreement between the purchaser of a mass market computer software program and the computer software company that developed the concerned software. This license purports to define the terms of the transaction as well as placing contractual conditions on the purchaser's use of the software. The license is normally connected to the software in such a manner that the purchaser should notice and read the license prior to using the software.[21] The terms of the contract must be communicated to the user otherwise lawyers can easily argue that they are not binding. The opening of the shrink wrap confirms that the customer has accepted the terms of the license. The acceptance of the agreement is inferred by opening the package or using the software even without the license terms being read.

Computer software companies rely a great deal upon the shrink wrap license agreement to guard their perceived interests in the mass market distribution of their software by retaining title to the copy of the software- the software is licensed and not sold to the purchaser. By doing so, the Computer Software Company theoretically attempts to impose conditions upon the licensee, the purchaser, that are not otherwise permissible under copyright law.

The principle terms of shrink wrap license[22] are:

- prohibition on making unauthorized copies of the software,
- prohibition on rental of the software,
- prohibition on reverse engineering and modifications of the software,
- limiting the use of the software to one central processing unit,
- disclaiming warranties; and
- limiting liability.

21 http://library.findlaw.com.

22 ibid.

Shrink Wrap contracts usually read something like, "By overling the packaging on this box you agree to the terms and conditions of the license."[23] The terms and conditions of the license are generally located inside the box. This way an indirect E-Contract is formulated.

The shrink-wrap license agreement purports to create a binding legal agreement (so it says) between the software vendor and the user. The agreement is usually found inside the box containing the software, printed on the envelope containing the CD-ROM or disks, or stated in the user manual. Usual Statement appears at the beginning, warning the user not to open the software envelope or use the software, if he or she does not agree with the terms and conditions of the agreement. Use of this type of agreement has become the legal licensing paradigm of the software industry for consumer mass-market software. The term "shrink-wrap" derives from the fact that such agreements used to be included on the outside of the software packaging, visible through the clear plastic shrink-wrap with which the package was sealed.

These are adhesion contracts and hence share procedural and substantive aspects. In particular, each of them shares the following three characteristics. Firstly, these contracts are not entered into between the parties as a result of meaningful negotiation. Secondly, the agreements are impossible to change. Thirdly, the buyer's or user's assent to the terms may be either absent or ambiguous. These are the three distinguishing traits that form the legal basis for challenging the enforceability of such agreements. Contracts of adhesion differ significantly from the traditional process of contract formation. In an adhesion contract, the parties do not negotiate because the terms and conditions that are presented to adherents are non-negotiable. The lack of meaningful bargaining between the parties leaves the adherent in the position that the deal is either accepted or there is no deal.

Evidentiary Value of E-Contracts

Proper evidentiary value has been accrued to any recorded or stored evidence which is obtained with the help of electtonic devices. A tape recorder recording voice, digital-voice recording by recorders, digital cameras, digital video cameras and video conferencing are some of the most newly added resources having evidentiary value. The status of video conferencing[24], cellular phones' call records[25]

23 David Callan, *How Click Wrap Contracts benefit over Shrink Wrap contracts*, http://lawyerintl.com.

24 State of Maharashtra v. Praful B Desai AIR, 2003 SC 2053: 2003 (2) AIT (Cri) 118 (SC), where examination of witnesses in criminal cases through video conferencing was approved.

25. State v. Navjot Sandhu, AIR 2005 SC 3820, Call records relating to cellular phones are admissible and reliable.

and SMS, MMS and electronic mail comprising the electronic documents in India has been well covered under the law, more so because of the judicial interpretation in plethora of cases. In the case of State of Delhi v. Mohd. Afzal,[26] it was held that evidence in the form of electronic records is admissible as evidence. If somebody questions the correctness of an electronic evidence or e-record on the basis of system mishandling, or operational oversight, or interpolation, then in that case, the person questioning it must prove it beyond reasonable doubt. The Court observed that apprehensions which are solely theoretical and general can in no case turn evident evidence deficient and that which is not admissible. The above-mentioned case indicated the admissibility of electronic evidence in numerous ways in the courts of India.

This era of information technology along with the enforcement of the IT Act, 2000 has been successful in bringing many amendments in some Acts which includes the Indian Evidence Act, 1872 as well. These changes were essential in light of the value of an electronic record as an evidence, electronic signature, and essentially, electronic contracts. The value of e-contracts as an evidence should be acknowledged considering the following provisions of the Indian Evidence Act. With regard to the presumptions as to electronic records, the relevant sections are 85A, 85B, 85C, 88A, and 90A; while admissibility of electronic record is dealt under Sections 65A and 65B.

Section 85A[27]: This section talks in terms of the presumption as to electronic agreements. It states that as soon as electronic signature is affixed to an electronic record which is of the form of an agreement. This provision has been incorporated to safeguard the validity of e-contracts. But, as regards the value of this presumption, some restrictions have been imposed.

Section 85B[28]: Section 85B states that it shall be presumed by court that the record being considered is not put to any type of variation, if contrary is not proved. It is

26 Delhi v. Mohd. Afzal, 2003(71) DRJ 178.

27 Indian Evidence Act, No. 1, Acts of Parliament, 1872, Sec. 85A, reads as: Presumption as to electronic agreements: The Court shall presume that every electronic record purporting to be an agreement containing the electronic signature of the parties was so concluded by affixing the electronic signature of the parties. Ins. by Act 21 of 2000, sec. 92 and Sch. II (w e f. 17-10-2000).

28 Ibid., Sec. 85B, Presumption as to electronic records and electronic signatures.- (1) In any proceedings involving a secure electronic record, the Court shall presume unless contrary is proved, that the secure electronic record has not been altered since the specific point of time to which the secure status relates.

(2) In any proceedings, involving secure electronic signature, the Court shall presume unless the contrary is proved that- (a) the secure electronic signature is affixed by subscriber with the intention of signing or approving the electronic record; (b) except in the case of a secure electronic record or a secure electronic signature, nothing in this section shall create any presumption, relating to authenticity and integrity of the electronic record or any electronic signature. Ins by Act 21 of 2000, sec. 92 and Sch. II (w e f. 17-10-2000).

necessary under this provision that the demand for a secured record can be made only till a specific time. Moreover, the assumption in such cases is that the affixation of electronic signature is clearly indicative of the intent to sign and approve the electronic record. Moreover, it is stated that the provision must not be misconstrued as one which draws any presumption regarding the integrity or authenticity of the electronic record or electronic signature in question.

Section 85C[29]: With regard to the electronic signature certificate, it shall be presumed by the court that the details provided in the certificate are correct and true. Here again the words 'shall presume' is used to indicate that the court doesn't have any discretionary power.

Section 88[30]: Section 88 talks about the presumption as to telegraphic message, whereas Section 88A[31] S. 88A reads as: Presumption as to electronic messages- The Court may presume that an electronic message, forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent.

Explanation- For the purposes of this section, the expressions "addressee" and "originator" talks about presumption in case of electronic messages. In light of these provisions, it may be presumed by the court that an electronic message that is forwarded to the addressee by the originator is analogous to the message that his system has stored with an inrention to transmit with the help of electronic mail server. However, the court shall not presume anything relating to the sender of the

29 Supra note 27, Sec. 85C, Presumption as to Electronic Signature Certificates.- The Court shall presume, unless contrary is proved, that the information listed in a Electronic Signature Certificate is correct, except for information specified as subscriber information which has not been verified, if the certificate was accepted by the subscriber. Ins by Act 21 o f2000, sec 92 and Sch. II (w e f. 17-10-2000).

30 Supra note 27, Sec. 88, The Court may presume that a message, forwarded from a telegraph office to the person to whom such message purports to be addressed, corresponds with a message delivered for transmission at the office from which the message purports to be sent; but the Court shall not make any presumption as to the person by whom such message was delivered for transmission.

31 Supra note 27, Sec. 88A, Presumption as to electronic messages- The Court may presume that an electronic message, forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent.
Explanation- For the purposes of this section, the expressions "addressee" and "originator" shall have the same meanings respectively assigned to them in clauses (b) and (za) of subsection (1) of section 2 of the Information Technology Act, 2000. Ins by Act 21 o f2000, sec 92 and Sch. II (we f 17-10-2000).

message. This provision is in itself very clear as it claims to emanate the fundamental rules of a valid agreement in the hard copy form. The phrase 'may presume' gives the power to the court that in respect of presumption, discretionary power can he used by it. Sections 85A and 85B consist of the phrase 'shall presume' which, in express manner, doesn't include the power of the court which is discretionary in nature.

Section 90A[32]: Where an electronic record is five years old and it is proven that it is in proper custody, then it may be presumed by the court that the e-signature was affixed for the purpose of authenticating the validity of the agreement. Here, the e-signature can be affixed by any authorized person. For this provision, when electronic records are in the custody of the person with whom they will naturally be, they are said to he in proper custody, except when the circumstances of a given case makes its genesis certain.

Sections 65A[33] and 65B[34] extensively talk about evidence which is related to electronic records and the admissibility of such records.

Section 65B states that within an e-record, any information that is printed on a paper or recorded, stored, copied on optical or magnetic media and produced by a computer shall he taken as a document and as far as its evidentiary value is concerned, in any proceeding, it shall be as admissible without any proof or production of the original.

Furthermore, it is given that in case of any proceedings where evidence of an electronic record has to be produced, a certificate consisting of the essentials given by Section 65B of the Evidence Act, and which is signed by person holding a respectable official position relating to the functioning of the given device or the management of particular activities will be considered sufficient evidence as far as the matters given in the certificate are concerned.

32 Presumption as to electronic records five years old.- Where any electronic record, purporting or proved to be five years old, is produced from any custody which the Court in the particular case considers proper, the Court may presume that the electronic signature which purports to be the electronic signature of any particular person was so affixed by him or any person authorised by him in this behalf.

Explanation: Electronic records are said to be in proper custody if they are in the place in which, and under the care of the person with whom, they naturally be; but no custody is improper if it is proved to have had a legitimate origin, or the circumstances of the particular case are such as to render such an origin probable. This Explanation applies also to section 81A. Ins by Act 21 of 2000, sec 92 and Sch. II (w e f 17-10-2000).

33 Supra note 27, Sec. 65A, Special provisions as to evidence relating to electronic record. The contents of electronic records may be proved in accordance with the provisions of section 65B. Ins by Act 21 of 2000, sec 92 and Sch. II (w e f 17-10-2000).

34 Indian Evidence Act, No. 1, Acts of Parliament, 1872, Sec. 65B.

The Supreme Court in the case of State v. Navjot Sandhu,[35]while analysing the provisions of recently added section 65B, held that in a particular case, it may be that the certificate consisting of the details under sub-section 4 of section 65B might not be filed, but that doesn't imply that secondary evidence cannot be given. It was held by the Court that it is allowed by the law that such evidence can be produced in the circumstances mentioned under sections 63 and 65 of the Indian Evidence Act. According to Section 63, secondary evidence means and includes, including other things, copies made from the original by processes mechanical in nature, which by itself ensures the authenticity of the copy.

Section 65 allows secondary evidence of the contents of a document to be produced if the original cannot be easily moved. Therefore, printouts obtained from computers by a process which is mechanical in nature and which a reputable official of the service providing company has attested, may be presented as evidence with the aid of a witness who is familiar with the certifying officer's signatures and can thus, recognise them or if he, based on personal knowledge, can speak about facts. In spite of following the essentials of section 65-B, which is a section relating to the admissibility of electronic records, there is no restriction to produce secondary evidence under sections 63 and 65 of the Indian Evidence Act.

The value of an evidence of an electronic record solely relies upon its quality. The Indian Evidence Act discusses the evidentiary value of the electronic records in detail. According to Section 3 of the Evidence Act, evidence means and includes all documents which include documentary evidence meaning the electronic records which are produced for the inspection of the court. Consequently, the provision throws light on the fact that documentary evidence can also be in electronic record form and is at an equal pedestal to the documents of the conventional form.

According to the IT (Amendment) Act 2008, Section 79A of the IT Act gives the power to the Central Government to appoint any department, body or agency to examine electronic form evidence and give expert opinion on it before any court or authority. As far as this section is concerned, 'electronic form evidence' means any information or probative value which is either stored or transmitted in electronic form including computer evidence, digital audio, digital video, cell phones and digital fax machines.

While concluding, we can say that e-contracts are similar to paper or hard copy contracts when we talk in terms of its evidentiary value. All the e-contracts are valid contracts as legitimised by the IT Act as well as by the amendment of 2008 and, hence, in case of any violation of terms and conditions, a person can be made liable.

35 AIR 2005 SC 3820.

Jurisdictional Issues

The efficiency of a legal system relies on the core of regulations- regulations that exemplify every facet of the functioning of a system and chiefly its jurisdiction. A court should have jurisdiction, location and suitable processes must be served in order to adjudicate upon a case and give an effectual judgment. Jurisdiction is a legal word enumerating which law is in operation at some specified period of time and decision of which court decision will be binding. Jurisdiction is primarily the authorised power with the help of which cognizance is taken by courts and matters are adjudicated upon.[36] It is the legitimate power of the court to hear a case and resolve a dispute between persons, property and subject matter.[37] Any decision of the court which is devoid of jurisdiction can be called ineffectual and fruitless. The term jurisdiction has been imported completely, and touches upon every form of judicial act. This jurisdiction is mainly of two types: subject matter jurisdiction and personal jurisdiction, and both of these should be fulfilled together and only then a judgment will be held valid. Subject matter jurisdiction includes the ability of a given court to hear the kind of case that is there before it. Personal jurisdiction includes the ability of the court to deliver a judgment against a party to an action or a proceeding.[38] It is because of the jurisdiction that the court exercises, which grants it the enforcement power and if such power is not there, the decision of the court doesn't hold any significance. Furthermore, only principles of jurisdiction accepted generally would warrant that foreign courts also implement other judicial bodies' orders.[39] One of the biggest legal difficulties posted by electronic commerce today is a result of one of its biggest benefits of the internet, which is that it traverses national and jurisdictional boundaries. This in turn instantly raises challenges relating to the domain of Private International Law or the Conflict of Laws. Particularly, two instant challenges we have to deal with in this context are: (a) which law will govern any contract; (b) would the Indian courts exercise jurisdiction to take up an action on the basis of such a contract. In case of the world that exists outside the realm of the online world, cases are solved using the conventional process which is litigation in the courts, essentially constructed on the basis of territory, i.e. every nation consists of its own laws and courts that solve disputes within their jurisdiction, essentially based on the implementation of local laws. Till the parties to an online dispute are part of the same jurisdiction, the problem is none since the dispute here will be solved like it in the case of offline contracts. For instance, ABC enterprises

36 S.K. VERMA & RAMAN MITTAL, LEGAL DIMENSIONS OF CYBERSPACE (Indian Law Institute), Chapter 10, *Resolution in Cyber Space ; Determining jurisdictional and applicable law.*

37 Vakul Sharma, *Information Technology Law and Practice- Cyber Law & E-Commerce*, Universal Law publishing Co. Pvt. Ltd., New Delhi, 2003.

38 ibid.

39 NANDAN KAMATH, LAW RELATING TO COMPUTERS INTERNET AND E-COMMERCE (A GUIDE TO CYBER LAWS & THE INFORMATION TECHNOLOGY ACT).

which is based in Delhi and having its customers in Delhi, manufactures certain kinds of goods and through their web site, sells them. If there is any dispute between ABC enterprises and their its customer, it will be resolved with the laws applicable in Delhi. But the issue arises in cases where their its customers belong to separate countries and transaction takes places between them on their web site. This dispute resolution mechanism, territory based, is plagued by a number of issues when its application is made on the disputes that arise on the Internet. The internet is, by its very definition, international in nature whose access can be gained from almost any part of this planet and therefore it can be called as multi-jurisdictional Digitised data on the internet can move from one country to another and in different jurisdictions so that it can travel to its destination. For instance, an issue might take place among two parties of different countries who contracted with each other on the internet. The question that arises is the courts of which country can exercise jurisdiction to solve this issue? Which country's laws must be considered to resolve the issue? What laws must be taken into account to resolve a particular dispute? These questions which are baffling are at present being encountered by courts all over the world due to internet's transnational nature by which people can transcend borders readily and rapidly. While most laws have territorial nexus, the internet flouts the idea of territoriality.[40]

Position in the US

As far as the position in US is concerned, there is uniformity in the two state acts which have been brought about by the National Conference of Commissioners on Uniform State Laws (NCCUSL)[41] in order to establish legal certainty to transactions made electronically. These are: the Uniform Computer Information Transaction Act (UCITA) and the Uniform Electronic Transaction Act (UETA). The UCITA deals with contracts or transactions in 'computer information'.[42] A contract which involves computer information, like a software license, may be made electronically or may be completed in person or by any other means. Thus, the UCITA is

40 *Supra* note 36.

41 Introduction to the Organization, The National Conference of Commissioners on Uniform State Laws, http://www.nccusl.org/Update/Desktop Default.aspx? tabindex = 0 & tabid = L

42 Comment 2 to UCITA Sec. 103. The scope of this Act turns initially on the definition of computer information transaction. Sec. 102(11). Computer information transactions are agreements that deal with the creation, modification, access to, license, or distribution of computer information. Sec. 102(a) (11). Computer information is information in a form directly capable of being processed by, or obtained from, a computer and any copy, associated documentation, or packaging Sec. 102(a) (10). As stated in subsections (b) and (c), if a transaction is a computer information transaction but also involves other subject matter, this Act ordinarily applies only to the aspects of the transaction that involve computer information.

concerned with information technology, and is not entirely concerned with e-contracting. On the other side, the UETA has a relatively extensive application, emphasising on every kind of e-transaction. The above acts, uniform in nature are not binding in a particular State till it is the adopted by the State through its respective legislative process. However, these Acts formed by NCCUSL have been adopted by all or many States and are essentially highlight the present and future trend. For instance, UETA has been adopted by 48 States.[43] On the other hand, UCITA has been adopted by only two States- Maryland and Virginia, where software and internet related businesses are located.[44]

The US Congress has also passed the Electronic Signatures in Global and National Commerce ('E-Sign') Act in 2000. The Act acknowledges the validity of contracts formed in an electronic form with the inclusion of electronic signatures in them. The underlying purpose of this Act was to give e-contracts validity which is at par with the conventional paper based offline contracts.

Conclusion and Suggestions

In this paper, the researcher has made an attempt to study the meaning and definition of e-contract and to understand the essentials of e-contract vis-à-vis the essentials of an offline contract given under the Indian Contracts Act, 1872. The researcher thus reached a conclusion that just like an offline contract, online contract or e-contracts are also legally valid as they fulfil all the essentials of a contract. Their legal validity is given under Information Technology Act which is made in consonance with the Model Law on E-Commerce adopted by UNCITRAL. Moreover, the researcher has discussed the various forms of e-contracts and their validity in detail. Further, the researcher has delved into the evidentiary value of e-contracts which is somewhat similar to that of traditional contracts, as enumerated under the Indian Evidence Act, 1872. In consonance with the above discussion, it is more or less clear that e-contracts, in varied forms are valid and enforceable. This assertion is rightly supported the decisions by the courts and the actions of the legislature. The click-wrap, shrink-wrap and web-wrap agreements and their enforceability is a domain which is moving towards growth and development. The researcher also looked into the jurisdictional issue that often creeps in the domain of e-contracts. The researcher has discussed laws, rules and regulations, as well as necessary

43 Legislative Fact Sheet on UETA, The National Conference of Commissioners on Uniform State Laws, http://www.nccusl.org/Update/uniformact_factsheets/ufmiformacts-fs-ueta.asp.

44 Sylvia Mercado Kierkegaard, *E Contract Formation: U S and EU Perspectives*, 3 Shidler J. L. Com. & Tech. 12 (Feb 14, 2007), at http://www.lctjournal.washington.edu/Vol3/a012Kierkegaard.html.

amendments brought about in India to govern e-contracts in contrast to the position in US. The basis of the legislations relating to e-commerce in US is that they validate e-contracts thus, creating legal certainty. And certainly, their laws are broader in scope.

However, in India, one suggestion with respect to the validity of e-contracts can be that although, the concept of offer and acceptance made electronically to form a contract has been acknowledged by the courts, the provisions of the Contract act must deal this more extensively and for that, an amendment to the act is necessary. A law must adapt itself to the dynamic nature of the society and this is also applicable to contractual laws. And therefore, it is the need of the hour to frame a definite and specific law governing e-contracts and their regulations in India.

REGULATING CRYPTOCURRENCY IN INDIA BIT BY BIT

Anjali Agrawal*

ABSTRACT

The currency that we use today is referred to as 'fiat currency'. The Latin word 'fiat' literally means 'let it be done'. Thus, the term 'fiat currency' means a currency whose value is decreed by a government, and the government promises to pay the holder of such currencies an equivalent amount in gold, if needed. Thus, such a currency is called 'centralised' because it is generally issued by a central body.

A cryptocurrency, on the other hand, is a medium of exchange that uses cryptography to manage the creation of new units as well as secure the transactions. The cryptocurrency network diminishes the need of a trusted third-party such as governmental agency, bank, etc. The cryptocurrency system is a peer-to-peer, client based, completely distributed currency that does not depend on centralised issuing bodies (a 'sovereign') to operate. The value is created by users, and the operation is distributed using an open source client that can be installed on any computer or mobile device. Numerous cryptocurrencies are currently active such as Bitcoin (the most widely known one), Ethereum, LiteCoin, Ripple and others. Today, the fundamental system on which most cryptocurrencies are based was created by an anonymous developer going by the pseudonym of Satoshi Nakamoto, the alleged creator of the Bitcoin.

Unlike fiat currencies, whose value is derived through regulation or law and underwritten by the state, cryptocurrencies derive their value through the principles of supply and demand – they have no intrinsic value and no backing, and their value depends entirely on what people are willing to trade for them. A cryptocurrency thus mirrors the economic market where the invisible hand of the market determines and regulates its value. One could thus go on to argue that a cryptocurrency is a contingent currency which can operate as a medium of exchange only if fiat currencies exist.

* *3rd Year, B.B.A. LL.B. (H.), University School of Law and Legal Studies, Guru Gobind Singh Indraprastha University, Dwarka, New Delhi*

The paper will attempt to answer the fundamental question raised about cryptocurrency – is it legally valid? In light of the prevalence of economic systems where the state has an absolute monopoly over currency, many have decreed cryptocurrency illegal. This paper will examine the different global perspectives on the issue and subsequently discuss the possibilities for India to deal with the legality of cryptocurrency. In addition, issues related to cryptocurrency such as tax implications, dealing with intellectual property, privacy, and data protection will be analysed in the paper. Given the electronic and networked nature of the manner in which cryptocurrencies operate, certain risks, in addition to risks borne by fiat currencies, are inherent to the system against which the network must be protected. These include, but are not limited to, cyber-attacks, hacking, money laundering, drug trafficking and terrorist financing. Against all odds, cryptocurrency has managed to spread and become the medium of exchange for numerous people. Therefore, regulating is of paramount importance.

Introduction

The currency that we use today is referred to as 'fiat currencies'. Thus, the term 'fiat currency' means a currency whose value is decreed by a government, and the government promises to pay the holder of such currencies an equivalent amount in gold, if needed. Thus, such a currency is called 'centralised' because it is generally issued by a central body.[45]

A cryptocurrency is a medium of exchange that uses cryptography to manage the creation of new units as well as secure the transactions.[46] The cryptocurrency network diminishes the need of a trusted third-party such as governmental agency, bank, etc. The cryptocurrency system is a peer-to-peer, client based, completely distributed currency that does not depend on centralised issuing bodies (a 'sovereign') to operate. The value is created by users, and the operation is distributed using an open source client that can be installed on any computer or mobile device. Satoshi Nakamoto created the fundamental system on which majority of the cryptocurrencies are based on.[47]

Satoshi Nakamoto published a paper online describing the Bitcoin for the first time. In his opinion, the major problem with conventional currency today is that,

45 Abba P. Lerner, *Money as a Creature of State*, 37 (2), AER, 312 (1947).

46 Andy Greenberg, *Crypto Currency*, FORBES (Nov. 05, 2017, 11:00 PM), https://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html.

47 Jerry Brito and Andrea Castillo (2013), *Bitcoin: A Primer for Policymaker*, MERCATUS CENTER, George Mason University. It is not sure whether Satoshi Nakamoto is the real name of the person or not.

trust is required to make the system work. But, looking at the history of fiat currency, it is full of breaches of such trust. Satoshi further states that banks use the currency entrusted to them to lend it out in 'waves of credit bubbles', with hardly anything left in reserve.[48]

And unlike fiat currencies, whose value is derived through regulation or law and underwritten by the state, Bitcoin derive their value through the simple principles of supply and demand – they have no intrinsic value and no backing, and their value depends entirely on what people are willing to trade for them.

Meaning of Cryptocurrency

Bitcoin was developed in 2008 as a concept by an anonymous developer going by the pseudonym of Satoshi Nakamoto, who posted a paper detailing the currency to a cryptography mailing list.[49] The paper details a decentralised system with no issuing authority that would serve as both a means of exchange but also as an anonymous and fully open log of all transactions (known as the blockchain). People running a client that would 'mine' value by verifying transactions would create the value, which encourages users to allocate processor time to confirm trades. When the algorithm was created by Nakamoto, a finite limit of 21 million on the number of Bitcoin that would ever exist was set.[50] Currently, over 12 million are in circulation.[51]

It is clear from Nakamoto's paper that this currency, unlike all the others, was based on math/cryptography and not trust. Bitcoin is simply allocating value arbitrarily to a program that performs the mathematical equations necessary to support the creation of a bitcoin. It is a self-referential and circular currency, and its only value is that which people give it, just like fiat money, but with faith placed in computer programming, not sovereign states.

What is blockchain technology?

The blockchain is a decentralised public ledger, or list, of all transactions of a particular cryptocurrency, and is the technology underlying most cryptocurrencies. It keeps a record of all transactions that take place across the 'peer – to – peer'

48 S. Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*, BITCOIN (Nov. 05, 2017, 11:00 PM), https://bitcoin.org/bitcoin.pdf.

49 *Ibid.*

50 Benjamin Wallace, *The Rise and Fall of Bitcoin*, (Nov. 05, 2017, 11:00 PM), http://www.wired.com/2011/11/mf_Bitcoin/.

51 Samantha Sharf, *$10: One Perspective On What Bitcoin Will Be Worth In 2014*, FORBES, (Nov. 05, 2017, 11:00 PM),https://www.forbes.com/sites/samanthasharf/2014/01/15/10-one-perspective-on-what-bitcoin-will-be-worth-in-2014/#7a4f62944ba7.

network. Users contribute to the network by providing computational power to assist with the verification of transactions in real-time (known as 'mining') as shown in figure 1.

The blockchain technology allows the users to transfer assets across the internet without the need for a central third-party. All personal information is encrypted; thus, no information is shared. However, a transaction record is created which is known as the ledger. For this reason, transactions are considered pseudonymous, not anonymous.

Ways to obtain the Bitcoin

There are three primary ways to obtain Bitcoin: first, mining new ones. Second, buying on exchange and third, accepting them for goods and services.

'Mining' is discovering new Bitcoin. In reality, it's simply the verification of Bitcoin transactions. In order to make sure a Bitcoin is genuine, miners verify the transaction. There are many transactions that individuals are trying to verify and not just one. These transactions are gathered into boxes with a virtual padlock on them which make up the 'block chains'. 'Miners' run software to find the key to open that padlock. Once the computer finds it, the box pops open and the transactions are verified. Hence, it can be said that while Bitcoin are 'mined' by individuals, they are 'issued' by the software.

Figure 1: The Blockchain Technology[52]

Tracking the transaction

Today, real currency is being used to purchase and sell Bitcoin at the current exchange value. Once the purchase has been made the value of the particular amount of Bitcoin is transferred from one wallet to another. Since every wallet has its own unique 33 characters and all Bitcoin wallets are synchronized, thus, a false entry by any single person being made is almost impossible. Although pseudonyms

52 PWC, *Making sense of Bitcoin, cryptocurrency, and blockchain*, PWC, (Nov. 05, 2017, 11:00 PM), https://www.pwc.com/us/en/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html.

are used for trading purposes, the history of every transaction in the form of continuously updated block-chain information is stored in the wallets.

Interaction of cryptocurrency with fiat currency

1. *Closed virtual currency scheme*

This scheme has minimal link to the actual economy. In this scheme, the user performs specified online tasks by paying a subscription fee to earn virtual currency. This currency can only be used to buy virtual goods and services within such community.[53]

2. *Virtual currency schemes with unidirectional flow*

In this scheme, real currency is used directly to purchase the virtual currency at a specified rate. Real goods and services may be bought in such a scheme using the virtual currency.[54]

3. *Virtual currency schemes with bidirectional flow*

In this scheme, fiat or real money is used to purchase cryptocurrency, which in turn is used to buy and sell virtual as well as real goods and services. In this scheme, the cryptocurrency can also he turned back into real money. Moreover, in this method, the cryptocurrency can be bought and sold in the exchange market. Bitcoin and most other currencies follow this scheme.[55]

4. *Supply and demand creation for cryptocurrency*

The price of any cryptocurrency is based on the basic principle of economics – more the demand higher the price. Thus, two variables on which the price of the cryptocurrency is dependent on are demand and supply. In 2010 when the cryptocurrency – Bitcoin was traded for the first time, the exchange value was between $0.008 and $0.08.[56] Today, the price of the same is nearly $7454.[57]. This clearly shows the increase in demand for cryptocurrency. Today, there are more than 1200 cryptocurrencies which are listed in the cryptocurrency

53 European Central Bank, *Virtual Currency Schemes*, EUROPEAN CENTRAL BANK, (Nov. 05, 2017, 11:00 PM), https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

54 *Ibid.*

55 *Ibid.*

56 Zebpay, *A look at the major milestones since the creation of Bitcoin*, ZEBPAY, (Nov. 05, 2017, 11:00 PM), https://www.zebpay.com/bitcoin-history.

57 Ryan Browne, *Bitcoin jumps $400 in one day and soars to a new record high*, CNBC, (Nov. 05, 2017, 11:00 PM), https://www.cnbc.com/2017/11/03/bitcoin-price-hits-yet-another-record-high.html.

exchange market.[58] The sheer amount of trading that is happening with the cryptocurrencies makes it an imperative of individual countries at a domestic level as well as an international level to come up with a regulation to protect investor and/or consumers (depending on how cryptocurrency is being treated) all around the world.

Global Perspective

Following are the initiatives that have been taken by different countries from all over the world for regulating cryptocurrencies. This list is illustrative and not exhaustive.

1. Canada

Canada is the first country to implement a national law for Bitcoin use. Businesses dealing in digital currency are now subject to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act of 2000* (PCMLTF). Under the PCMTF, 'dealing in virtual currencies'[59] has been subjected to the same reporting requirements as other money-services businesses.

Dealers in digital currency in Canada need to register as 'Money Services Businesses' (MSBs). Anyone that deals with customers will need to register as an MSB with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). The process involves contacting FINTRAC to provide initial information and gaining access to the MSB registration site; this requires answering numerous questions regarding the business owners, senior officers, banking relationships and projected revenues. While undertaking the process is not costly, it can take time, especially if the regulator requires clarification.

There are certain filings that need to be made to FINTRAC, which include[60]: Digital Currency MSBs are required to report every suspicious financial transaction and attempted suspicious financial transaction to FINTRAC. Crucially, there is no monetary threshold that triggers the requirement to report a suspicious transaction. A Digital Currency MSB must file a 'terrorist property report' with FINTRAC when it has property in its possession or

58 *Cryptocurrency Market Capitalizations*, COIN MARKET, (Nov. 05, 2017, 11:00 PM), https://coinmarketcap.com/all/views/all/.

59 The phrase *"dealing in virtual currencies"* was not defined and it is not known what the defined term will encompass in terms of transactions but the government has clarified that it will apply only to digital currency exchanges.

60 Christine Duhaime,*Canada implements world's first national digital currency law; regulates new financial technology transactions*, DUHAIME LAW, (Nov. 05, 2017, 11:00 PM), http://www.duhaimelaw.com/2014/06/22/canada-implements-worlds-first-national-bitcoin-law/.

control that it knows is owned or controlled by or on behalf of a terrorist or terrorist group; and when it has property in its possession or control that it has reason to believe is owned or controlled by or on behalf of a listed person. Digital Currency MSBs are subject to onerous record-keeping obligations under the PCMLTFA. Digital Currency MSBs are required to report to FINTRAC when they receive an amount of $10,000 or more in cash during a single transaction, unless the funds are received by a public body or a financial entity. When a Digital Currency MSB sends or receives an international money transfer of $100,000 or more, it must determine if it involves a politically exposed person (PEP) inside or outside of Canada. Further, if it determines that the funds involve a PEP, it must confirm the source of funds. Digital Currency MSBs are required to implement a compliance program to meet reporting, record keeping and client identification obligations under the PCMLTFA. Digital Currency MSBs must undertake a risk assessment to evaluate and identify, in the course of its activities, the risk of the commission of money laundering offences and terrorist activity financing offenses.

Failures to comply with certain obligations envisaged in the PCMLTFA are criminal offences and can make directors, officers, employees and the Digital Currency MSB liable to be on the receiving end of fines and even imprisonment terms. Digital Currency MSBs should obtain compliance advice with respect to their exposure and should understand the connection in Canada between the compliance regime and a due diligence defence.

In November 2013, Canada's Revenue Agency (CRA) confirmed rules that required users of Bitcoin to pay tax on transactions in the digital currency, based on two separate tax rules that are applicable to barter transactions and objects/products that are bought and sold for speculative purposes. It was clarified that the matter will be dealt with on a case by case basis. Barter transactions are allowed under Canadian law, but the CRA states that the value of goods or services obtained by bartering digital currencies must be included into the taxpayer's income if they are business related transactions.[61]

2. *United States of America*

The US Congress' Bill 'HR 5777' proposed a five-year moratorium on regulation of digital currency within the US. The Bill is titled 'The Crypto-currency Protocol Protection and Moratorium Act' and would hold off any 'statutory restrictions or regulations' for a period of five years after 15th June 2015.[62] Additionally, the draft law proposes that 'virtual currencies' be classified

61 *Is Bitcoin Legal?*COINDESK, (Nov. 05, 2017, 11:00 PM), http://www.coindesk.com/information/is-bitcoin-legal/.

62 Stan Higgins, *US Congressman to Submit Bitcoin Tax Bill*, COINDESK, (Nov. 05, 2017, 11:00 PM), http://www.coindesk.com/us-congressman-submit-Bitcoin-tax-bill/.

as 'traditional currencies' under the tax regulations of the country. The Internal Revenue Service (IRS) currently taxes Bitcoin holdings as though they were another form of property. However, the language of the moratorium bill implies that the IRS should be treating Bitcoin and distributed ledger systems as currencies rather than assets.[63] The bill criticizes the current taxation perspective, arguing that it fails to address the multifaceted characteristics of cryptocurrency. Should it receive the assent of Congress, the bill would require the IRS to revisit and rework its current regulations for digital currencies.[64]

According to the current standards of the IRS, treating Bitcoin as 'property' for taxation purposes means that:[65]

- Digital currency payments made to independent contractors and service providers must be reported via Form 1099.
- Profits and losses from the sale of digital currencies are subject to capital gains when being used as capital assets.
- Wages paid to employees in digital currencies are taxable and must be reported

For the IRS, only US bills and coins are legal tenders in the United States and thus, Bitcoin defaults to the status of an 'asset'. Despite its use as a currency, Bitcoin ironically continues to be taxed like property.[66] However, the District Court of Eastern District of Texas recently held[67] that Bitcoin is a form of currency and must be treated as money.[68] There are no rules at any level in the US, neither at the federal nor at the state level, and there is no infirmity when it comes to cryptocurrency.

63 Stan Higgins, *Proposed US Law Calls for Five- Year Moratorium on Bitcoin Regulation*, COINDESK, (Nov. 05, 2017, 11:00 PM), http://www.coindesk.com/proposed-us-moratorium-Bitcoin-regulation).

64 Pete Rizzo, *IRS to Tax Digital Currencies as Property, Not* Currency, COINDESK, (Nov. 05, 2017, 11:00 PM), http://www.coindesk.com/internal-revenue-service-treat-digital-currencies-property/.

65 Kirk Phillips, *Bitcoin Taxation: A Gift From the IRS & the Coffee* Problem, WALLSTREET & TECHNOLOGY, (Nov. 05, 2017, 11:00 PM), http://www.wallstreetandtech.com/compliance/Bitcoin-taxation-a-gift-from-the-irs-and-the-coffee-problem/a/d- id/1318419?_mc=RSS_WST_EDT

66 *In the Matter of Virtual Currency Exchanges*, PUBLIC ORDER, NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES, 5 November 2017.

67 VaneesaAbhishek, *Growing interest in Bitcoin: Time for India to welcome it as "currency,* ECONOMIC TIMES, (Nov. 05, 2017, 11:00 PM), http://articles.economictimes.indiatimes.com/2014-06-18/news/50678868_1_currency-notes-Bitcoin-satoshi nakamoto.

68 Andrew Trotman, *Bitcoin banned in Thailand*, TELEGRAPH UK, July, 13, 2013.

In March 2014, the New York State Department of Financial Services had officially invited Bitcoin exchanges to apply to them, and published draft regulations for virtual currency businesses. According to those, the businesses would have to provide receipts of transactions, undertake disclosures of risks, implement consumer complaint mechanisms, maintain a cyber-security program, hire a compliance officer, and verify details about their customers to effectively follow the anti-money- laundering rules, as per FinCEN.[69]

Another US bill, AB 129, was meant to repeal the law that renders any use of alternative currencies illegal. It was signed into a law in June 2014 and came into effect from 2015. Besides Bitcoin, the alternative currencies that now fall within the purview of the bill include gift cards, reward points, and virtual tokens.[70]

3. Australia

In August 2014, a draft ruling of Goods and Services Tax (GST), a guidance paper, and four tax determinations on the treatment of Bitcoin and other virtual currencies were issued.[71] From 1 July 2017, any sale or purchase of cryptocurrency is no longer subject to GST because of the changes in the GST law. Thus, the guidance paper that was issued is under review at present.[72]

4. China

In December 2013, China's central bank (People's Bank of China), along with four ministries and commissions, issued a Notice on Precautions against Risks of Bitcoin.[73] The notice stated that the nature of Bitcoin is of a 'virtual

69 John WeruMaina, *AB 129 – California Legally Approves the Use of Bitcoin*, CRYPTOCOINS NEWS, (Nov. 05, 2017, 11:00 PM), https://www.cryptocoinsnews.com/ab-129-california-legally-approves-use-bitcoin/.

70 Securities & Exchange Commission v. Trendon T. Shavers and Bitcoin Savings and Trust, US DISTRICT COURT, (Nov. 05, 2017, 11:00 PM), https://ia800904.us.archive.org/35/items/gov.uscourts.txed.146063/gov.uscourts.txed.146063.23.0.pdf.

71 *Tax treatment of crypto-currencies in Australia – specifically Bitcoin*, AUSTRALIAN GOVERNMENT, (Nov. 05, 2017, 11:00 PM), https://www.ato.gov.au/General/Gen/Tax-treatment of-crypto currencies-in-Australia---specifically-bitcoin/.

72 *Ibid.*

73 s()•N2-/Ôkyt^Î'i-„v•áw [Notice on Precautions Against the Risks of Bitcoin] (issued by the People's Bank of China, the Ministry of Industry and Information Technology, China Banking Regulatory Commission, China Securities Regulatory Commission, and China Insurance Regulatory Commission, Dec. 3, 2013) Yin Fa, 2013, No. 289, http://www.pbc.gov.cn/publish/goutongjiaoliu/524/2013/20131205153156832222251/20131205153156832222 251_.html (China). An unofficial English summary of the Notice is available at BTC CHINA, https://vip.btcchina. com/page/bocnotice2013.

commodity' and not a currency. Therefore, Bitcoin should not be traded as a currency in the market.[74] Furthermore, the notice also prohibited the Financial Institutions in China from trading in Bitcoin. The notice went on to mention that overseeing of internet sites that dealt in services relating to the Bitcoins was to be made more stringent. The notice included a general warning regarding money laundering through the use of Bitcoin.[75]

5. United Kingdom

The United Kingdom has outlined the way tax will be imposed on Bitcoins[76]. It has been indicated by the UK customs and tax department (HMRC) that Bitcoins will be considered 'single purpose vouchers'. This classification will render a levy of VAT extending up to 10-20% on the sale of Bitcoins. This development has been at the end of heavy criticism by those involved in the sale of Bitcoins, alleging that this would lead to a slowdown of massive proportions in the trade of Bitcoins for those in the UK.

6. European Union

Insofar as the status of Bitcoin as a currency is concerned, no legislation has been passed by the European Union yet.

The European Central Bank published detailed report on virtual currency, which also discussed the Bitcoin system and briefly analysed its legal status within the EU.[77] However, in the conclusion of the report, the Bitcoin was kept outside the purview of directive 2007/64/EC since the directive does not deal with electronic money and the financial institutions are not allowed to deal in it either.[78] In December 2013, European Banking Authority (EBA), EU's regulatory and advisory agency in matters of banking institutions, e-money regulation etc. issued a warning about the dangers of using virtual currency, and stated that the consumers might still be taxed when using virtual

74 *Ibid.*

75 *Ibid.*

76 *Revenue and Customs Brief 9 (2014): Bitcoin and other cryptocurrencies*, GOV.UK, (Nov. 05, 2017, 11:00 PM), https://www.gov.uk/government/publications/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies.

77 European Parliament and of the Council Nov. 13, 2007, *Payment Services in the Internal Market*, Amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and Repealing Directive 97/5/EC, 2007 O.J. (L. 319).

78 Press Release, European Banking Authority, EBA Warns Consumers on Virtual Currencies (Dec. 13, 2013), http://www.eba.europa.eu/-/eba-warns-consumers- on-virtual-currencies.

currency as Bitcoin is not regulated in the European Union and is not the subject of any specific legislation.[79]

7. Germany

BaFin (*Bundesanstalt für Finanzdienstleistungsaufsicht*), the German Federal Financial Supervisory Authority issued a communication on Bitcoin on December 19, 2013.[80] In Germany Bitcoin have been classified as a financial instrument but not any form of currency.[81] The Federal Ministry of Finance discussed briefly the tax treatment of Bitcoin in some statement. The ministry, among other things, discussed the possibility of levying value-added tax liability for Bitcoin transfers, lack of long term capital gains liability for Bitcoin that are held for more than a year.[82]

Position in India

At present, there is no law regulating cryptocurrency in India. Although, RBI has issued a press release cautioning users, holders and traders of virtual currencies, including Bitcoin, about the potential financial, operational, legal, security related risks that they are exposing themselves to.[83]

If cryptocurrency is treated as a currency then the Central Government will be allowed to legislate according to Entry 36 and 46 of List 1 of the Seventh Schedule of the Constitution.

The possible laws that could govern cryptocurrency are:

1. The Constitution of India, 1950
2. The Foreign Exchange Management Act, 1999

79 Jens Münzer, *Bitcoin: AufsichtlicheBewertung und RisikenfürNutzer (Bitcoin: Supervisory Evaluation and Risks for Users)*, BAFIN, (Nov. 05, 2017, 11:00 PM), http://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/ 2014/fa_bj_1401_Bitcoin.html.

80 Kreditwesengesetz (BANKING ACT), Bundesgesetzblatt I at 2776, (Nov. 05, 2017, 11:00 PM), http://www.gesetze-im-internet.de/kredwg/ index.html (Ger.).

81 Franz Nestler, *Deutschland erkenntBitcoinals privates Geld an (Germany Recognizes Bitcoin as Private Money)*, FRANKFURTER ALLGEMEINE ZEITUNG , (Nov. 05, 2017, 11:00 PM), http://www.faz.net/aktuell/finanzen/devisen-rohstoffe/digitale-wachrung-deutschland-erkennt-Bitcoiu-als-privates-geld-an-12535059.html.

82 Charles Arthur ,*Bitcoin now 'unit of account' in Germany*,THE GUARDIAN, (Nov. 05, 2017, 11:00 PM), https://www.theguardian.com/technology/2013/aug/19/bitcoin-unit of account-germany

83 Press Release 2016-17/2054, *RBI Cautions users of virtual Currencies*, RBI, (Nov. 05, 2017, 11:00 PM), https://rbi.org.in/scripts/bs_pressreleasedisplay.aspx?prid=39435, Press Release : 2013 2014/1261, *RBI cautions users of Virtual Currencies against Risks*, RBI, (Nov. 05, 2017, 11:00 PM), https://rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=30247 .

3. The Reserve Bank of India Act, 1934
4. The Coinage Act, 1906
5. The Sale of Goods Act, 1930
6. The Goods and Service Tax Act, 2016
7. The Indian Coutract Act, 1872
8. The Income Tax Act, 1961

Cryptocurrency as a Currency

The three statutes - The Foreign Exchange Management Act, 1999[84], The Reserve Bank of India Act, 1934[85] and The Coinage Act, 1906 together define and regulate the issuance, utilisation and disposal of currencies.

The FEMA defines 'currency' as to include, *'all currency notes, postal notes, postal orders, money orders, cheques, drafts, travellers cheques, letters of credit, bills of exchange and promissory notes, credit cards or such other similar instruments, as may be notified by the Reserve Bank'.*[86] The question now is can 'virtual currency' or 'cryptocurrency' come under the purview of this definition. Keeping in mind that 'other similar instruments' have to be specifically notified by the Reserve Bank of India, cryptocurrencies cannot be considered as 'curreney' under the Indian regime.

Cryptocurrency as a Good

The term 'goods' has been defined in the Sale of Goods Act as *'every kind of movable property other than actionable claims and money; and includes stock and shares, growing crops, grass, and things attached to or forming part of the land which are agreed to be severed before sale or under the contract of sale.'*[87]

Cryptocurrencies maybe considered as a good since they are listed and traded on stock exchanges around the world but there is no specific formal recognition in India for cryptocurrencies. Moreover, if cryptocurrencies are recognised as goods under the Indian law, there will be tax implications on the same.

If cryptocurrency is dealt in a manner similar to gold, then the holders of cryptocurrency will need to pay 3% Goods and Service Tax[88] on the same, apart from the capital gains tax as mentioned under the Income Tax Act, 1961.

84 Hereinafter referred to as FEMA for brevity.

85 Hereinafter referred to as RBI Act for brevity.

86 Section 2(h) of The Foreign Exchange Management Act, 1999.

87 Section 2 of The Sale of Goods Act, 1930.

88 *GST impact on gold jewellery: Larger players to emerge ast biggest beneficiaries,* THE ECONOMIC TIMES, (Nov. 05, 2017, 11:00 PM), https://economictimes.indiatimes.com/industry/cons-products/fashion-/-cosmetics-/-jewellery/gst-impact-on-gold-jewellery-larger-players-to-emerge-as-biggest-beneficiaries/articleshow/59376739.cms.

Cryptocurrency and Contracts

The essentials of a contract are; competency of parties, lawful consideration and object and free consent. At best, the cryptocurrencies can be considered as lawful consideration or lawful object. According to Section 23 of the Indian Contract Act, certain considerations are unlawful in nature and cryptocurrencies do not fall under it. Since, cryptocurrencies cannot be considered as currency as seen above they can only be considered as goods, hence, they can be regarded as consideration under the Indian Contract Act and not as consideration under the Sale of Goods Act.

Cryptocurrency and Intellectual property

The advent of technology coupled with the advancements in digital space, the concept of intellectual rights has now become dynamic. Big businesses are out there to protect their intellectual assets at any cost in every jurisdiction. At present, MtGox, the world's most prominent Bitcoin exchanged based in Tokyo holds the trademark for Bitcoin.[89] The question is can the same be registered as a trademark in India? According to the Trade Marks Act, 1999, any mark which is capable of being represented graphically and which is capable of distinguishing the goods or services of one person from those of others can be accorded trademark protection.[90] Thus, Bitcoin maybe covered under the trademark law of India. However, today the term 'Bitcoin' is used interchangeably with cryptocurrency thus, it may be difficult for the people to mark the uniqueness of 'Bitcoin'.

Cryptocurrency and Privacy

At present, in India, the right to privacy is considered as a fundamental right post the decision of the Supreme Court in the case of *Justice K S Puttaswamy (Retd) v. Union of India*[91]. Thus, a citizen may enforce this right against the State but not against any private individual. The concept of cryptocurrencies is based on a decentralised network, hence pin pointing one person for instituting a case will be next to impossible. Therefore, it is suggested that there be a data protection law in place which will not only protect the blockchain technology but also the private information of the users of the same.

89 *Mt. Gox to Sell Bitcoin Trademark, But Could a Buyer Enforce It?*, COINDESK, (Nov. 05, 2017, 11:00 PM) http://www.coindesk.com/mt-gox-sell-bitcoin-trademark-buycreenforce/.

90 Section 2 (m) of the Trade Marks Act, 1999 defines mark to include a "device, brand, heading, label, ticket, name, signature, word, letter, numeral, shape of goods, packaging or combination of colours or any combination thereof."

91 Writ Petition (Civil) No. 494 Of 2012 decided on 24 August 2017.

Risks associated with Cryptocurrencies

Cryptocurrencies have numerous advantages associated with it. Some of them include cost effective way of storing, spending and receiving digital money, radically lowering the cost of retail payment as well as cross border transactions. Although, there are advantages but there are numerous issues related with cryptocurrency.

Some of the risks associated with cryptocurrency include; firstly, the volatility in the price of the cryptocurrency. Recently, when the Chinese exchange BTCC announced that it will stop offering trading services, the price of the Bitcoin went down by $500 in one day.[92] This clearly reflects on how volatile the price of the Bitcoin really is. At present, there is more cause for concern, since most of the countries are not sure of how they are going to regulate the cryptocurrency as is evident from the above discussion, thus, each and every announcement of any country relating to cryptocurrencies or blockchain technology has a great impact on the price of the cryptocurrencies.

Secondly, cyber-attack is another issue that makes the users of cryptocurrencies at a high risk of losing money. There have been numerous cases of cyber-attacks on Bitcoin wallets. The most highlighted case is that of Mt. Gox, a Bitcoin exchange, where $400 million were stolen from the system. The high-end security of the system was breached and people lost their money. Moreover, since there were and are no regulations in place for such a happening, the possibility of recovering the stolen money is next to impossible.[93]

Thirdly, cryptocurrencies open the gates for laundering money as there is no centralised authority keeping a watch on how this money is being transacted or used by individuals. The famous example of the Silk Road, which was a popular website for buying narcotics anonymously was taken down by the Federal Bureau of Investigation (FBI) when the FBI arrested the administrator of the same. Bitcoins were being used for the purchase of drugs.[94]Thus, the issues of money laundering and drug trafficking also need to be looked into while regulating cryptocurrencies.

Fourthly, every bitcoin transaction is not entirely anonymous. Since very entry on the blockchain is publicly shared and stored forever, people who intend to defraud or who have mala fide intentions will be able to link one transaction of a particular person with another and slowly and steadily even connect the public key with one's computer IP address. Thus, this highly motivated person with mala fide intentions

92 Stan Higgins, *Bitcoin's Price is Down More Than $500 Today*, COINDESK, (Nov. 05, 2017, 11:00 PM), https://www.coindesk.com/bitcoins-price-fallen-500-today/.

93 Russell Brandom, *Who Stole $400 Million from Mt. Gox*, THE VERGE, (Nov. 05, 2017, 11:00 PM), https://www.theverge.com/2014/2/26/5450206/who stole-400-million-from-mt-gox.

94 Andy Greenberg, *End of the Silk Road: FBI Says It's Busted The Web's Biggest Anonymous Drug Black Market*, FORBES, (Nov. 05, 2017, 11:00 PM), https://www.forbes.com/sites/andygreenberg/2013/10/02/end-of-the-silk-road-fbi-busts-the webs-biggest-anonymous-drug-black-market/#10213445b4f9.

will then be aware of how much money you have stored in the Bitcoin and where you live amongst other things.[95]

Fifthly, no computer in this world is immune from hacking. A highly motivated person if interested in your details, may just hack your computer or phone and get access to your private key which will in turn give him/her complete access to all your funds stored as virtual currency. Moreover, if one has linked their bank account with their digital wallet, they might also be at a risk of losing their money from their bank account and their identities. Today, with the linking of Aadhar with one's bank account, one's personal details – place of birth, place of residence and many more will also reach in the hands of the hacker, thereby putting an innocent user at the risk of identity theft.

Sixthly, there are no regulations in place for cryptocurrency. thus, making it the best way of investing and avoiding taxes.

Seventhly, keeping in mind the advent of technology and the effect of the Blue Whale game, chances of someone blackmailing you over the internet for your private key are also very high. Thus, not only are you prone to blackmailing and identity theft, you might also be asked to do illegal activities.

CONCLUSION

Cryptocurrency, most notably identified in its iteration of Bitcoin, is gaining popularity globally at a very rapid pace. Despite the attention it has received from business, customers, and entrepreneurs, the amount of attention cryptocurrencies has received from governments is distual. Very few countries in the world recognise cryptocurrencies, or an iteration of cryptocurrencies (such as Bitcoin or Ethereum) as a commodity, much less a currency. While a few countries have made progress, legal recognition of cryptocurrencies or even the technology that drives them – the blockchain – is lacking. This means that the potential security concerns that the technology raises as well as the potential positive uses it may be put to are largely disregarded. This is indubitably problematic, and policymakers need to direct their attention to the idea of virtual currencies in the form of the newly emerging cryptocurrencies. It is a matter of fact that laws are unable to keep pace with technological developments, and the speed with which advancements are made is incredibly high and this makes it tough for legislators and advisors. Coupled with the wary approach of law-makers approach instances of technology and the vast amounts of input required to put into place a well thought out policy, it is no wonder that governments have failed to clarify the position of cryptocurrencies.

Despite the scepticism and irrespective of the speculation regarding the eventual position of cryptocurrencies and their viability in the long run, it is irrefutable that cryptocurrencies need a regulatory framework in every country.

95 Consumer Advisory, *Risks to consumers posed by virtual currencies*, CONSUMER FINANCIAL PROTECTION BUREAU (Nov. 05, 2017, 11:00 PM), http://files.consumerfinance.gov/f/201408_cfpb_consumer-advisory_virtual-currencies.pdf.

DEMONETIZATION : A PUSH TOWARDS E-GOVERNANCE

Mahima Ahuja* and Archit Aggarwal**

Introduction

Demonetization is the act of stripping the status of a country's currency as its legal tender. According to the Black's Law Dictionary, demonetization is "The disuse of a particular metal for purposes of coinage: the withdrawal of the value of a metal as money."[96] Interpreting this definition it can be accordingly said that the disuse of a particular Currency which was being used as a country's legal tender and replacing the same with the other is known as demonetization. Money, "in usual and ordinary acceptation, means gold, silver, or paper money used as circulating medium of exchange"[97] and Currency is "Coined money and such banknotes or other paper money as are authorized by law and do in fact circulate from hand to hand as the medium of exchange."[98].

Demonetization is the process in which a current form of currency is pulled out of circulation from the country's economy and reduced with a new form of currency notes and coins. Demonetization in any country can take place by the order of the government of that particular nation as it had taken place in India. In India, Demonetization had taken place thrice and twice in India post-independance in the years 1978 and 2016 respectively and was done keeping in mind the various objectives and goals of the Government of India. On November 8th 2016 the Prime Minister of India Mr. Narendra Modi announced demonetization which derecognized the two denominations of the Indian currency, i.e. Rs 500 and Rs 1000 paper currency notes and introduced new Rs 500 and Rs.2000 paper currency notes. Demonetization in India was done various motives but majorly it was to curb the nation's black wealth and to reduce the nation's share in the black market operations. The demonetization had impacted the population to the core whether it was a resident of the country or a tourist in the country- Difficulties

* 3rd year, BBA LLB, College of Legal Studies, University of Petroleum and Energy Studies
** 3rd year, BBA LLB, College of Legal Studies, University of Petroleum and Energy Studies

96 Henry Campbell Black, BLACK'S LAW DICTIONARY (4), 519
97 Henry Campbell Black, BLACK'S LAW DICTIONARY (4), 1157
98 Henry Campbell Black, BLACK'S LAW DICTIONARY (4), 458

were faced by all. Therefore, to reduce the impact of a sudden decision of the government which resulted in commercial collapse, a 50-day period ensued where the people could exchange their demonetization legal tender money for the new legal tender money it into their or otherwise deposit it into their respective bank accounts.

The then President of India, Mr. Pranab Mukherjee in his speech on the occasion of nation's 68th Republic Day i.e. on 26th day of January, 2017 also mentioned the Demonetization drive by the government of India. He said that "Demonetization, while immobilizing black money and fighting corruption, may have led to a temporary slowdown in economic activity. As more and more transactions become cashless, it will improve the transparency of the economy."[99] These thoughts can be seen as positive words for demonetization and encouraging the people of the country to take demonetization drive as a positive initiative taken by the government of India and promoting the cashless economy and country's digitalization drive.

E-Governance is an initiative of the government for providing its services and Information through the Electronic medium (information and communication technology) i.e. through the way of Digitalization of the government departments. For a developing nation like India, the step to implement E-Governance at all the levels of the government and also to popularise this system among the public is very important for the country's growth. E-Governance has various parts which include E-Government, E-Industry, E-Innovation/R&D, E-Learning, E-Security, E-Inclusion and Internet Governance. Now, these are the parts which collectively form the concept of the E-Governance. The aspect of E-Industry covers the promotion of electronic hardware manufacturing and software development and Information & Technology-Information & Technology Enterprises industry in the country while the aspect of E-Innovation/R&D covers the Implementation of R&D Framework - Enabling creation of Innovation/ R&D Infrastructure in emerging areas of ICT (Information Communication and Technology) & Establishment of a mechanism for R&D translation. E-Learning provides for the development of e-skills and knowledge networks. E-Security covers the area where the government works to secure India's cyberspace. E-Inclusion promotes the use of information communication technologies for more inclusive growth.

Internet Governance enhances India's role in Global Platforms of Internet Governance. Going by the mission of Ministry of Electronics and Information

99 President's address on the eve of Republic Day 2017, The Hindu, (Jan. 27, 2017 11:23 a.m.), http://www.thehindu.com/news/resources/Presidents-address-on-the-eve-of-Republic-Day-2017/article17101716.ece

Technology (Government of India) whose is to "promote E-Governance for empowering citizens, promoting the inclusive and sustainable growth of the Electronics, IT &ITeS industries, enhancing India's role in Internet Governance, adopting a multipronged approach that includes development of human resources, promoting R&D and innovation, enhancing efficiency through digital services and ensuring a secure cyberspace."[100] This further explains the Idea of E-Governance in the country and the objective of the Indian government towards the implementation of E-Governance at all the levels of the government.

For a country to reach the position where the government is providing and offering the information and services of the government to its people through E-Governance is a stage which has to be reached by climbing through the stepping stones that lead to the fulfilment of the final objective. These stepping stones can be rules, procedures, laws, guidelines and many steps taken by the government of India for the fulfilment of the objective of E-Governance and it refines the government processes through technology. For example, The forms through which the information is collected are simplified and made available online so that the government service can reach the maximum number of people. Further, these forms when submitted online or offline are given with the tracking number which can be used to track the progress and correct status.

For E-Governance, all information and databases should be in electronic form and not manual. The workflow inside government departments and agencies should be automated to enable efficient government processes and also to allow visibility of these processes to citizens. IT should be used to annomate, respond and analyse data to identify and resolve persistent problems.

Relationship of E-Governance and Demonetization

Demonetization and E-Governance are two absolutely different concepts. They may be interdependent and it could be deduced that they are essential for the others success and thus both the concepts have inter-related elements. The first is related to the derecognizing of a country's currency as the legal tender and the latter is related to the government providing its services and governing the country using information and technology. The E-Governance is continuous in nature whereas demonetization was a one time thing. The Indian Government through various projects and schemes is trying to bring E-Governance in the country whereas in

100 Mission of MEITY,The Ministry of Electronics and Information TechnologyGovernment of India, (Oct. 10, 2017), http://meity.gov.in/about meity/vision mission

case of demonetization the government through its legal mechanism can derecognize the nation's currency as a legal tender.

Demonetization is a push towards E-Governance. The basic idea to support this statement can be made clearly observing the country's situation after the night when Demonetization was announced by the Prime Minister of India, Mr. Narendra Modi on 8th November 2016. The effects of the demonetization were observed on a macro scale as the money held by the people in the form of Rs. 500 and Rs. 1000 paper notes was derecognised and they were told to deposit their money in their bank accounts. Further, old notes were allowed to be exchanged through the banks providing new notes issued by the RBI (Reserve Bank of India) but it too had a cap of Rs. 24000 per week which was increased to Rs. 50000 per week. The problems started when most of the ATMs were not calibrated according to the new system and people did not have money for their day to day activities. The queues outside the banks were increasing day by day as the banks were not able to give new currency to the public. Then the government, in order to have a better handle on the situation started developing and promoting its digital services and other digital platforms which could be used to make the day to day activities simple. The government announced various schemes and projects to push E-governance to a new level be it the digital platforms to make payments and funds transfer, to the promotion facility like E-Stamping where non-judicial e-stamps can be purchased online through the government websites.

The Government has made the filling up of various forms more easy and the process for the same has been made available online so that the people can avail the online services. For example, earlier for applying for an Indian Passport the people had to go to the passport office and purchase a form which had to be filled and submitted as hard copy/ physical copy along with the copy of the documents which are needed for verification in the hard copy too. But now the process has changed, the form for the passport can be filled online and by paying the necessary fees which had to be paid digitally, the form can be submitted easily and the documents needed for the verification are also submitted in the form of soft copy/ scanned copy of the original document which has made the process applying for an Indian passport easier.

Post demouetization, the government started to give a push to the digital modes of the payments and funds transfer. It started taking steps to make the people of the

nation aware of the advantages of the digital modes of the payments. The government encouraged various modes like Internet Banking, Mobile Banking, Various banking apps, third-party payment websites, payments through credit cards and debit cards and provided various discounts to the users if they make payments online. Even the taxes were waived by the government which were levied before on the consumers who made payments through the digital modes of the payments. The government tried to bring the previous mission i.e. Final Inclusion mission into the picture in the support of Demonetization. Various E-Commerce websites like Amazon, Flipkart, Snapdeal, Oyo, Ola etc. have applauded the move of demonetization stating that the consumers are now using the digital modes of making payments and thus making the process simpler and faster. Companies like Paytm and Freecharge saw a sudden increase in the number Users of E-wallets to make the payments in their day to day lives after the demonetization.

The Government also launched 'BHIM', which is a Unified Payments Interface application developed by the National Payments Corporation of India (NPCI). NPCI is an umbrella organisation for operating retail payments and setdement systems in India. It is an initiative of Reserve Bank of India (RBI) and Indian Banks' Association (IBA) under the provisions of the Payment and Settlement Systems Act, 2007, for creating a robust Payment and Settlement Infrastructure in India.[101] A Unified Payments Interface (UPI) is an instant real-time system developed by NCPI facilitating transactions between the banks. The interface is regulated by the Reserve Bank of India and works on the platform of IMPS i.e. Immediate Payment Service by instantly transferring funds between two bank accounts on a digital platform.

Demonetization also affected the role of e-governance in the Income tax department of the country. For a person to file an income tax return, he needs a Permanent Account Number(PAN). There are two ways in applying for PAN: one is an old method which is a physical method and the other is the online method which is faster and more convenient. The services like TDS (Tax deducted at source), Filing of Income Tax Returns (E-Returns), Making tax payments, and checking the status of the refunds were already online[102], but due to demonetization it was observed that the people started using these online services more. The e-filing of returns for the fiscal year 2016-2017 may have faced some technical glitches, therefore, the deadline for filing the returns was extended to 5th August 2017 which was earlier

101 Who we are, BHIMUPI, visited 01-11-2017 02:24 p.m., https://bhimupi.org.in/who-we-are.

102 E-Governance initiatives, Income Tax Department Government of India, Last updated 04-09-2014, visited 01-11-2017 03:00 p.m., https://www.incometaxindia.gov.in/Pages/e-governance-initiatives.aspx.

31st July, 2017.[103] The technical glitch was making the nation question the government's initiative for digitalizing India but the extension of the deadline can be viewed as an initiative by the government to promote the E-governance in the income tax department.

The effect of demonetization can be seen in various operations of public sector Undertakings. Taking the example of railways, the government encouraged the people to book tickets online through the railways website (IRCTC) and offered incentives in the form of reduction of taxes on booking of e-tickets. Also, the government installed swipe machines at the railway booking counters so that the travellers can use their cards to make the payments for their railway bookings as this option was not earlier available to the public before Demonetization. Further, all railway passengers who bought an online ticket were given free accidental insurance cover of upto Rs 10 lakh.

After Demonetization, the electronic transfers with regard to E-Governance has increased significantly. The transactions such as commercial taxes, utility payments, and E-courts have shot up. (People now prefer to transact through the digital modes of payment than cash). On the basis data avaible for some stats from a leading newspaper, the initial days after demonetization, Gujarat has registered 3.58 crore digital transactions, followed by Telangana and Andhra Pradesh where 2.06 crore and 2.02 crore such payments have been made.[104]

Advantages and Disadvantages of Demonetization

David Suzuki said "Humans are distinguished from other species by a massive brain that enables us to imagine a future and influence it by what we do in the present. By using experience, knowledge, and insight, our ancestors recognized they could anticipate dangers and opportunities and take steps to exploit advantages and avoid hazards,"[104]. This is the basic phenomenon on which decisions are taken and how they are later analysed. The step of Demonetization was one of them.

The main motive of the NDA government for pursuing demonetization was to eradicate corruption, black money and put a stop to the counterfeiting of currency and terror funding. But this is something that was aimed at. Now the question that

103 SamikshaPatnaik, Snag hits income tax e-filing website-Twitterati questions Modi's Digital India, Hindustan Times, (Oct. 30. 2017 5:00 p.m.), http://www.hindustantimes.com/india-news/snag-hits-website-on-last-day-of-filing-tax-returns-twitter questions-modi-s-digital-india/story-OI44P3nMaBh4fUK7ZEgqKP.html

104 Surabhi,Electronic transactions see sharp rise in 2016, The Hindu (Business Line), (Nov, 02, 2016), http://www.thehindubusinessline.com/economy/electronic-transactions-see-sharp-rise-in-2016/article9411940.ece

has arisen before us whether the aims have been fulfilled or not? Let's start with the positives aspects: the amount of fake currency that was being circulated has been controlled as the number of fake notes that were being circulated and used in a number of illegal activities have the same value as a piece of paper now.

Secondly, there has been a control in the rate of inflation[105] as the scarcity in the amount of currency led to a decrease in demand, which led to fall in prices leading to a positive impact on the economy.[106]

Thirdly, the step of demonetization helped in recovery of tax and disclosure of black money to a large extent as all notes of higher denomination of 500 and 1000 had to be deposited and brought under the radar due to which there has been a increase of 17.3 per cent in the percentage of filing of tax returns in the year of 2016-2017 when compared to the previous year.[107]

Fourthly, the deposit of the bank notes led to high liquidity stock for the bank, leading to a decrease in the rate of interest as the lending capacity of the banks had increased[108].

Fifthly, the combination of low inflation and a low lending rate of interest makes a good combination for the Gross Domestic Product of the nation but this is not something that the International Monetary Fund agrees upon. Electronic payment has been promoted by the government rather than use of cash through different online mechanisms such as PayU India.

Other advantages of Demonetization include eradication of the funds that are hidden from the government in an attempt to evade their liability to pay tax i.e. black money. Over two lakh of shell companies have been shut down as they were treated as a mechanism to launder money. Lastly, several accounts have been opened under the Jan Dhan Yojna Scheme leading to creation of safe savings for the major chunk of the population[109].

105 Demonetisation: The Nielsen View, Insight (November 15, 2016) http://www.nielsen.com/in/en/insights/reports/2016/demonetisation-the-nielsen-view.html.

106 Reserve Bank of India, Inflation, Macro Impact of Demonetisation (March 10th, 2017) https://rbi.org.in/scripts/PublicationsView.aspx?Id=17447.

107 Cash deposits of ₹ 2.89 lakh crore post demonetisation under I-T dept. radar, The Hindu (August 31, 2017 17:09) http://www.thehindu.com/business/cash-deposits-of-rs-289-lakh-crore-post-demonetisation-under-i-t-dept-radar/article19594442.ece.

108 Reserve Bank of India, Financial Sector, Macro Impact of Demonetisation (March 10th, 2017) https://rbi.org.in/scripts/PublicationsView.aspx?Id=17447.

109 One year of demonetisation: Five positive impacts on economy, Times now, (October 26, 2017 14:59) http://www.timesnownews.com/business-economy/article/latest-news-one-year-of-demonetisation-five-positive-impacts-on-economy/113360.

The NDA government received its share of criticism from the opposition as well as from the minority share of the population for the step of demonetization and some of that criticism is valid on the grounds that firstly, the scarcity of the currency not only lead to chaos and panic within the country but also lead to decline in demand and disruption in the economy as majority of the transactions were being done by cash in the developing country of India. The sudden limitation lead to the population high and dry and not only that organized manufacturing sector of the economy had to lay people off leading to unemployment as the lack of demand was leading them to incur loss.[110]

Secondly, the lack of currency with increasing level of unemployment with low demand leads to fall in GDP of the nation and similar has been predicted by the IMF.

Thirdly, the black money did enter the system through fraudulent ways, as the expected amount of currency was not received by the government. A general fact to be pointed out is that any individual with high amount of black money would not like to keep his currency in cash rather would keep it in the form of certain investments like gold or deposit the amount in swiss banks as they have been a popular medium in the past.

Fourthly, the disruption of trade was especially for the rural population and the illiterate part of the population as the paper currency has been limited by the government and the digital currency was not something that they were comfortable with and had easy access to and even in the metropolitan cities disruption of trade had taken place.

Fifthly, the amount of money, which has been received by the RBI, is still under survey, is less than the amount that has been spent on the printing of new notes and the whole process of demonetization leading to a net loss for the RBI[111]. And a special mention has to been given to the individuals who lost their lives while standing in the lines for depositing their hard earned money and withdrawing their money so that they could live their lives on a day to day basis. Also, no special consideration was given to anyone who might had a wedding or a medical emergency and one thing that the NDA government should have considered in that the rural population and the population which is below poverty line would have no

110 Reserve Bank of India, Growth, Macro Impact of Demonetisation (March 10th, 2017) https://rbi.org.in/scripts/PublicationsView.aspx?Id=17447.

111 Demonetisation hits RBI's profit margins: SBI Research, The Hindu (AUGUST 31, 201714:42) http://www.thehindu.com/business/Economy/demonetisation-hits-rbis-profit-margins-sbi-research/article19593426.ece.

access to digital payment as most of the transactions are either through cash or on the basis of their daily wages leading to discomfort for the aam aadmi[112].

Advantages And Disadvantages of E-Governance

As it has been explained above how e-governance has evolved in India, now we can analyze how has its implementation been for the country. The positive aspect is that it has been a step towards democratization as e-governance acts as a platform between the government and its people which leads to flow of information for both the government as they receive the views of the people and their reactions to different scenarios giving them an edge for their future prospects and how the people want the future of this country to be and the people receive information in regard to different schemes of the government and how they are being implemented.

Secondly, the shift of the governance in an electronic form leads to an environmental bonus, as there is a decrease in usage of paper, which is not only environmentally friendly but cost effective as well.

Thirdly, e-governance leads to speedy, efficient and convenient governance as it not only eliminates the middleman and the corrupt methods but also saves time on travel and the information is easily accessible and available for all rather than selective.

Fourthly, E-governance is a great push towards public approval as it lets the public be aware of the system and appreciate it well.[113]

Fifthly, the system of e-governance leads to transparency within the country as every piece of information which is relevant for the public will be available online leading to a safe feeling and a development of trust within the public[114].

The negatives are that the new relationship between government and its people is electronic in form and once it starts developing there will be exchange of communication and surveillance, which could lead to loss of privacy for the general population.

112 Tom Worstall, India's Demonetisation Kills 100 People Apparently - This Is Not An Important Number, The Forbes (December 6th, 2016 4:47 pm) https://www.forbes.com/sites/timworstall/2016/12/08/indias-demonetisation-kills-100-people-apparently-this-is-not-an-important-number/#5a9e7960237a.

113 P. K. Doraiswamy, Has e-governance made citizens happier?, The Hindu (DECEMBER 13, 2009 01:35) HTTP://WWW.THEHINDU.COM/OPINION/OPEN-PAGE/HAS-E-GOVERNANCE-MADE-CITIZENS-HAPPIER/ARTICLE16853021.ECE.

114 Aloysius Xavier Lopez, More transparency in e-governance likely, The Hindu (JUNE 06, 2013)HTTP://WWW.THEHINDU.COM/NEWS/CITIES/CHENNAI/MORE-TRANSPARENCY-IN-EGOVERNANCE-LIKELY/ARTICLE3735401.ECE.

Secondly, an enormous amount has been spent on the development of online portals which have been placed to slowly but efficiently replace the corrupt system but the problem present is that India hasn't developed to that extent in the area of cybersecurity and data protection laws leading its major step towards e-governance to be a vulnerable ground or an open wound.

Thirdly, the rural, the elderly and the individuals in our country who are below the poverty line as they are not even able to make ends meet would not be able to access the online portals due to certain factors like lack of financial support, illiteracy and the fact that they need face to face assurance that there work is being done[115].

Fourthly, it has been stated in the earlier point that e-governance is not for all but it also needs to be established that since the system is new and there are no such particular guidelines being provided it can lead to creation of corrupt practices through middlemen and there could be lack of transparency and accountability as the government would only upload the information on its portal online that it wants the public to access leading to lack of quality in public access.

Critical Analysis Between Demonetisation & E-Governance

8th November, 2016, was the day on which demonetization was announced and at first, it was a move towards eradication of black money but later, another objective was highlighted and promoted by the NDA government, a cashless society. Rome wasn't built in a day and similarly an economy in which 98 per cent[116] of the transactions took place through cash cannot just overnight become a cashless economy. Demonetization cannot be the only step towards a cashless economy or a corrupt system through E-governance, but it is the people of the country who have to adapt and accept different mediums and shapes through which payments can be made. From the moment demonetization was announced till midnight, which eighty six percent of the currency in our country ceased to exist, which lead to the promotion of e-governance through the trinity of Jan Dhan, Aadhar, Mobile, Rupay Card and the Unified Payment Interface by the government[117]. The NDA government had formed the National Payments Corporation of India in regard to the unified payment interface where promotion of usage of debit cards,

115 KR SRIVATS, Demonetisation: A baby step to a 'less-cash' economy, The Hindu: Business Line (December 23, 2016) http://www.thehindubusinessline.com/specials/demonetisation-a-baby-step-to-a-lesscash-economy/article9442316.ece.

116 Impact of Demonetisation on E-Commerce, Deccan Chronicles (Mar 3, 2017, 12:41 am) http://www.deccanchronicle.com/business/economy/030317/impact-of-demonetisation-on-e-commerce.html.

117 Raja Gopal R v. State of Tamil Nadu, (1994) 6 SCC 632, 649 : AIR 1995 SC 264

credit cards and other online portals for payment was being and a committee had been formed to look into the matter. Another promotional scheme by the NDA government was the Unique Identification Authority of India which is in regard to the Aadhar card and how payments can also be made through our cell phones using our Aadhar card in just moments, whereas the National Payment Corporation of India is just a direct transfer of amount between two accounts.

Payments could also have been made through other digital platforms such as PayU India and Paytm as earlier these platforms were mainly used for activities like mobile recharges and paying of utility bills but now they are being used for payment for food in restaurants and even payment for purchase of garments, raw vegetables and electronics, and other online portals such as zomato and swiggy are examples of hyped local delivery. The evolution of our economy can be observed. The NITI Aayog report had reported that after demonetization there has been a 217 per cent increase in the usage of online portals for payment and all of the above-stated points indicate that we might not be a cashless economy yet but we are a step closer. The Government has made an attempt to promote the digitization movement by giving directives to the banks that at least one million new PoS machines should be added, and that RBI has been giving guidelines which promote small-scale organizations in the promotion of the movement but some of those organizations are non-banking financial institutions which are not under the ambit of the RBI. It is to be pointed out that people prefer convenience and cash is convenient whereas online transactions through e-governance are time-consuming and create hindrances in regard to network issues, transaction charges, illiteracy. In India, under certain circumstances the individuals prefer cash transactions as they are easier to cover up and every citizen would like its own privacy and would not like its mobile numbers and bank accounts details to be connected to a card and make this information easily accessible to the government, every citizen has its right to privacy[118]. Companies such as snapdeal, flipkart and amazon welcomed demonetisation with open hands as for them it meant cashing their profits in the future. Another point which should be pointed out is that digital transactions should go hand in hand with cash transactions and both of this mechanism should be parallel to one another and shall be treated as a substitute for one another. Also instead of a cashless economy we should go for an economy with less cash and say that the step of demonetization or e-governance was rash and immediate is wrong, because the government on various occasions ask the citizens to pay their taxes,

118 99 per cent of demonetised notes returned, says RBI report, *ManojitSaha,* The Hindu (Nov, 2, 2017), http://www.thehindu.com/business/Economy/only-12-of-demonetised-1000-notes-did-not-return-rbi/article19590311.ece

disclose their illegal income and request requested to open their account under the Jan Dhan Yojna Scheme. Hence, these two steps might not have been rash and immediate but their implementation had been poor as the general population had to suffer to a great extent whether it was physical, mental or emotional.

Conclusion

Prime Minister Modi in his reign has successfully portrayed himself as a leader willing to take difficult decisions and not given a moments thought to what the opposition is referring to. As we are near the first anniversary of demonetisation, its effects can be observed even today. Even if it is being said that black money was converted into white legitimate money fraudulently and there has been not been a complete stop in the illegal activities then what has to be seen is that even in the conversion of that black money there has been generation of tax revenue for the government, later in an announcement it was addressed by the Prime Minister that the money that has been deposited in the accounts of citizen who were below the poverty line. There weak position was being used as a ploy by the rich to get the money deposited. The poor people will not be questioned and the money can be kept by them. Similarly, the rich cannot now pursue any legal action for their black money unless they want to fight their cases for breach of contract while being in the tail.

According to our Finance Minister Mr. Arun Jaitley "That people have been compelled to deposit black money into the banks is itself a good evidence of its success".[119] According to him, in lieu of the present circumstances, it was one of the objectives of demonetization to curb black money but due to demonetization, people who possessed black money were forced to deposit their money into the banks. Thus it was a collective achievement. Not only demonetization effected the black money holdings in the country, rather there was a drop in the anti-national activities in the country as well. But it can be said that this statement of Mr. Jaitley was just to counter the negative opinions of the people towards demonetization.

In December 2016, digital payments accounted for 15 per cent of the $1.5 trillion capacity of consumer spending in this country. Due to demonetization and e-governance we could see the 15% transforming into 60-70% overall consumer spending in the next two years, said Mrinal Sinha, operations head at e-wallet

119 S P S Pannu , How Demonetisation has pushed India towards a digital economy, Business Today (December 8th 12:21) http://www.businesstoday.in/current/economy-politics/how-demonetisation-has-pushed-indin-towards-a-digital-economy/story/241958.html

company Mobi Kwik[120]. Tea sellers, vegetable vendors, auto drivers and other local vendors have also opted for online payment mechanism such as MobiKwik, Paytm and others.

Jeremy Bentham[121], often referred to as the father of the positivist school of law, believed in the concept of pleasure and pain. The two concepts of demonetisation and e-governance beffitted these two roles, as demonetisation led to pain for the nation of the people, and e-governance led to pleasure as it acted as medicine to a bruised wound. The concept is in regard to minimum pain and maximum pleasure and this is how e-governance had been implemented as minimum pain for the individual but maximum pleasure as it provides a speedy system, effective results and efficient working which is the need of the moment for our country.

120 Jeremy Bentham, *An Introduction to the Principles of Morals and Legislation*, 1781.

121 Privacy international, *Communication Surveillance*, <https://www.privacyinternational.org/node/10> accessed on 10th Dec, 2016

VIRTUAL CURRENCY : A NEW COINAGE

Ashi Jain* and Diksha Dubey**

ABSTRACT

With a stratospheric rise in internet and online payments and virtual transactions, there are various alternatives available in the world for investment and its payment which has made it easy for the lazy people to do their work without too much hustle-bustle. One of the new inventions in the field of currency is in the form of virtual-currency known as 'Bitcoin'. Bitcoin is a cyber currency in the form of cryptographic technique. It has taken a global stance for settling monetary transactions. It is a new type of peer to peer base currency which is not controlled or issued by any authority and rather it is run on software and block chain system. Bitcoins are gaining the legal stance in various countries like Australia, U.S., Canada and many more. The status of bitcoin in India is disputed as it is not legally recognized in India and especially RBI guidelines make it clear that bitcoins are not authorized by it and further cautioned its users. This paper will try to analyze the merits of having a virtual currency while critically evaluating the pros and cons of plastic currency, money and E-wallets. Further the research will include the legality and scope of whether the bitcoin can find resort in Indian economic and legal fields. Though there are a lot of issues attached with bitcoin like double usage of currency, usage in unlawful purposes and assault on the users privacy and many more but demerits can be dealt with and new laws can be framed in order to pave the way for this new coinage, as even if bitcoin is not given legality there are other alternatives cropping up like litcoin and it is sure that the money will never be the same again.

INTRODUCTION

In this techno-freaks internet era, everything from fun to business has gone digitalised. People around are fascinated by this new digital world where everything is easy and viable by just being a little technological friendly. Everything has gone virtual from entertainment to businesses. Virtual knowledge, virtual game, and virtual gifts- everything is available online. Going with the flow, the basic means of exchange which allows the world to enter the market also needs to be a little virtual. And for that are emerging various virtual currencies, one of them is Bitcoins, which have some different features from the routine regularised currency we use in our day to day lives.

* 2nd Year, Hidayatullah National Law University, Raipur

** 2nd Year, Maharashtra National Law University, Nagpur

Almost every currency we use is 'fiat currency' i.e. a currency which is regulated by the government and financial institutions. Satoshi Nakamoto, the Japanese software designer invented a new virtual currency and released a software for managing this new currency known as Bitcoins. He wrote a paper about Bitcoins in 2009 detailing the workings of the cyptocurrency system. Bitcoin is peer-to-peer digital public money in the form of electronic currency. It is also known as 'cyptocurrency' which is beyond the traditional control and regulation of organisations. It is not a government regulated payment system. 'It is controlled by all the users around the world.

Bitcoin is the very first implementation of a concept called '"cryptocurrency", which was first talked in 1998 by Wei Dai on the cypherpunks mailing list , suggesting the idea of a new form of money that uses cryptography to control its creation and transactions, instead of a central authority. A cryptocurrency is a medium of exchange that uses cryptography to manage the creation of new units as well for the security of the transactions. These are a subset of digital currencies. One of the features of cryptocurrency is that it removes the need for a trusted third party such as a governmental agency, bank etc.

How does a Bitcoin work?

A bitcoin, from the point of view of a user, is a mobile app or a computer program that facilitates the users with a 'bitcoin wallet' by which the users can send and receive the bitcoins all around the world. These digital wallets contain a public key and a private key. Public key is similar to an Email ID which the user shares with the other bitcoin users in order to receive bitcoins from them. Whereas, the private key is akin to the pin number of a debit card, with a purpose to confirm that the user wants to spent the bitcoins in his wallet.

There are two methods of acquiring bitcoins-primary and secondary. The primary method involves creation of new bitcoins using the method known as 'mining'. In that the miners have to solve a complicated mathematical problem for which users employ special computer software. When the problem is solved the miners are rewarded with some extra bitcoins.

The secondary method involves trade i.e. buying and selling of bitcoins. A bitcoin from a user point of view, is a mobile app or a computer program that facilitates the users with a 'bitcoin wallet' by which the users can send and receive the bitcoins all around the world. These digital wallets contain a public key and a private key. Public key is similar to an Email ID which the user shares with the other bitcoin users in order to receive bitcoins from them. Whereas, the private key is akin to the

pin number of a debit card, with a purpose to confirm that the user wants to spent the bitcoins in his wallet.

The bitcoin has been planned to be released in a finite limit of 21 millions in circulation. There is a pre-determined schedule and it is said that the last bitcoin would be mined in 2140. The whole system was intended to be set up in a way that the difficulty of mining every next Bitcoin is greater than the previous one.

The bitcoin works with the help of blockchain technology. Bitcoins and blockchain technology was developed to weed out the need of trusted third parties and to allow a peer-to-peer transactions. The Bitcoin network is sharing a public ledger known as the "block chain". This ledger contains each and every transaction ever processed whereby allowing a user's computer to verify the validity of each and every transaction. The authenticity of each transaction is safeguarded by digital signatures corresponding to the sending addresses, thereby allowing all the users to have full control over sending bitcoins from their Bitcoin addresses.

PROS AND CONS OF BITCOINS

Here are a few advantages of using bitcoin and other similar cryptocurrencies

Firstly, it is a fully decentralized system, and hence it cannot be manipulated by governments and institutions. It is not regulated by a third party. Also, Privacy is protected as there are 2 keys involved: Public and Private which help in recording the bitcoin transactions alongwith anonymous identities.It is always available and has no borders and therefore leads to very low payment costs as it does not involve exchange fees etc. And, Bitcoins cannot be stolen as they are virtual currency and is not available in physical form.

Nevertheless, there are also some disadvantages mentioned by critics:

Now since the transactions are anonymous, cryptocurrencies could be easily used for illegal purposes. For example, Silk Road, an online market place housed within the 'Dark Internet' trades only in Bitcoin. Also, although there may be an increase in number of shops and markets which accept payments in bitcoins,, they are still a very small percentage of the all total.And, there is a risk of data lost which may result in the loss of the bitcoin wallet and you have to eat the loss as there is no legal backing for the bitcoin transactions In addition, the Bitcoin have been used by speculators, and their prices suffered from high volatility as the value of the bitcoin is not fixed.

Legality of Bitcoin

Bitcoin-peer to peer and cryptographic currency is legally a vexed issue. As due to its volatility and lack of regulation, countries are hesitant to legalize its usage. But still there are some countries like Germany, which view Bitcoin transactions as financial transactions that must fulfill strict standards of observation. Stance of India is quite clear when it comes to virtual currency, as with the press release of 2013 RBI, cautioned it users that any use of virtual currency is not authorized by central bank neither any monetary organization.

Thus, in order to understand the legality of Bitcoin, its stance as money or instrument of financial exchange needs to be looked into. World has seen evolution of mode of exchange from barter system, fiat currency to virtual currency. Fiat currency i.e. the notes, coins or visible form of currency is legally recognized. Further Bitcoin comes into existence when high end users mine them wherein gold is used to back fiat currencies, but still Bitcoin can be used to exchange traditional currency, can be used to purchase goods, can be stored online, so it resembles some of the features of currency which is legally recognized like plastic money i.e. credit cards.

Further it is also used as a mode of investment, due to its volatile nature. Government of India is responsible for minting of coins as per Coinage Act and to issue bank notes under the guidance of RBI, whereby Bitcoin is not regulated by the Indian government due to its decentralized nature. Though Bitcoin is able to fulfill major functions of money like medium of exchange, measure of value, standard of deferred payment and store of value but still it cannot be included in money supply of the country, as it is quite difficult to determine money held by public with reference to Bitcoin.

Bitcoin is certainly not the first attempt towards electronic payment system, earlier too attempts were made like companies made the efforts to create digital currency i.e. Digicash, GoldMoney, Pecunix and Web-Money, but these attempts went in vain, as companies like Digicash asked for credit card details though they promised high anonymity unlike Bitcoin which did not ask users to furnish their credit card details. Further GoldMoney and Pecunix denominated in gold and many users were not interested in shopping in such unfamiliar currency . The most important takeover point of Bitcoin over these currencies is its low transaction cost. Also there are virtual currencies being used in games like Farmville, as facebook came up with credit points to be used in Farmville. But they can fail due to lack of system governing fraud and further these currencies are centralized, Bitcoin can cover up for them like it can be a de facto standard for these virtual game currencies and also then users will not have to worry about the inflation of the

currency, when they used to be, due to discretionary power of the company over currency

Stance of Different Countries

Bitcoin from the beginning is under no one's control or authority, and is functioning largely unregulated. So many countries are hesitant to legalize it, but still attempts are made to make its stance clear. Therefore in order to understand its position in different countries, the study can be divided into three categories – a. Countries that attempted to legalize Bitcoin, b. No attempts to regulate it or banned c. Tax regimes for Bitcoin.

Thus going by the first perspective, amidst a lot of opposition of Bitcoin, still some countries have attempted to legalize it among which are Germany, Brazil and Sweden. Brazil in 2013 with its law no. 12865, Article 6 , provides for.or gives way to Bitcoin as it is stated in the definition of e-money, that it comprises of resources stored in device or electronic system that allow the end user to perform payment transaction. And also provides for a provision for payment mechanism whose ancillary function is converting physical or book currency into e-money. Germany is also receptive when it comes to Bitcoin, as it is the first European Country which has legalized Bitcoin, and exempted Bitcoin transactions held for over one year from 25% capital gains tax. Further according to BaFin (Germany Federal Financial Supervisory Authority) Bitcoins are units of account and fall under the definition given in S.1 (11) of German Banking Act. Sweden though does not have a regulatory framework for Bitcoin but has reiterated that Bitcoin constitutes a financial service subject to mandatory reporting requirement.

Second category constitutes of the countries that have not made any attempts to regularize Bitcoin or have banned it; they are– Alderney, Argentina, Australia, Belgium, Canada, Chile, Croatia, Cyprus, Denmark, Estonia, the European Union, France, Greece, Hong Kong,India, Indonesia, Ireland, Italy, Japan, Malaysia, Malta, the Netherlands, New Zealand, Nicaragua, Poland, Portugal, Russia, Singapore, SouthKorea, Taiwan, and Turkey. As it can be seen, many countries have not attempted to regularize Bitcoin, despite its many advantages as they are opting for wait and see approach to analyze the fervency of this new coinage. Further there are a few countries which have banned or restricted Bitcoin like China, Thailand and Iceland. Thailand has out rightly banned Bitcoin, though in China Bitcoin is not illegal, but there are strict provisions which prohibit their Central banks and institutions from dealing in Bitcoin, further the main cryptographic exchange in China i.e. OKcoin, Houbi and BTC China have ceased their operations due to government orders.

The third category comprises of the country which imposes tax on Bitcoin, for example United Kingdom, though Bitcoin is unregulated in UK but it has been reported "that Her Majesty's Revenue and Customs has classed bitcoins as "single purpose vouchers," rendering any sales of them liable to a valueadded tax of 10–20%" whereas in Spain, Bitcoins are considered as digital goods under their civil code and thus the ones who deal in them are required to issue an invoice with value added tax in euros. While in Finland Bitcoin is taxed as per Finish income taxation Act.

Thus it can be concluded that opinion and status of countries with respect to Bitcoin is dispured and still many are in a phase of analyzing this new coinage.

Conclusion and Suggestions

Bitcoin has come up in the virtual currency world to facilitate the monetary transactions, though it has faced a lot of opposition, but still it has occupied a position for dealing in financial transactions. Certainly Bitcoin is favorable when it comes to plastic currencies like credit and debit cards, as Bitcoin removes the middle man which is otherwise there, like banks in case of plastic currency, further it has low cost of transactions as other payment modes have higher transaction costs due to government regulation, monopolization of certain systems and implementation of certain fraud protection schemes. While e-wallets like Paytm and PayPal are also not devoid of third party and are just facilitator of exchange of money, but Paytm is accepted by RBI and it also got the permission to establish payment banks , which certainly was a good lead of India towards recognizing electronic mode of payments. But despite of Bitcoins advantages and favorable character over other mode of payments, it suffers from certain inconsistencies and defects. Due to its unregulated nature, Bitcoin can be used for illegal purposes like can be used by terrorist organization, can be used in drugs smuggling, and for criminal use on silk road and thus giving way to an illegal market. Another disadvantage of using Bitcoin is that it is prone to fraud and the most apt example of this is of Mt.Gox, which was a Bitcoin exchange launched in Japan in 2010 and was controlling almost 70% of Bitcoin exchange transactions by 2013, but it was alleged that over $450 million of user'sbitcoin were stolen by unknown hackers. Thus in order to minimize or reduce the effects of these inconsistencies there are a few suggestions like:

- Countries where it is regulated must come up with a system to try cases of fraud and counterfeiting, as it was done in SEC v. Shavers, wherein SEC (Securities exchange commission, U.S.) charged the organizer of an alleged ponzi scheme involving Bitcoin with defrauding investors. , thus countries like

India can also try cases involving fraud under the guidance of SEBI (securities exchange board of India).

- Establish regulating organizations like FinCEN (financial crimes enforcement network, U.S.A.)
- To curb money laundering, bring Bitcoin under the acts of which regulate money laundering like India can make efforts to include Bitcoin in its prevention of money laundering Act, 2002.
- Make the regulation system strong or government must take initiative to protect the users of Bitcoin, as if the example of Mt. Gox we must emulate, as in that case users lost their invested amount, so a mechanism must be establish to indemnify the users.

Thus it can be concluded that though Bitcoin is being opposed and not recognized by many countries, but still it is paving its way gradually and if not Bitcoin then its offshoot like Litecoin (improved version of Bitcoin with some technical differences) and dogecoin(differs from Bitcoin as it provides more efficiency in conducting transactions) will be given space in the financial market. Thus it is for sure that currency will not remain the same.

RIGHT TO PRIVACY V. NATIONAL SECURITY IN THE FORM OF COMMUNICATION SURVEILLANCE

Anushka Sachdev*

Overview

Communication surveillance is performed by many states to ensure national security. This interception of communication must be lawful and duly authorized across all jurisdictions. It interferes with right to privacy of individuals and hence the law that allows for it should be in accordance with human rights principles.[122]It should meet the minimum standards of being both necessary in a democratic society to achieve a legitimate aim and proportionate to that aim. It should not be arbitrary and individual's right to communicate privacy should not be interfered with unless it is in accordance with a clear and transparent law.

There are many laws in place both at international and national level which provide for lawful surveillance i.e. surveillance done by taking into account the right to privacy of the individuals but most processes around this remain unclear. Often these laws are interpreted broadly by courts and secret surveillance authorized by courts and the concerned individuals are not notified of the same.[123] Some of these legislations have lost their relevance in light of new technologies which are clearly not waiting for the legislations to catch up. Thus there is an urgent need of new and improved laws in this area to pave way for the courts to interpret them such that due importance is given to individual's privacy rights even at the advent of new and powerful technology.

This paper will first firstly highlight certain important international human rights principles in this regard and will then analyse cases on this issue from various eras and jurisdictions in light of those principles.

* 5th year B.A.LL.B (Hons.), National Law University, Delhi

122 Privacy International, *Communication Surveillance*, available at <https://www.privacyinternational.org/node/10> accessed on 10th Dec, 2016

123 Human Rights Council, Report on the Twenty seventh Session, 27th Sess., UN Doc. A/HRC/27/37 (2014)

International Human Rights Framework

The Report of the Office of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age noted that:

"In the digital era, communication technologies also have enhanced the capacity of Governments, enterprises and individuals to conduct surveillance, interception and data collection. As noted by the Special Rapporteur on the right to freedom of expression and opinion, technological advancements mean that the State's effectiveness in conducting surveillance is no longer limited by scale or duration. Declining costs of technology and data storage have eradicated financial or practical disincentives to conducting surveillance. The State now has a greater capability to conduct simultaneous, invasive, targeted and broad-scale surveillance than ever before."[124]

Thus the international human rights framework exists with regard to communication surveillance to balance the fundamental right of privacy of individuals with the protection measures ensued by the state to enable national security. The right to privacy is enshrined in both international and regional human rights documents. The most prominent ones are Article 12 of the Universal Declaration on Human Rights and Article 17 of the International Convention on Civil and Political Rights. Article 12 of the Universal Declaration of Human Rights provides that "*no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*"[125] Article 17 of the International Covenant on Civil and Political Rights provides that "*no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation*".[126] It further states that "*everyone has the right to the protection of the law against such interference or attacks.*"[127]

Three essentials of an individual's right to privacy in communication include the need for the communication to be private, secure and anonymous (if they choose)[128]. Privacy in this sense refers to the exchange of ideas between individuals that is beyond the reach of other members of the society, private sector and the state.[129]Security implies that the communication reaches the recipients it is intended for and there are no alterations in its content and intrusions in its reception.

124 Article 12, Universal declaration of Human Rights

125 Article 17,International Covenant on Civil and Political Rights

126 *Ibid*

127 Human Rights Council, Report on the Twenty third Session, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc. A/HRC/23/40 (2013)

128 *Ibid*

129 *Ibid*

[130]Anonymity of communications is a recent phenomenon enabled through internet and facilitates free expression by individuals without any fear.[131]

This right to privacy of individuals is held in high regard under international human rights law and any interference with it is permissible only when such interference is neither unlawful nor arbitrary.[132] Thus no interference is permissible unless specifically provided in the law and if such law is arbitrary in its application and allows for an intrusion that is against the provisions of the International Covenant on Civil and Political Rights, it would come under the ambit of arbitrary and would not be permissible.[133] Thus the exceptions provided in national laws should be in accordance with human rights principles for them to be valid under international law. The law must also be reasonable such that "any interference with privacy must be proportional to the legitimate end sought and be necessary in the circumstances of any given case".[134]National security for prevention of terrorism or any other crime comes under the ambit of "legitimate aim" as per article 17 of ICCPR if the degree of interfereuce is proportional to the purpose and necessary to yield desired results. [135] The protection measure sought must be least intrusive amongst the instruments available to the state and the state has the onus to prove the necessity and proportionality of such a measure.[136] Thus article 17 of ICCPR is subject to the same limitations test as described in other general comments of the Human Rights Committee.

To cater to the negative impacts of communication surveillance on human rights and to account the concerns of member states, the General assembly adopted a resolution on right to privacy on digital age in December 2013.[137] Another measure in this direction was taken by civil society groups and International Principles on the Application of Human Rights to Communications Surveillance were launched in 2014.[138]

Case Analysis

One of the first cases that dealt with the importance of right to privacy when weighed against the security of the state through communication surveillance was

130 *Ibid*
131 *Supra* note 3
132 *Ibid*
133 *Ibid*
134 *Ibid*
135 *Supra* note 7
136 General Assembly Resolution 68/167 on "The right to privacy in the digital age".
137 International Principles on the Application of Human Rights to Communications Surveillance , <https://www.eff.org/files/necessaryandproportionatefinal.pdf>
138 United States v. United States District court, 407 U.S. 297 (1972).

the 1972 decision of United states Supreme Court of *United States v. U.S. District Court*[139]. It brought about the requirements of the fourth amendment of the US Constitution in which the right to privacy is enshrined. These requirements include prior judicial approval for domestic surveillance in the form of a warrant as the government's duty to safeguard domestic security has to be weighed against the potential danger that such surveillance poses to individual'sprivacy and free expression.[140] This danger becomes apparent when the government's start exercising power under the vague head of 'domestic security' and thus proper safeguards need to be put in place to prevent unbridled exercise of power. [141] These requirements were upheld in further cases and thus these form the basis of the balance between the two conflicting rights.

The jurisprudence in this regard continued in this direction until the 9/11 terrorist attacks in 2001 which brought about a major transition in the balance brought about by the courts. The National Security agency launched a foreign intelligence program post 9/11 by the name of Terrorist Surveillance Program. The purpose of this program was to intercept the international telephone and internet communications of numerous persons and organizations within the United States, without obtaining warrants.[142] This was outside the ambit of Foreign Intelligence Surveillance Act of 1978and was in violation of the principles laid down in the constitution as well as previous cases. This was challenged in the case of *American Civil Liberties Union v. National Security Agency*[143] in 2007 in which the United States Court of Appeals for the Sixth Circuit decided against the plaintiffs to hold that they had no locus to sue National Security Agency because there was no sufficient proof to establish that they were wiretapped by the NSA.[144] Thus their injuries were of amorphous character and were not a direct consequence of the program.[145] The court did uot get into the merits of the case and thus the fate of the program was left undecided. As the Supreme Court refused to rule on the case, the Americans were denied the chance to challenge the unwarranted wiretapping of their communication and "national security" was again used as an excuse for encroaching the privacy of individuals.

These dated ideas of communication surveillance have been addressed by civil societies and courts and notable advancements have been made in the jurisprudence

139 *Ibid*
140 *Ibid*
141 *Ibid*
142 493 F3d 644 (6th Cir. 2007)
143 *Ibid*
144 *Ibid*
145 ACLU v. Clapper, No. 13-3994 (S.D. New York December 28, 2013)

in this regard. The disclosures by Edward Snowden in US were a reflection of the government's capability to operate in secret and to conduct surveillance in unaccountable ways due to the technical advancements. The core question to the court in this case was regarding the relevance of the metadata collected by the government through phone calls made to people in the USA.[146] The Court didn't buy the expansive construction of 'relevance' to include the idea that it may be used to look for patterns connection to national security threats. [147]It instead upheld that notion that if only some of this data turns out to be relevant for such investigations, most of it doesn't matter at all. Thus it held that the collection of metadata is an overboard search and is thus beyond the most expansive definition of relevance.[148] This paved way for a stricter jurisprudence regarding construction of relevance of surveillance data throughout the world and limited the powers of governments to great extent.

This development led to the judgment of the European Court of Justice[149] which held the Data Retention Directive to be invalid. The directive provided for the retention of data generated by providers of publicly available electronic communications services or of public communications networks for investigation etc of crime particularly terrorism.[150] It enables the providers to retain data related to traffic, location and other data for identifying the subscribers but leaves the retention of content out of its ambit.[151] The court held that the combination of this retained data will lead to precise information on the private lives of individuals which include routine habits, place of residence etc. [152]This results in serious interference with fundamental right to privacy by the directive. It also held that by adopting this directive, EU infringed the principle of proportionality and thus reduced the discretion of legislature and made the review of that discretion strict. [153]It reiterated that even though the directive has a legitimate objective, it results in a serious interference of fundamental right and thus this interference should be limited to what is necessary. It identified certain problems with the directive. The directive provided for no differentiation or exception to attain its objective of fighting serious crime but instead covered all individuals in a generalized manner.[154]

146 *Ibid*
147 *Ibid*
148 Joined Cases C 293/12 and C 594/12 Digital Rights Ireland and Seitlinger and Others
149 *Ibid*
150 *Ibid*
151 *Ibid*
152 *Ibid*
153 *Ibid*
154 *Ibid*

Secondly, the directive did not lay down any objective criteria which enabled the access only to competent national authorities who used the data only for legitimate purposes of prevention, detection or criminal prosecutions. [155]This was important to justify the serious interference of fundamental right it resulted in. It also did not provide for any procedural or substantive conditions that need to be satisfied for national authorities to access the data which includes prior approval of a judicial or administrative body. Thirdly the directive provided for a data retention period which ranges from 6 months to 24 months and did not distinguish on the basis of categories of such data, the persons concerned or the usefulness of the data. [156]Thus it laid down no objective criterion for determining the data retention period and thus does not ensure its extent to what is strictly necessary. Thus the directive did not provide for sufficient safeguards to ensure its protection from abuse against any unlawful access and use and was thus held invalid by the court.[157] This decision of ECJ established nuanced factors that need to be taken into account for a law to balance the conflicting rights of privacy and national security.

The most recent case on this issue is the 2016 case of FBI v. Apple where the FBI wanted Apple to create a new software and thus provide reasonable technical assistance to the FBI to unlock a work-issued iPhone 5C that was recovered from one of the shooters in a December 2015 terrorist attack in San Bernardino, California, that killed 14 people and injured 22.[158] Apple declined to create the software and argued that this would have a chilling effect and would act as a master key which would enable the FBI to open millions of locks thus infringing privacy rights of millions of others.[159] However, a day before the hearing was supposed to happen, the government obtained a delay, saying they had found a third party able to assist in unlocking the iPhone and it was announced that the FBI had unlocked the iPhone and withdrew its request.[160]

Conclusion

Thus it is observed by the researcher that even though jurisprudence in this direction was initially developed in favour of privacy rights of individuals but in the wake of 9/11 terrorist attacks and increased amount of national security threats in the 21st century, the jurisprudence is being moving in the opposite direction and is

155 *Ibid.*

156 *Ibid.*

157 *Breaking Down Apple's iPhone Fight With the U.S. Government*, N.Y. TIMES, March 21, 2016.

158 *Ibid.*

159 *Ibid.*

160 Preamble, Convention on International Sale of Goods, 1980.

slightly favoring the protection measures initiated by the governments to ensure national security. There are a few exceptions due to increased activism of civil society groups but most of these principles and laws lack proper implementation and most of such surveillance activities continue to take place in secret and unlawful manner. Such arbitrary exercise of powers by the government even in light of ensuring security causes more harm than good as most of this surveillance data is not relevant for security purposes and unduly infringes the privacy of individuals. Thus such unbridled power in the hands of the government should be curbed especially in view of the advent of digital age. A balance needs to be stuck between the two conflicting rights using the international human rights framework and concepts of reasonableness, necessity, proportionality etc.

ISSN 2249-4421 UGC Approved Journal No. 42016

CONVENTION ON CONTRACTS FOR THE INTERNATIONAL SALE OF GOODS AND INDIA – RATIFICATION V. ABSTENTION

Bhavana Asthana* & Nehul Sharma**

ABSTRACT

The CISG is a self-executing multilateral treaty that governs transnational trade in goods, is binding upon the signatories, and provides standardised laws around the international sale of goods. The treaty was curated and accepted by the UN Commission on International Trade Law and put in place in Vienna, in the year 1980. As of 29 December 2015, UNCITRAL has testified that 84 States have ratified and adopted the Convention on International Sale of Goods.

So as to attract a substantial number of countries to join the treaty, there were numerous concessions made within the terms and scope of the CISG. These included reservations made by some of the signing countries as their conditions towards ratifying the CISG. More often than not, these concessions are said to have added many complications to the issues that the CISG originally aimed to resolve. Nonetheless, most of the prominent Global players are signatories to this convention. India, interestingly, has abstained from ratifying this Convention. Other notable abstainers include Brazil, Britain, et cetera.

India's ratification to the Convention would imply that the CISG would override the familiar rules of the Indian Sale of Goods Act 1930 and direct the rights and duties of both Indian buyers and sellers, whilst transacting internationally. While this may seem like a total discourse from what is widely accepted, well-practiced and intrinsically entrenched in Indian Commerce, the fact that over two-thirds of the nations are party to this Convention speaks volumes of the positives in favour of ratification. The aim of this paper is to understand and evaluate the implications of abstention and ratification of CISG by India and apprise the major options that stand in the best interests of India as a player in the world market.

OVERVIEW

The United Nations Convention on Contracts for the International Sale of Goods is essentially of the nature of an overlay i.e. it rests upon the national sales code of each of the member nations that have adopted it. In most of the situations, this is

* 5th year, B.A.LL.B.(Hons.) USLLS, GGSIPU

** 5th year, B.A.LL.B.(Hons.) USLLS, GGSIPU

a domestic regime which may either be of the nature of a civil law or common law. This multilateral treaty governs the transnational sales contracts in cases where both the parties to the contract are housed in Contracting States or the norms of private international law operate such that the law of contracting state is the one that is reasoned to be applicable.

The Preamble attached to the CISG signposts the intent of the drafters - "the adoption of uniform rules which govern contracts for the international sale of goods and take into account the different social, economic and legal systems would contribute to the removal of legal barriers in international trade and promote the development of international trade."[161] To the tune of this, the drafters proceeded to chart out the requirements in detail for the same to be met through the formation of a sales contract, along with the various rights and obligations of parties to the contract.

The primary objective and foundation of this convention is to guarantee a considerable degree of party autonomy. The parties are authorized to, by means of an agreement, override any rule so stipulated by this Convention or further, even exclude the applicability of the CISG in its entirety, replacing the same with any other law that may be in place. When the CISG is adopted, even then it does not oversee each and every issue that can arise out of an international sales arrangement. For instance, complications with regard to the validity of the contract or the applicability of the arrangement on the property and goods in question, as stipulated by the CISG, outside of the ambit of the Convention in question, are left to the law applicable as per the arrangement and the rules of international law. As a matter of general practice, questions relating to the matters overlooked by the CISG, however not directly attended to therein are usually decided in conformity with the general principles of the Convention, and in lieu of the same, as per the law applicable vide the rules of private international law.[162]

KEY PROVISIONS AND STRUCTURE OF THE CISG

The Convention on International Sale of Goods is bifurcated into essentially four parts which are further divided into numerous sub-divisions. The major parts are:

A. Scope of Application and General Provisions

161 Harry M. Flechtner, *United Nations Convention on Contracts for the International Sale of Goods*, Audiovisual Library of International Law (1980), http://legal.un.org/avl/ha/ccisg/ccisg.html.

162 *Explanatory Note by the UNCITRAL Secretariat on the United Nations Convention on Contracts for the International Sale of Goods*, United Nations document V.89-53886 (1989), http://www.cisg.law.pace.edu/cisg/text/p23.html.

B. Formation of the Contract

C. Sale of Goods

D. Final Clauses

The head of Scope of Application and General Provisions is further divided into sub-heads of Scope of Application, Party Autonomy, Interpretation of the Convention, Interpretation of the Contract and Form of the Contract. This head essentially stipulates the scope of applicability of the Convention and consistent interpretation of the convention across all major legal systems. It further clarifies that the Convention *per se* doesn't instruct a mandate as to the form of the contract so entered into by the parties, however, there is an enabling provision which, if endorsed by the parties, makes it necessary to have the contract and any amendments to it in writing.

The Formation of the Contract head deals with the various questions that may arise in the process of entering into an arrangement. When the formation of the contract takes place in accordance with the provisions herein, the contract is concluded when the acceptance of the offer becomes effective.

The third part that governs the Sale of Goods under the Convention and is sub-divided into eight parts, viz. Obligations of the Seller, Obligations of the Buyer, Remedies for Breach of Contract, Passing of Risk, Suspension of Performance and Anticipatory Breach, Exemption from Liability to Pay Damages and Preservation of the Goods. As intrinsically indicated by the sub-heads, this part enumerates the various rights, obligations and duties of the parties to the Contract and the various remedies and provisions vis-à-vis the sale and purchase of goods and any situation that may arise in the event of non-conformity or anomaly.

The fourth and final section of the CISG spells out the final clauses which include the usual provisions associated to the Secretary-General in the capacity of depositary and announcing that the CISG is subject to ratification, acceptance or approval by those States that signed it by 30 September 1981, that it is open to accession by all States that are not signatory States.[163]

CONCESSIONS UNDER THE CISG

So as to attract as many as possible countries to join in and conclude the treaty, there were numerous compromises which were made in the terms and the scope of the CISG in order to make it a flexible document. These compromises were

163 *What Is The Purpose Of CISG*, Law Teacher, https://www.lawteacher.net/free-law-essays/international-law/what-is-the-purpose-of-the-cisg international-law-essay.php.

vastly in the nature of revocations and reservations made by certain members as their precondition in order to agree to the CISG. More often than not, these concessions further difficulties to the questions that the Convention aims to cater to, adding up to the various limitations which the CISG is inflicted with.

Particularly, Article 98 of the Convention authorized the contracting parties to make reservations as preconditions to joining the CISG. Specific instances include:

1. Article 92 of the Convention on International Sale of Goods allows the exclusion of Part II (which deals with the formation of contracts) and Part III (which is related to the obligations of the buyer and seller and remedies in the event of breach). For instance, Scandinavian States have professed that they, by virtue of this article, won't be bound by Part II of the Convention.

2. Article 93 of the Convention authorizes a Contracting State wherein two or more regional units practise distinct regimes of law in order to declare that the Convention doesn't extend to each of the territorial parts. For instance, Australia has stated that the Convention is not to extend in application to certain territories.

3. Article 94 of the CISG authorizes any State which may have an ongoing contract in relation to matters overseen by the Convention in order to announce that the Convention on International Sale of Goods wouldn't extend to parties having a place of business in such territory. By virtue of this Article, inter-Scandinavian trade is excluded from the application of CISG.

4. Article 95 of the CISG instates that Article 1(1)(b) of the very same can very well be excluded. Article 1(1)(b) of the Convention deals with the conflict rules whilst defining the jurisdiction of the Convention. Notable countries that have stated that they won't be bound by the said provision include China, Singapore and the USA.

5. Article 96 of the Convention authenticates the actions of a State to exclude any provision of Article 11, 29 or Part II (providing for the contract to not necessarily be in writing under the Convention), given that their law requires contracts to be in writing. Notable countries that have made declarations under this article include Argentina, Chile, Russia and China.[164]

Now the issue that arises out of this flexibility is, to a point, the negation of the underlying principle the CISG operates upon. The intended uniformity across

164 Arthur Rossett, *Critical Reflections on the United Nations Convention on Contracts for the International Sale of Goods*, 45 Ohio State Law Journal 265-303 (1984).

jurisdictions vis-à-vis sale of goods is compromised and there arise complications in unvarying application.

INDIA'S OPTIONS – TO RATIFY OR NOT?

Amongst notable countries which have abstained from ratifying the Convention on International Sale of Goods are United Kingdom and interestingly, India. It only makes sense for a country having recently opened its market to the world to opt for a multilateral treaty as far reaching as the CISG. However, it is important to note that every option comes with pros and cons. India's approval of the application of the CISG by ratification would signify CISG being the overriding set of norms in international sale of goods and not the widely recognized (although, domestically) rules of the Indian Sale of Goods Act 1930, which would oversee the privileges of the buyers and sellers, when trading internationally (that is to say, the Indian buyers and sellers).

The Indian trading community and the associated legal personnel, aided by resilient case law and precedent, can precisely forecast the plausible result of an algorithm employed in the buying and selling (of goods). For a country like India, ratifying the CISG would be wise only in the case its advantages outweigh the disadvantages, when employed in a practical situation. Space consideration prevents full discussion of them; however, the following paragraphs discuss some important ones.

ARGUMENTS IN FAVOUR OF RATIFICATION

The primary agenda behind concluding this Convention was to achieve simplicity and unify the legal position vis-à-vis international sale of goods. About two-thirds of the nations have ratified the CISG, contributing to its unparalleled popularity. It is also contended that various matters, when ultimately resolved as per the provisions of CISG are ultimately compiled under Case Law of the UNCITRAL text which would create a cohesive body of precedential law, only making the Convention stronger with every going day.

When we compare the ongoing regime of domestic law with the CISG, it proves to be relatively obsolete and the new international Convention definitely appears to be a more recent, flexible and viable set of rules to be able to govern the modern day complex trade relations between buyers and sellers of goods. Further, the CISG plays a pivotal role in the 'gap-filling' whilst a cross-border agreement is entered into by phone, fax, telex et cetera. Moreover, in an event of entering into an international sale of goods agreement, there is a possibility that the Indian buyers and sellers may have to play by the rules established by the foreign party as per their own law. In any such scenario, it always helps to go by an established international

body of principles rather than an unknown foreign legislation. The nature of Convention law is intrinsically neutral, which makes it easier for both the parties to accept its operation in buying-selling of goods. It is one of the better drafted convention of modern day and also assists in avoiding tricky situations which may arise due to conflict of laws.[165]

Accounting for the more practical and subject-matter related aspects of the CISG, it is important to note that the Convention accounts for the modern realities and emerging trade practices. It is drafted in simple language, making it easier for the parties to understand even without massive involvement of legal personnel. The need for practical rationality reflects in the provisions of this Convention as it caters to real world scenarios with regard to purchase and sale of goods, for instance, requiring the parties to the contract to preserve goods in their possession which ultimately belong to the other party. Owing to the uniformity in transactions that it confers, the Convention facilitates effective and efficient cross-border trade, saving money, time and effort.[166]

ARGUMENTS AGAINST RATIFICATION

It is of common knowledge that any and every time a new legal document is introduced, it brings along with itself a set of complexities and uncertainties with regard to the application of new rules. Such uncertainty arises due to there being novel undefined terms and phrases which haven't been interpreted earlier by courts and tribunals which demand to be developed in the international domain. Often, the complications that arise in course of purchase and sale of goods are basic and familiar. Having to apply an entirely new and global regime to such recognizable, even domestic problems can prove to be an unnecessary complication. Further, the option to be able to exclude partial application of this Convention contributes to its redundancy in entirety.[167]

The essential nature of the Convention on International Sale of Goods is accommodating and compromising, which often gives lopsided solutions and dodges real world issues in the process. Further, the Convention is subjected to multiple methods of interpretation across the globe and in process, the integrity of this document is threatened by varied interpretational techniques and traditions. Courts around the globe, practising varied legal traditions, partly due to vague

165 Louis F Del Duca, *Practice Under the Convention on International Sale of Goods (CISG) A Primer for Attorneys and International Traders*, 27 IICC Law Journal 331-370 (1950).

166 *Adoption of the UN Convention on International Sale of Goods in South Africa*, (1999) 116 SALJ, Pt II, 323-370. www.cisg.law.pace.edu/cisg/biblio/eiselen.html.

167 Article 55, Convention on International Sale of Goods, 1980.

wording, have interpreted provisions inconsistently. The Convention on International Sale of Goods is not all-inclusive. It doesn't encompass essential ingredients such as provisions vis-a-vis the validity of the contract, that is to say, with the matters of unlawfulness, misrepresentation or scams with regard to the contract.

Further, there are many discrepancies in drafting that lead to general difficulty in application and lack of clarity. One of the manifestations of the same can be seen if we compare the provisions of Article 14 and article 55. As per Article 14, there need to be two essential elements present in order for there to be a valid contract of sale. These include:

- an intention to be bound
- a sense of definiteness furthered by:
- a clear description of subject matter of sale
- fixed quantity
- fixed price

On the flipside, Article 55 of the Convention makes a contract valid even if the price is not clearly stipulated. It is worded as: 'Where a contract has been validly concluded but does not expressly or implicitly fix or make provision for determining the price, the parties are considered ... to have impliedly made reference to the price generally charged at the time of the conclusion of the contract ...'.[168]

Clearly, this article applies in situations where the price i.e. the consideration is not fixed, however, the contract is validly concluded. On the flipside, Article 14 makes the contract invalid in the first place on occasion of the price not being fixed. Many other features of the CISG are of the nature that causes there to arise inconsistencies with the ongoing domestic practice in India, some being the concept of "fundamental breach"[169], making it hard to ascertain whether or not a particular act passes the test to be called so and so on.

CONCLUSION

One cannot deny that the Convention on International Sale of Goods has been one of the most successful documents of its kind. While opting in seems to be the direction to head in, given that it eases and accelerates international trade in goods with India being one of the parties, it is also true that the Indian practitioners in law

168 Article 25, Convention on International Sale of Goods, 1980.

169 DimitriosZissis&DimitriosLekkas, Addressing Cloud Computing Security Issues, 28 Future Generation Computer System 584, 583-92, (2012).

haven't yet explored international laws in the kind of depth that may be required to truly become an aware body of professionals. Not ratifying to the CISG may provide a much wider scope to be able to explore the laws of other nations and expand our own horizon and knowledge base.

CISG *per se* is not an all-inclusive code like many other documents. It primarily seeks to accompany specific areas of the law, overlooking all of the issues which may fall within its ambit of operation. There were certain matters which were held to be way too contentious in order to be included within the Convention because the domestic laws of various nations differed too much on the subject matter, making it hard to accommodate all the approaches. In order to attract as many signatories as possible, the makers of this document left these issues outside of the purview of CISG. They instead chose to go forth with a more widely suitable document instead of an all-inclusive, self-standing complete but contentious convention.

For any tradition of law and the system following the same, it is pivotal to differentiate among cases and situations wherein the contract continues to be operational irrespective of its breach by one of the parties and those cases wherein party that is affected is to be allowed to terminate the same, putting an end to the contractual obligations and recovering what's lost. The CISG is not quite as accommodating in this aspect for it lays down the provision of remedy of avoidance quite apathetically and the same policy is recognised by the judges.

The Convention on International Sale of Goods definitely has a big potential to be adapted into something of the nature of the dominating international sales law, and it's right on the bandwagon. It is entirely upon us to confirm that joining in would accelerate the agenda that leads the Indian sales and purchases in the world market. If not, abstention is the way to go.

MAJOR HASSLES OF CLOUD COMPUTING CONTRACT AND THE LEGAL FRAMEWORK

Richa Mishra* **and Aparna Tiwari****

ABSTRACT

Cloud computing as a means to replace the bulky and expensive hard drives is the need of the fast moving information technology sector. Starting from an individual to small and large organizations, cloud computing is used by everybody. Owing to its boundless nature and lack of geographical conformity, various legal issues arise out of the service of cloud computing and it is often seen that the legal framework of any individual country is not yet sufficient to tackle these issues. All these legal issues shrink down to the contract of cloud computing between the cloud service provider and the end user. Therefore the contract plays a pivotal role in understanding and curing the nuisance of cloud computing. This article tries to critically analyze the contract of cloud computing and focus on the major issues which are detrimental to the right of customers. The article also discusses the legal framework of some countries and how this framework lacks in catching up with the fast moving world of cloud computing.

A. INTRODUCTION TO CLOUD COMPUTING

A working paper was developed by The European network and Information Security Agency (ENISA), which was based on securities feature of cloud computing. The definition which ENISA formulated was based on recommendations from the National Institute for Standard and Technology (NIST), the Vaquero definition, and others: "Cloud computing is an on demand service model for IT provisions, often based on virtualization and distributed computing technologies."

"The term Cloud Computing is inspired by the cloud symbol which is often used to represent the Internet in flow charts and diagrams.[170] Natural Cloud holds water, the internet cloud holds mammoth amount of data the analogy thus results in coining the term cloud computing." It works as a substiture for hardware and software as it is made to share a pool of information, resources and data. As

* 3rd year, B.Com LLB(Hons), College of Legal Studies, University of Petroleum and Energy Studies.

** 3rd year, B.A. LLB, College of Legal Studies, University of Petroleum and Energy Studies.

170 The National Institute of Standards and Technology (NIST), Available at -http:// www.nist.gov.itl?cloud?upload?cloud-def-v15.pdf.

defined by NIST "Cloud Computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources(e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[171]Cloud computing means to share resources freely and conveniently from the nebula of computers.

B. CLOUD COMPUTING CONTRACT: COMPONENTS

Just like another click wrap agreement where the terms and conditions of the contract is already written and there is very little room left for negotiation in the contract cloud computing contract in the other count on that list. In click wrap agreement the user either has to accept the contract terms as it is or avoid the contract. The party first has to go through the entire terms and conditions of the service and then has to express its decision either by clicking on "I agree" or "I disagree". Click wrap agreements are mainly used with software licenses and online transactions. Contract of cloud computing varies with different cloud service provider and also on the kind of service one is looking for. Some cloud service providers provide the option of customization of services according to the need of the end user. A contract of cloud computing though varies from one service provider to, however the main components of a contract of cloud service are:

1. **Terms of service:** It is also known as terms of use. It establishes the relationship between the supplier and the customer. It specifies the legal terms and conditions related to the service of cloud.

2. **Privacy Policy:** This part of the cloud contract describes what all data stored in the cloud is accessible by the provider and how they can use it. It also mentions the kind of right the provider is going to have on the data stored in the cloud on account of it being the service provider.

3. **Acceptable usage policy:** It lays down the permitted and prohibited practices one has to observe in the course of using the service of the cloud provider. Like prohibiting hate speech or forbidding use of service to deliver spam.

4. **Service Level Agreement (SLA):** A part of the contract known as service level agreement describes what all service would be provided. SLA mentions the period for which service will be available and when not. It also mentions the compensation provided in case of bad service. "It verifies what

171 Mitchell Cochran & Paul D. Witman, *Governance and Service Level Agreement Issues in a Cloud Computing Environment*, Journal of Information Technology Management (2014).

administrators have access to the data and if there are logs that are retaining personal logs.[172]"

The cloud service providers draft their own contract suited to their service and the kind of users they intend to sell and thus the contract vary. For example the providers whose buyers are commercial banks will be focusing more on their privacy policy clause similarly whose buyers are interior designers will be focusing on the IPR clause. Some clauses which are prerequisite to a cloud service contract are discussed below:

1. **Liability:** This clause settles the right and liabilities of the parties to the contract. It discusses mainly the responsibility of the service provider in case of service outage or data loss and other types of losses. Most of the service providers use this clause to shed off their liability. However the customer can negotiate depending on their status if they want unlimited liability in case of breach of data protection, privacy or confidentiality.

2. **Intellectual Property Rights (IPR):** This clause makes clear the stand between the service provider and the customer as to who owns the intellectual property right over the material which is developed by using the cloud services.

3. **Termination of the contract:** This clause discusses the minimum service period of the contract, consequences of early termination of the contract etc.

4. **Governing law and jurisdiction:** This clause clears the jurisdiction of the court that would be entitled to enforce the terms of the contract. Jurisdiction clause may provide to resort to arbitration or mediation before going to any court of law and the name of the arbitrator. Or it may restrict the jurisdiction to a particular geographical area.

5. **Lock In/Exit:** This clause is considered to be an important one as it provides the duties of the providers post termination of the contract. This clause may impose a duty on the service providers to ensure that the data stored in the cloud is deleted after the termination of the contract. This clause also mentions if the cloud service provider would provide transition-out assistance and if yes at what cost. It also mentions the transition –out assistance if provided by the provider at additional cost.

172 S.O. Kuyoro, F.Ibikunle&O.Awodele, "Cloud Computing Security Issues and Challenges" (2011) Vol. 3(5) International Journal of Computer Networks 247.

C. MAJOR ISSUES RELATED TO CLOUD COMPUTING CONTRACT

C.1. ISSUE OF DATA PRIVACY AND SECURITY

Doing wonders for all users be it a large multinational company or be it an individual who stores his data on the cloud just to avoid the cost of hard disks, cloud computing holds its major drawback in its contract which decrease the trust of the users. Though the demand of cloud computing services is increasing at a very fast pace yet the customers feel reluctant in using cloud services, privacy issues being the top fear of all.[173]Generally an individual would be less reluctant in sharing his data with the service provider but a large organization would think twice before sharing its proprietary data with anyone. Information leakage is likely to take place when information of one user is given to other as a very large number of users share their information on a single platform. Organizations in some specific sector are forbidden by law to share certain data like hospitals through their privacy policy are bound not to disclose medical information of their clients, RBI has issued guidelines for banks to follow a code of conduct when they give their services to a third party.[175] Cloud computing in its very nature is designed such to store and make copies of the content we upload in order to make it available wherever the customer wants it to be. The increasing usage of the services like google drive, drop box etc. makes it a concern for the advocates of privacy to criticize the cloud computing model as most of the cloud computing contract explicitly provides in one of its privacy policy that they own the right to monitor the data on the cloud at its own will.[176] For example, given is one of the clauses of google drive cloud computing contract:

"When you upload or otherwise submit content to our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content."

173 A. chhibber, *"Security Analysis of Cloud Computing"* (2013) 2 (3) International Journal of advanced Research in Engineering and Applied Sciences 2278-6252. Retrieved 27-2-2015.

174 Nishith Desai, Cloud Computing Risks/Challenges Legal & Tax Issues (March, 2013), http://www.nishithdesai.com/fileadmin/user_upload/pdfs/Cloud_Computing.pdf.

175 Michelle Maltais, Who owns your stuff in the cloud?, Los Angeles Times (Apr. 26,2012),http://articles.latimes.com/2012/apr/26/business/la-fi tech-savvy-cloud-services-20120426.

176 PTLB, *Legal Framework for Cloud Computing in India, Perry4 Law Organization's Blog* (Wednesday, October 17th, 2012), http://perry4law.org/blog/?p=118.

Cloud computing contracts fly right in the face of much wanted right in the current jurisprudence of India i.e. right to privacy to which the Supreme Court recently nodded in affirmative. Adding to it, hackers can get an enormous amount of data of different companies and individuals from the clond with a single attack known as "hyper jacking". Moreover through cloud computing India is becoming endemic to e surveillance in absence of dedicated laws. For example companies like Research in Motion through their cloud service provide e-surveillance to the Indian intelligence agencies.[177] Cloud service providers are obliged by law to hand over all the sensitive data of the user in case an order has been made by government or its agency without our consent and even without our knowledge. So one never gets to know what the government is looking for and what they extracted from the cloud.[178] We don't even come to know that a third party had accessed to our data.

Now let us look into the kind of laws we have enforced to make our cloud safer. Section 72 of Information Technology imposes a deterrent punishment for those who breach confidentiality and ptivacy of electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned to any other person.[179] Keeping in mind the urgency to develop some legal obligation over the cloud service provider especially to those service providers who deal with monetary transactions, Information Technology (Intermediaries Guidelines) Rules 2011 introduced the concept to due diligence requirements for the cloud service provider companies as well as the intermediaries to ensure that privacy is maintained and respected in the cloud so as to save the data stored in the cloud from any kind of unauthorized access.[180]

Though our statutes somehow attempts to secure our data on cloud yet these rules become redundant at the moment we sign a contract with the service providers. And the services providers can easily escape the rest of the charges like due diligence by simply showing that they did all that could have been done owing to

177 The Information Technology Act, 2008 § 72.

178 Vanya Rakesh, *Cloud Computing in India: The current Legal regime and the main Issues and Challenges*, http://www.indialawjournal.org/archives/volume7/issue 1/article3.html, (last visited Sept. 11, 2017).

179 Kasturika Sen, Privacy Issues in Cloud Computing With Reference To India (Dec. 4, 2013), http://www.moudaq.com/india/x/279070/Data+Protection+Privacy/Privacy+Issues+In+Cloud+Computing+With+Reference+To+India.

180 PILB, *Cloud Computing Legal Issues in India*, Perry4 Law Orgatization's Blog *(June 24, 2014)*, http://perry4law.org/cyberlawsinindia/?p=119.

the very nature of cloud computing environment. Contract of cloud computing are made in such a way that the user is left with no other option than to either accept all the terms of the privacy policy or not to use the service. A very little bargaining can be done by large organizations but small organization and individuals have no power to bargain on the privacy policies. The cloud service providers take advantage of their upper hand over the users and continue to trade on these terms only.[181] It has been seen that the issues relating to cloud computing are yet to be satisfactorily dealt by Indian laws as compared to other countries.[182] Cloud computing is a vehement no in government organization. Even Infosys and Confederation of Indian Industry have doubted the use of cloud computing for governmental projects and public services till suitable and appropriate safeguards are made in this respect.[183]

C.2. ISSUE OF JURISDICTION

Jurisdiction is the extent to which a certain power that can be enforced. The jurisdiction of the courts of state is limited within the boundaries of that state and, it is where the problems come in case of services that are received through the world wide net. Internet is huge network that has crossed all the borders and boundaries.

Many thinkers of the modern have commented that the network and its far and wide reach have diluted and if not diluted then, it has definitely posed a threat to the concept of the sovereignty of nations at least in the cyber space. In case of internet there has often, arose an ambiguity so as to which jurisdiction can apply in case of a criminal activity that occurs in inter twinkled web of data that is setup in multi-jurisdictional space. As the problem which always arise is that an act which is considered a crime in certain territory might not be a crime in the other therefore the law of lands which has been establish and working since ages seems useless in the cyber world.[184] When talking about jurisdiction three important elements exists which are firstly, the power to prescribe that is establish by law, secondly, the power to adjudicate that is exercise by the courts and thirdly, the power to enforce which is the application of compliance.[185] In case of cloud computing where the services

181 PTI.B, *Cloud Computing: Legal and Regulatory Issues in India* (Feb. 5, 2013), http://www.electroniccourts.in/blog/?p=617.

182 GeetaDalal, *Legal Framework For Cloud Computing In India*, International ICT Policies and Strategies(June 25, 2011, 4:17 AM), http://ictps.blogspot.in/2011/06/legal framework-for-cloud-computing-in.html

183 Alan Harris, *The Legal Standing of Data in a Cloud Computing Environment* (31 May 2012), www.comp.dit.ie/dgordon/Research/dissertations/AlanHarris.pdf.

184 Reeta Sony, *Data protection under cloud computing: a jurisdictional aspect*,Law Journal of Higher School of Economics, Dec 2013, at 81, 91.

185 HARRIS, *supra* note *15*.

are provided to the user who is in various corners of the world huge disputes arise regarding the jurisdiction to proceed with the legal action. The cloud computing is established as domestic and trans border clouds. In domestic system, the cloud is established within the jurisdiction of the same nation state it is also knowo as the mono-judicial system whereas in trans border system, the complete cloud system is not limited to one or same jurisdiction of a certain nation. Therefore, cloud computing including both national and international elements which gives rise to various questions like which law and which jurisdiction would apply to this huge amount of data that is broken into various parts and stored in storage center which can located anywhere in this multi-jurisdictional world .[186] The difficulties that arise in the cloud computing is that this data travel across that the net therefore it becomes very difficult to locate this traveling data and even if it is located another set of ptoblem that arise that to whom does this data belong, by whom is this data processed and who would be responsible for the data leakage and the security issues.[187] In cloud computing environment the cloud the user is in country A, the cloud service is based in country B, and the data center can be located in country C.

Usually the law of the country which receives the services is applied. Some of the recent issues that have come up are that, what happens when the data center is located in some country that does not provide adequate law for data protection, what happens in a country that does recognizes the user's right. There are multiple copies of the same data is made and if the service is over then which law govern theses copies and how are they destroyed are given back to user and in case of some natural disaster and what happens if there information leakage.[188]Therefore it shows that the just the national laws is not sufficient and there is need for global initiative to govern the cloud computing environment.

Presently the cloud user accepts the jurisdiction in case of conflict by clicking on the standard form contract, and in most of the cases the responsibility is on the user organization instead of the cloud provider. And in a research done it was found that 15 out of 31 big cloud providers does not mention the locatiou of the data center and what steps would be taken to protect this moving data.[189] Therefore the user origination should ptoperly negotiate with the cloud provider, which should include detailed clause for the jurisdiction, data protection and data ownership.

186 SONY,*supra* note *16*.

187 See *Id.*

188 W.Kuon Hon, Christopher Millard & Ian Walden, *Negotiating Cloud Contracts - Looking at Clouds from Both Sides Now*, 16 STAN. TECH. L. REV. 79 (2012) http://stlr.stanford.edu/pdf/cloudcontracts.pdf.

189 See *Id.*

C.3. ISSUE OF OWNERSHIP OF DATA

The ownership of the data on the cloud is also one of major concerns that have attracted huge attention. In reality, cloud is nothing but various servers that are housed on thousands of acre of facility that are owned by some multiple national corporate. Thereby storing the data on some computer to which we cannot have direct access.[190] When we agreed to store our data on the cloud, then basically agree to give access to your data to the third party. [191]The contention lies at the point where we believe that, as the data stored by us, therefore it belongs to us and we hold the ownership to it, but the cloud provider has the possession of the data so, now the question arises that does the cloud provider also holds ownership to your data. There are various arguments that as the data has been transferred therefore now the cloud provider has right to it as they the retainer of the data and secure them and the other argue that the only role played by the provider is of the care taker where he takes care of the digital data.[192]

There are two categories of data stored in cloud Firstly, the produced by the user before storing it on to the cloud and second category is the produced on the cloud itself.[193]

The ownership is governed by three kinds of law that is the contract, copyright and confidentiality and the details of these laws may be different according to different countries therefore data produced and stored in different countries are subjected to different laws.[194] The data that is produced before using of cloud service and then stored in cloud is subject to the copyright law of the country where they were created whereas when the same user created a new data on the cloud itself it is subjected to the laws of the countries where the data is stored.

There is problem when the laws of all countries might not be so advance in order to detect the nuisance of cyber world. There are laws of certain countries that are much strict to tackle the cyber nuisance and are capable of acknowledging the rights of the people in the virtual world as well. Therefore, when there is clash between the legal systems which are far away from each other in terms of their advancement issues are bound to happen. In this present state of confusion, all the

190 Rick Delgado, *The Ongoing Question of Data Ownership in the Cloud*, socPub Formerly CMS Report, https://www.socpub.com/articles/the-ongoing-question-of-data-ownership-in-the-cloud 13749 (last visited Aug10, 2017).

191 See *Id.*

192 See *Id.*

193 *Who owns the data?* , E-SCIENCECITY, http://www.cloud-lounge.org/who-owns-the-data.html (last visited Aug 15,2:00).

194 DELGADO,*supra* note 22.

right and duties concerning the cloud service comes down to the contract that is accepted by both the parties.[195] There are some providers that reserves all the rights to access the data with them only while some other reserve only certain rights in the data. There is also a practice where the provider reserves their right to the data as a way to lock in their client so that the user might not have an option to switch their cloud service. After entering into the contract power of negotiating with cloud provider lost and the contract is often more biased toward the provider.

The situation can be avoided by certain initiatives and by been more cateful while contracting. In order to avoid the hindrances due to different law and different parameters of sternness there should be a global initiative for a standard law for amount of ownership and authority that can be guaranteed by the cloud provider to their user.

The most important precaution that can be taken is to carefully analyse the terms of the conttact that is entered with the cloud provider. Careful consideration should be done, before accepting the following terms of the cloud contract.

Firstly, the contract states the procedure through which the data would be returned to the user at the termination of the contract or ending of the contract midway; the data should be in a format that is easily accessihle and commonly used by the user aud not in some inaccessible form; the contract should clearly define the time period within which, after the termination of the contract, the data would be made available to the user; the contact should mandatorily provide for the destruction of all the other copies of the data after the contract of service is over as well as the process and the time by which it will be done. In order to authenticate these actions there should also be a certificate of destruction should be given to the user. [196]

The solution to this problem is also given in the form of data cryptography which is science of writing and solving code therefore it basically can be used for secret communication. This data encryption should be used be by the secret key and not through the secrecy of algorithm.[197] By having the encryption service the user will have the right to audit the security and storage center of the data, the encryption can be used to provide notification in case of any security breach.[198] This ensures

195 Thomas J. Trappler, *When your data's in the cloud, is it still your data?*, COMPUTERWORLD (Jan 17, 2012 9:58 AM) PT https://www.computerworld.com/article/2501452/data center/when your-data s in the cloud—is-it-still-your-data-.html.

196 Ed Gelbstein, and Viktor Polic, *Data Owners' Responsibilities When Migrating to the Cloud*, 6 ISACA Journal (2014) https://www.isaca.org/Journal/archives/2014/Volume-6/Pages/Data-Owners-Responsibilities-When-Migrating-to-the-Cloud.aspx.

197 Patrick Gray , *Legal Issues to consider with cloud computing*, TECHREPUBLIC. (March 5, 2013), http://www.techrepublic.com/blog/tech-decision maker/legal-issues-to-consider-with-cloud-computing/.

198 GELBSTEIN, *supra* note 28.

that data is readable and accessible only by authorized people.[199] There are also certain concern related to the encryption as it increases the complexity and required cyber professional to establish this system.[200]

The hybrid model can also be solution to the problem of ownership in cloud computing. In hybrid model, a big enterprise can store the most important and critical data on their private cloud which is present on their premise and the less important data can be stored in the public cloud. Therefore, the ownership of the critical data is in tacked.

C.4. ISSUE OF CHANGE IN TERMS OF CONTRACT

Let's suppose that the customer being a vigilant one carefully kept an eye over all of the clauses and fetched for himself an appropriate and less risky cloud computing contract, but then he come to the last clause which mentions that the abovementioned contract terms can be changed at any point of time unilaterally by the cloud service provider. A large number of contract contained the terms providing that provider could amend the contract simply by posting an update of the service. No consent other than mere continuing to use the service is essential and would amount to a deemed acceptance. The cloud providers play very safely as they give a notice to the customers to check their lengthy and complex terms and conditions line-by-line. The providers do not even highlight the modified clauses nor do they even provide the date of revision. So one must be very watchful and need to constantly look up to the contract to see if the almighty cloud provider has done anything to it. If we take into consideration the law on this point, a valid modification can happen only if the parties to the contract give assent to the subsequent changes, if any party dissents, the changed modifications are not enforceable.

D. LEGAL FRAMEWORK IN SOME COUNTRIES AND INDIA

The issue that the legislation of most of the countries tackle in case of cloud computing is the privacy and security of the of the personal data and information of the user that is stored in the cloud service. Given below is major legislative framework adopted by some of the countries around the globe.

United States of America

There is still no direct law in America to protect the privacy of the people. Still the right to privacy of American citizens is protected through various other legislations. The law regulating the privacy depends upon the type of the private information that is breached therefore it information specific.[201]

199 See *Id.*

200 GRAY, *supra* note *29*.

201 15 U.S.C. §§41-58.

Under the Federal Information Security Management Act (FISMA), 2002 the US National Institute of Standards and Technology (NIST) have issued the guidelines to handle the privacy and security issues arising in cloud computing along with their safeguards.

Few other major statutes that govern privacy right are in USA

The Federal Trade Commission Act [202](FTC Act) – the deceptive or unfair practices are prohibited through this law. This law is used for online and offline data securities as well as privacy policies of USA.

The Financial Services Modernization Act [203] governs the use, disclosure and collection of financial resource and information.

The Health Insurance Portability and Accountability Act [204] it govern the medical information therefore applying pharmacies, data process and health care facilities and all the institution that have any medical data.

The HIPAA Omnibus Rule also revised the Security Breach Notification Rule[205] it provides for the notification in case of breach of any health care information.

The Federal Trade Commission regulate the business that use the cloud technique in storing information and it has also given report to bring about changes to accurately tackle the cloud computing issues.[206]

THE EUROPEAN UNION

The Data Protection Directive 95/46/EC regulated the privacy and security of the personal data of the EU while free transmission of data. It has following major features where the subject need to be informed about their data collection; he should be informed about the party collecting the data; he should be informed about the measures taken to protect the data from theft, misuse, loss; the sharing to data with third party should not be done without permission of the owner; the data should be used only for the stated purpose. [207]

202 Gramm-Leach-Bliley Act (GLB) 15 U.S.C. §§6801-6827.

203 (HIPAA) 42 U.S.C. §1301 et seq.

204 45 C.F.R. Part 164.

205 M.R. Sreenivasa Murthy, and Dr. K. Syamala, *Is India gearing up to face cloud technologies? Data privacy & security issues and regulatory framework in India, usacbrew,* 8 MLJ 2016 http://www.lexisnexis.com/in/legal/search/homesubmitForm.do#0||BOOLEAN||||.

206 Margaret Rouse, *EU Data Protection Directive (Directive 95/46/EC),* http://whatis.techtatget.com/definition/EU-Data-Protection-Directive-Directive-95-46-EC (last updated in Jan,2008).

207 MURTHY, supra note 37.

European Convention of Cyber Crime, the first international treaty on computers and Internet was adopted in the year 2001. This covers the following nuisance of cyber-crime like cyber fraud, data and system interference, illegal interception and misuse of the devices. [208]

Canada

Canada has a single legislation to govern the security and privacy of data which is the Personal Information Protection and Electronic Documents Act (PIPEDA) 2000. It is based on ten principle like consumer right to challenge compliance, accuracy , individual access, limiting collection, consumer consent, data safeguards, limiting use and retention and openness. It governs the personal data of the consumer that is held by private organization. [209] Canada has maintained office for privacy commissioner which acts as the national regulator for the data for the privacy issues.[210]

India

India has only recently started given importance to the internet intermediate liabilities therefore India hardly has any law in regulating it as compared to the western counties like USA , Canada, European union and many more.

According to consultation paper on cloud computing by telecom regulatory authority of India[211] following were the existing law which would protect personal information therefore help in data protection and privacy.

The definition of 'telecommunication service' given under section 2(k) of Telecom Regulatory Authority of India Act, 1997 can include the cloud computing which covers "service of any description that is made available to users by means of any transmission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, radio, visual or other electromagnetic means".[212]

The breach of privacy and security by cloud computing can come within Information Technology Act of 2000 which fixes the liabilities for the internet intermediary.

---

208 Understanding Canada's Private Sector Data Security Laws (PIPEDA & PIPA), varonis https://www.varonis.com/.(last visited Aug 12,3:00).

209 Alan Harris,*The Legal Standing of Data in a Cloud Computing Environment(31 May 2012),* www.comp.dit.ie/dgordon/Research/dissertations/AlanHarris.pdf.

210 Consultation Paper on Cloud Computing by Telecom Regulatory Authority of India, (June 10, 2016), www.trai.gov.in/sites/.../Cloud_Computing_Consultation_paper\.

211 See *Id*...

212 Akhil Deo, *How the Right to Privacy Judgement Will and Won't Impact India's Data Protection Regime,* THE WIRE (Aug 24, 2017), https://thewire.in/170689/right-to-privacy-data-protection/. .

Section 43 of this Act aims at the protection of the user computer system form database theft, digital profiling, unauthorized copying and extraction and it section 43A when read with the Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 protect the security of the personal information that is held and handled by a corporate and in case of any negligence in providing adequate security by the corporate, which results in any kind of loss or gain to any person then the body corporate would be liable to pay compensation to any affected person.

Section 65 of the IT Act provide the protection against the meddling of the computer source document like altering , destroying and concealing of the computer source code.

Section 66 of the Act, provides punishment up to three years of imprisonment and fine up to five lakh rupees or even both, for offence done under section 43 of the Act. In case of breach of the contract by the intermediary service provider like cloud computing which results in loss or wrongful gain of the personal information that is held by them, the punishment for such breach is given under the section 72A of the Act which imprisonment up to three years aud fine up to five lakh.

The Section 75(2) of the Act, provide for extra territorial jurisdiction whereby the offender can be liable whether he/she is within the Indian Territory or outside with condition the offence include computer system or network that is located in India.

On August 24, 2017 a landmark judgment on the right to privacy will pave new way for the data protection legislature in India. The Supreme Court in the case of ***Justice K.S. Puttaswamy (Retd) vs Union of India*** passed the judgment on making right to privacy as a fundamental right. This unanimous decision by a nine judge bench has not only protected the right to privacy in the physical world but also in the electronic and virtual world.[213] Even though the right is not absolute and all the restriction that is imposed on the Article 21 (that is right to life and personal liberty) are applicable to right to privacy as well. Yet this right can be used to protect the citizen of India against the arbitrary and unjustified breach of privacy in digital world by government or even private organization. The future of the data protection lies on how the interpretation of the judgment is done in the light of the present circumstances.

213 Akhil Deo, *How the Right to Privacy Judgement Will and Won't Impact India's Data Protection Regime*, THE WIRE (Aug 24, 2017), https://thewire.in/170689/right-to privacy-data-protection/. .

D.1. GLOBAL INITIATIVE FOR DATA PRIVACY AND PROTECTION

The first ever legal framework on global level for data protection was in the 1980, OECD Guidelines which aimed at protecting Trans boarder flow of data. More changes were brought to this guideline in 2013 when it acknowledged the basic value of privacy as well as the free flow of personal data as well as the intensity of risk associated with it. It recognized the need for better privacy framework and co-operation amongst nations for privacy protection. Certain principles recognized under it are Use Limitation Principle, Data Quality Principle, Collection Limitation Principle, Security Safeguards Principle, Accountability Principle, Purpose Specification Principle, Openness Principle, and Individual Participation Principle.

Another initiative was seen in the form of privacy framework by Asia-Pacific Economic Co-operation (APEC) in 2004[214], the basic aim for his regulation was toward the accountability the organization handling personal information.

E. CONCLUSION

Through this article, we can understand that the two major stakeholders involved in a cloud computing service are the cloud service provider and the end user whose rights and liabilities are dependent on the contract they enter. The issues arise out of the cloud computing contract mostly because the contract gives an upper hand to one of the party while ignoring the reasonable rights of the other one. Therefore, it is the need of the hour that a legal framework is drafted which is common to the countries of the globe because this menace cannot be tackled by the law of a particular nation owing to the very global nature of cloud computing. United Nation seems to be the appropriate organization for taking this initiative as it has the highest membership of countries of the globe. UN can pass a resolution containing the mandatory guidelines to be followed by each cloud service provider. Such a guideline would be the answer to every intricacies of cloud computing service. Every country signing the resolution would get connected in the group of countries which will have common law for cloud computing issue and thus would create a platform where the right and liabilities of the parties to the contract will be governed by some basic principles of justice and not just by the terms of contract. On the other side, countries who have not signed such a resolution will be blocked from providing its service ro this group of countries.

There are already groups such as Cloud Security Alliance (CSA) and Open Web Application Security Project (OWASP) who are gathering and analyzing information about cloud computing related standards from solution providers and individuals

214 *supra* note42.

to find out the best practices for the security of information on cloud.[215] OWASP also maintains a list of vulnerabilities to cloud computing service and SAS and keeps it updating according to the change in threat. Some of the already acknowledged solutions are given below[216]:-

1. Data access control will check the access control with the cloud service provider each time the service is used by the consumer.

2. Cloud service provider must check that the access devices are secured from malware and must be featured with advance authentication features.

3. The cloud service provider will provide every information and audit report if a query has been made by the user.

4. The cloud service provider should mention about the process as to how the data will be deleted from the cloud and such process must find a place in the contract so as to comply with it mandatorily. Also, they should verify the deletion of data from the providers each time the drive is abandoned.

Such a legal framework should be such that it creates a balance of interest between the providers and the customers so that the scope of cloud computing can be expanded. Moreover the framework should address the present issues and be wide enough to expand to cover the issues of future also. The customers should act prudent and vigilant while negotiating the terms of the contract and not just click "I agree" like any other click wrap agreement. Only then the hassle of cloud computing contract will be in control.

215 Prince Jain, *Security Issues and their Solution in Cloud Computing, conference I-Society, International Journal of Computing & Business Research*, http://www.researchmanuscripts.com/isociety2012/1.pdf.

216 Pathak, P B. Malware Growing Cybercrime Threat: Understanding and Combating Malvertising Attacks, 2016, International Journal of Advanced Research in Computer Science.

DATA PRIVACY - CONCERN OF DIGITAL WORLD

Akshat Shonak* and Himanshi Hans**

INTRODUCTION

Cybercriminals are constantly brilliant, quick, and unimaginably versatile and continually searching of traps and systems, chances to cause harm and bargain. Ransomware is a type of infection or malware that keeps or points of confinement clients from getting to their framework assets. The infection extorts amount via some online installment techniques in order to give entry in their frameworks, and recover information.[217] Criminals basically concentrate on the refinement of current devices and procedures. The threat is definitely advancing dynamically. Consequently, it becomes practically impossible for a user to understand the functioning of Ransomware and ascertain the most ideal approaches to prevent oneself from the attack. Versatile Ransomware assaults are relied upon in order to increment because of the relocation of business on convenient gadgets thus it ends up plainly fundamental we ought to have the capacity to recognize how, where, when, and why a danger works.

The exemplary growth of social media in the last decade has redefined the communication systems and framework via internet in the midst of individuals by captivating it to new level all together. The technological innovation has made it conceivable to go into a person's home without thumping their entryway and which is similarly conceivable in cooperation with the State and non-State actors.

LITERATURE REVIEW

Elisa Bertino (July 2015)[218] researched on "Agenda for security and privacy in big data" and addressed the problems related to confidentiality of the matter under the ambit of big data.

Dr.EnginKirda[219] "Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks" researched on the behaviours of some of the ransomware samples and concluded that apparently most of the ransomware types are basic.

* 4th Year, Amity Law School, Delhi (Affiliated to GGSIPU)

** 4th Year, Amity Law School, Delhi (Affiliated to GGSIPU)

217 Big Data "(BigData Congress), 2015 IEEE International Congress 2379-7703"

218 Amin Kharraz, William Robertson, Davidefbalzarotti, Leyla Bilge, "Cutting the Gordian Knot A Look Under the Hood of Ransomware Attacks"

219 Supra note 1

Dr.P.B.Pathak[220] "A Dangerous Trend of Cybercrime: Ransomware Growing Challenge" after analyzing the types and working of a Ransomware concluded the prevention mechanism.

RESEARCH METHODOLOGY

Being an informative and elaborative study, it depends on secondary information from scholarly work, writings, dally papers and magazines. Keeping in view the aims and objectives of the examination, an expressive methodology has been adopted to have more efficiency and thorough scrutiny of research work. The reachable secondary data is used for research study.

WHAT IS DATA PRIVACY?

Person, as citizens or purchasers require the mode in order to exercise their privilege to remain safe and prevent their files and data from being misused. To safeguard our local laws and traditional culture, data laws have been put in force so that information remains private and citizens remain secure.[221]

Data Protection laws have been enacted with the intent to protect our files and information and to prevent it from being a recording framework. In the present scenario, the only way to secure and protect our own data is that basic data protection laws curtail the powers and functions of the governmental organisations. The governmental organisations have emphasised that until the work of the citizens confine to their prescribed standards, they will continue to gather private information without the citizens even knowing about the same.[222]

NEED OF DATA PRIVACY

Every opportunity and interaction with an online server for exchange of information via purchase or enrolment some data is shared in the open space and data is therefore provided. This data is further manipulated by various organisations and companies who trap it unethically by data mining. Therefore, there is a severe need of an enactment aiming at information assurance and prevention by governmental organisation.

Since the 1960s and the extension of data innovation capacities, business and government associations have been putting away this individual data in databases. Databases can be sought, altered, cross-referenced and information imparted to

220 "Daniel Solove, 10 Reasons Why Privacy Matters published on January 20, 2014"

221 Christina P. Moniodis, "Moving from Nixon to NASA: Privacy 's Second Strand- A Right to Informational Privacy", Yale Journal of Law and Technology (2012), Vol. 15 (1), 159.

222 "Michael L. Rustad, SannaKulevska, Reconceptualizing the right to be forgotten to enable transatlantic data flow, 28 Harv. J.L. & Tech. 349"

different associations and over the world.[223] Once the gathering and handling of information wound up plainly far reaching, individuals began making enquiries about was going on to their data once it was turned over. Who had the privilege to get to the data? Is it safe to say that it was kept precisely? Is it accurate to say that it was being gathered and scattered without their insight? Would it be able to be utilized to segregate or mishandle other key rights?

From this, and developing open concern, information assurance standards were formulated through various national and global discussions. The German locale of Hesse passed the main law in 1970, while the US Fair Credit Reporting Act 1970 additionally contained a few components of information assurance. The US drove advancement of the 'reasonable data practices' in the mid 1970s that keep on shaping information insurance law today.[224] The UK likewise settled an advisory group around a similar time to audit dangers by privately owned businesses and arrived at comparable conclusions. National laws rose soon thereafter, starting with Sweden, the US, Germany and France. Encourage energy was included 1980 when the Organization for Economic Cooperation and Development (OECD) built up its security rules that included 'protection standards', and presently the Council of Europe's tradition came into constrain.[225]

Currently, there is a scenario of distrust and an urgent need of a robust mechanism or procedure is there in many countries with regard to their data in the hand of the government agencies. Contrary to this, about 100 countries have exceptionally worked to formulate the laws and rules for the regulation of data.[226] Albeit most nations have acknowledged information insurance is essential in chosen segments, they have not yet created far reaching information security law that applies to all business segments and to government.[227]

RIGHT TO PRIVACY

The right to privacy is an inherent fundamental right. This right secures the inward circle of the person from impedance from both Government and private individuals and enables them to take independent and self-sufficient decisions of their lives.[228]

223 "Michael L. Rustad, SannaKulevska, Reconceptualizing the right to be forgotten to enable transadantic data flow, 28 Harv. J.L. & Tech. 349"

224 "Samuel D Warren and Louis D. Brandeis, The Right To Privacy, 4 HARV. L. REV. 193 (1890)

225 Gary Bostwick, 'A Taxonomy of Privacy: Repose, Sanctuary, and Intimate Decision (1976) 64 California Law Review 1447."

226 "Jeffrey M. Skopek, Reasonable Expectations of Anonymity, Virginia Law Review (2015), Vol.101, 691-762"

227 "Richard A. Posner, Privacy, Surveillance, and Law, The University of Chicago Law Review (2008), Vol.75, 251"

228 (1973) 4 SCC 225.

The most obvious example of such principles being given effect is PUCL v. Union of India[229], in which the right to privacy was recognized in light of the "International Covenant on Civil and Political Rights 1966 (Article 17)[230]" and "the Universal Declaration of Human Rights 1948 (Article 12)[231]", to which India is a party, both of which recognise a right to privacy. The ICCPR specifically have explicitly mentioned the commitment upon the signatory states to secure the achievement of the norms. The judgment also finds it relevant that while becoming a party to the ICCPR, India had filed reservations against Articles 1, 9 and 13, however, no such reservation was filed against Article 17 and this indicates the acceptance of the right to privacy and a commitment to respect and protect it.[232]

In an article "privacy was described as having an image problem"[233]. It is contemplated, "old-fashioned at best and downright harmful at worst - anti-progressive, overly costly, and inimical to the welfare of the body politic"[234].

"When privacy and its purportedly outdated values must be balanced against the cutting-edge imperatives of national security, efficiency, and entrepreneurship, privacy comes up the loser. The list of privacy counterweights is long and growing. The recent additions of social media, mobile platforms, cloud computing, data mining, and predictive analytics now threaten to tip the scales entirely, placing privacy in permanent opposition to the progress of knowledge."[235]

Massive concerns are as of now winning as for the insurance of individual information and data, generally the privilege to one's security. The union of advancements has brought forth an alternate arrangement of issues concerning security rights and information assurance. Creative advancements make individual information effortlessly available and transferable.

229 "Article 17 of the ICCPR states:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks."

230 "Article 12 of the UDHR states: The Right to Privacy. Nobody should try to harm our good name. Nobody has the right to come into our home, open our letters, or bother us or our family without a good reason."

231 "Report of the Group of Experts on Privacy (16 October, 2012), Government of India, available at http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf".

232 "Julie E Cohen, What Privacy Is For, Harvard Law Review (2013), Vol. 126, at p 1904"

233 Ibid.

234 Ibid, at pages 1904-1905.

235 VrindaBhandari and Renuka Sane, "Towards a privacy framework for India in the age of the internet", October, 2016, http://macrofinance.nipfp.org.in/PDF/BhandariSane2016_privacy.pdf.

DATA (PRIVACY AND PROTECTION) BILL, 2017

Open talk around data protection is most likely at its apex in India today. In the Supreme Court, a nine-judge bench has also declared Right to privacy as a fundamental right of the privilege to life of a person under Article 21 of the Constitution of India. In the mean time, individual from Parliament Baijayant Jay Panda tabled the Data (Privacy and Protection) Bill, 2017 in the LokSabha as of late, proposing the privilege to security as a crucial ideal for Indian natives.

This isn't the first run through a Bill proposing such a privilege has been set down in Parliament. Panda himself had introduced a Bill going back to 2009, titled "The Prevention of Unsolicited Telephonic Calls and Protection of Privacy Bill", which went for restricting spontaneous phone calls by business promoters or people to people who would not like to get such calls. It expressed that each individual should have the independence to security and flexibility to lead and make the most of his existence with no unjustifiable encroachment.

The "Data (Privacy and Protection) Bill, 2017", stipends a legal Right to Privacy under Section 4 of the Bill. Be that as it may, this Right to Privacy is just in accordance with Articles 19 and 21 of the Constitution. Even though a legislative acknowledgment of the Right to Privacy might be cheered on being an infant footstep the correct way, it is basic to welcome the threats of connecting with Fundamental Rights under Articles 19 and 21.[236]

Nonetheless, it is indispensable to take note of that this Bill applies to private organizations or body corporate, as well as is similarly relevant to state elements, government offices or some other people following up for their benefit. Indeed, even the meaning of an "outsider" under this Bill incorporates people in general experts. This symbolizes a noteworthy transformation in legal setup from the current administration within the current "Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011" ("SPDI Rules").

The Bill additionally aims to make more efficient the information insurance administration in the country by giving an inclusive system and proposes the making of the "Data Privacy and Protection Authority". This specialist will go about as both the controller and adjudicator of debate emerging from the Act and will likewise have the ability to start suomoto activity against an information processor or controller. All the more importantly, the Bill proposes to overridingly have an effect on the "Information Technology Act, 2000", and the "Telecom Regulatory

236 Bowen, B. M., Hershkop, S., Keromytis, A. D., Stolfo, S. J. "Baiting inside attackers using decoy documents", Springer, (2009).

Authority Act, 1997", and some other enactment tending to the accumulation, handling and capacity of individual information.

Further, as per the definitions given in Section (2) of the Bill, the two information processors and information regulators are characterized, giving clearness on who holds information. Be that as it may, the Bill does not recognize the commitments or liabilities between information processors or information controllers. The Bill additionally has a squeezing midpoint around the well-informed and clear-cut assent by a man giving individual data. With regards to sensitive and individual data, the individual must give his or her express and positive assent for the capacity, utilize, preparing of any such information.

Section 10 of the Bill includes the "Right" to look for taking out of information. This Right to look for procuring of information will force a more prominent obligation on information processors/regulators who are to expel the information given inside the fixed period. The production of such a Right is liable to awesome level headed discussion, as saw with regards to the Right to be overlooked with regards to the European Union. Further, this Right is liable to specific constraints, for example, shielding open intrigue or in encouragement of a Judicial Decree.

Section 14 of the Bill expressed that "while giving consent", the individual might have a "reasonable expectation" that the information controller/processor will comply with the arrangements of this Act, who must take all safety efforts essential for shielding such individual information with "due diligence". While the goals of the Bill are to give a man a well being net against information insurance ruptures, it is basic to clarify the trouble in coordinating such guidelines of assurance as digital assaults and information burglaries keep on evolving, regularly leaving existing safety efforts repetitive. This might lead to conduits of case. The Bill likewise presents the idea of pseudo-anonymisation of information, so a man can't be distinguished utilizing such data without the utilization of extra information. In any case, pseudo-anonymisation is failed to command but rather is just "empowered", expanding escape clauses particularly with regards to assurance of touchy, individual information.

Under Section 36 of the Bill, no individual can assist or direct inspection of a man. Notwithstanding, an exception is created for state organizations, conditional on specific confinements and earlier support by the DPPA. The time span for putting away such information should be decided and no information which is not any more vital for the Government organization ought to be collected to following 365 days from the DPPA's endorsement which guarantees the Government does not forget about a man's entitlement to security ceaselessly. On a comparable note,

individual profiling has been denied by the Bill and any occasion of profiling would add up to an attack of a man's Right to Privacy. Be that as it may, concerning delicate, individual information, Section 20(2) of the Bill gives that, no sensitive information might be prepared for some other reason separated from its planned utilize yet can be utilized by welfare plans and social insurance laws. Thus, this would suggest that the Aadhaar plan of "BHIM (Bharat Interface for Money)" would likewise approach a man's close to home, delicate data.

Ultimately, the Bill made all offenses within the arrangements cognisable offenses and has expanded all money related punishment and detainment time span for all current ruptures. Further, the idea of applying a high fiscal punishment on an every day premise, in light of amount of days of infringement of information security), has been forced, to guarantee defaulters are compelled to take fitting measures to cure the break on an auspicious premise. Subsequently, while this Bill presents a couple of much-required changes as far as growing the extent of materialness information insurance laws and perceiving the Right to Privacy, such euphoric arrangements are similarly shadowed by areas that empower use of delicate, individual information for welfare plans, in this manner forcing statutory impediment on the Right to Privacy. However, what stays certain is that an adjustment in the current system is the need of great importance and if late occasions are characteristic of this transformation, change is practically around the bend!

Highlights

- One of the important features is that the Bill has characterized phrasings and in addition "forms" like information handling, and profiling of people.
- Clearness of definitions is one of the fundamental territories of worry around laws in India, as definitions have frequently been abused for implementing the state's power by empowering clear speculations.

For instance, Section 66A of the Information Technology Act, which was revoked by the Supreme Court in 2015.

- The bill takes after a rights-based approach and commands the assent of a person for accumulation and preparing of individual information.
- The tabled charge communicates that the last proper way is to change or oust singular data from any database, paying little respect to whether open or private, rests only with the individual.
- All the more critically, the "exemptions" against this privilege are characterized barely, accommodating a case-by-case thought.

- The bill obliges the generation of an end customer standing up to position of data affirmation officer for grievance redressal, with a course of action for offer to the Data Privacy and Protection Authority (DPPA).

RANSOMWARE AS A THREAT TO DATA PRIVACY

Ransomware primarily targets and endeavors to blackmail the clients with the objective to gain monetary benefits. The basic power of tainting the victim's machinery, the records and even the archives by bolting the device or the computer either by encoding or encrypting, puts the malware in a dominant and prime position. The extortion is sought by the majority either through a content record or sometimes in the form of site page of the web program.[237] It is by this mode that a person is exposed to humiliation and dread to deliver the extortion.

Ransomware is malicious software that blocks access to computer system and threaten to publish the victim's data unless huge random is paid. Modern ransomware families include crypto ransomware which encrypts your data. For instance, the attack on May 12, 2017 which had used 'Wannacry' ransomware appeared to be massive attack in the cyber world.[238]

It serves as a method and a medium of Income generation by way of encrypting and encoding the individual information furthermore, documents on Pc and Locker Ransomware locks the PC or gadget, keeping casualties from utilizing them.

It is a type of malicious software that blocks access to the victim's data or threatens to publish it until a ransom is paid. It has become the most damaging threat that the user interface has faced. Each attack uses specific malware which is more enhanced and have much effect on the system. This can be best seen by comparing the previous attacks.[239]

237 "Carrier, B. File System Forensic Analysis, Addison-Wesley Professional, (2005)"

238 "Prince, B. CryptoLocker Could Herald Rise of More Sophisticated Ransomware, http://www.darkreading.com"

239 "MattiasWecksten, Jan Frick, Andreas Sjöström, Eric Järpe, A novel method for recovery from Crypto Ransomware infections, Computer and Communications (ICCC), 2016 2nd IEEE International Conference."

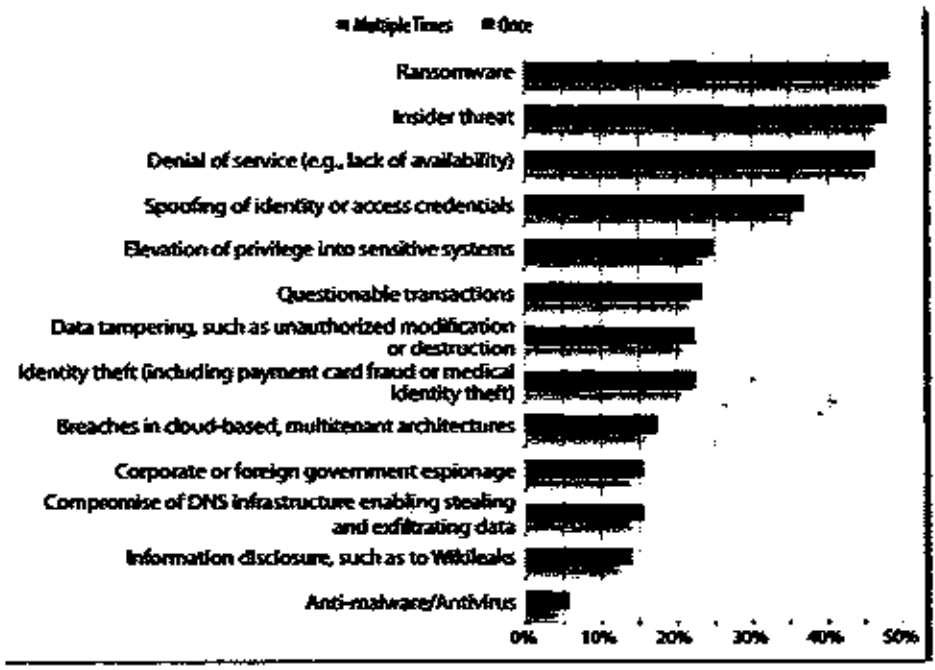

Figure 1. Top threats to Sensitive Data

The first asymmetric Ransomware prototype was developed during mid 90s. The idea of using cryptovirology for attacking the system was introduced by Adam L.Young and Moti Yung in the 1996 proceedings of the IEEE Symposium on Security & Privacy. Even though the first prototype of malwares for ransom was publicized, it had logistic problems due to which they were traced and arrested but the chain continued for another attack and this time they were successful in their getting huge ransom.[240] Due to this, the attacks increased rapidly, influencing the cyber world. The scam has evolved in past years enhancing their techniques to lock the computer systems.

Ransomware which locked the computer for the first time was seen in Russia in 2009, before which the Ransomware were used for the payment for decryption key. The next Ransomware used another technique by displaying the pornographic image and demanding huge ransom to remove that image from their system. The payment was done through messages. This shaming activity made this attack a successful as huge ransom was retrieved from the users.[241]

240 "Heater, B. (2016, May). How ransomware conquered the world. PC Magazine Digital Edition, 109-118".

241 "Nikolai Hampton, Zubair A. Baig, Ransomware: Emergence of the cyber-extortion menace,"The Proceedings of [the] 13th Australian Information Security Management Conference, held from the 30 November - 2 December, 2015 (pp. 47-56), Edith Cowan University Joondalup Campus, Perth, Western Australia."

Due to the threat of publication of the record of inappropriate activities done by the user of the computer victim would easily pay the ransom to the attacker. The last change made to this technique was changing the mode of payment. They got into digital money named as 'bitcoins'.

The creative instinct of the cyber criminal is to make the danger of Ransomware pertinent and that one can be exposed to it in an assortment of manner. One of the major ways is the downloading by uniformed clients through going to pernicious or traded off sites. Ransomware assaultes regularly utilize stratergies like entrusting pornographic content on your screen to request you pay a pay-off to expel the explicit entertainment.

TIMELINE

Though ransomware concept was introduced in 1990s, the attackers used different methodologies as all the attacks their own methodology of attacking the system. GP code was related to torjan encryption which matches the code of the user file extension. Cryptowall was noticed after the downfall of the famous Cryptolocker. Cryptowall uses I2P network proxies for communicating the live command for favoring the bitcoins as bitcoins just were introduced by crypto locker.[242] Torrent locker is a family of file encrypting data using spam emails and easily being geographically targeted.

Initially, the victim receives an infected mail link which contains a malicious link or malware which leads to an infected web page. If the victim clicks ok on the link then at the backdoor the malicious activity gets started and pc gets affected. The downloader uses a list of domains to download the ransomware. The contacted link responds by sending the requested data back to the victim. The malware then encrypts the hard disk and useful content stored on the victim's PC. Then a warning screen appears showing that your data has been encrypted, and to pay the ransom for decryption key.[243]

Exploit kits does not require interaction from the victim but do require the vulnerable software to be installed in the victim's computer. They are most inexpensive if rented but if it hosted it can be gained.

Malwares work on cryptoviral extortion which erases public as well as private keys, as public key allows the malware to perform trapdoor one-way operation on victim's computer that can only attacker can undo. It achieves "end-to-end

242 "Hiran V. Nath and Babu M. Mehtre, Static Malware Analysis Using Machine Learning Methods,International Conference on Security in Computer Networks and Distributed Systems, 2014."

243 "Bhardwaj, A., Avasthi, V., Sastry, H., &Subrahmanyam, G. V. B. (2016). Ransomware digital extortion: A rising new age threat. Indian Journal of Science and Technology, 9, 14."

deniability".[244] The functioning of the Ransomware fosters it to falsely and unknowingly lead the operator to send of the asymmetric key to the attacker.

The malware prompts user to send asymmetric key to attacker who will decipher it and return the symmetric decryption key for free but the victim needs the symmetric key to get the files back if there are no backups of them.

In order to secure the monetary benefit from the infected or the compromised system Botnets and Downloaders are brought into use. These acts as distribution agents of the malwares. Once the malware infects the computer after entering it further installs the secondary malware in to the system to render it dysfunctional.

WANNACRY: RANSOMWARE ATTACK

On May 12, 2017 this attack has stricken around 104 countries, it has been one of the largest cyber attacks. Over 200,000 computer systems were affected.[245] In lieu of decrypting data Wannacry demanded around $300-$600 in bitcoin.

The feature of the Ransomwarewannacry to jump and spread form Pc to Pc within the computer from the same network was exposed by anonymous group "Shadow Brokers". Therefore the spread of the malware extended via exploiting the known vulnerability in the operating system.

The most affected countries were:

- USA
- UK
- Japan
- Italy

The process of execution was in three steps: the vulnerability of main file was ensured so that Wannacry may get entry, the installation and then getting it run in the victim's system.

But the vulnerability of this attack was limited to new version of Windows as Window XP, Windows 2003 were outdated one so over there the attack was not possible.[246]

244 "Nolen Scaife , Henry Carter, Patrick Traynor , Kevin R.B. Butler. "CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data",2016, IEEE 36th International Conference on Distributed Computing Systems"

245 "Solander, A. C., Forman, A. S., &Glasser, N. M. (2016). Ransomware—Give me back my files!.Employee Relations Law Journal, 42(2), 53-55".

246 "Kharraz A., Robertson W., Balzarotti D., Bilge L., Kirda E. , "Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks"". In: Almgren M., Gulisano V., Maggi F. (eds) Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA. Lecture Notes in Computer Science, vol 9148. Springer, Cham, 2015."

The dialogue box appeared this time had automated features of timings as the timings were increasing the bitcoins demanded were increasing as time limit for specific no.ofbitcoins,with geographical targeted which means the message were displayed in victim's language likewise if the victim was from Russia the message displayed was in their native language which was more consulting.

There are six steps in which Ransomware accomplishes its goals:

Figure 2.Ransomware cycle

Firstly through spam emails and attachments the distribution process takes place. As user opens the spam mail the malicious activities get started in the system. They may include several steps. Then the attackers start to search the encrypt server files for encrypting the public key afterwards it searches the important data to be encrypted and further it displays the message of demanding the ransom.[247]

At this point the user has no choice other than paying the ransom to get back the data.

247 Lin Liu, "Security and Privacy Requirements Engineering Revisited in the Big Data Era", *Requirements Engineering Conference Workshops (REW) IEEE International*, pp. 55 55, 2016.

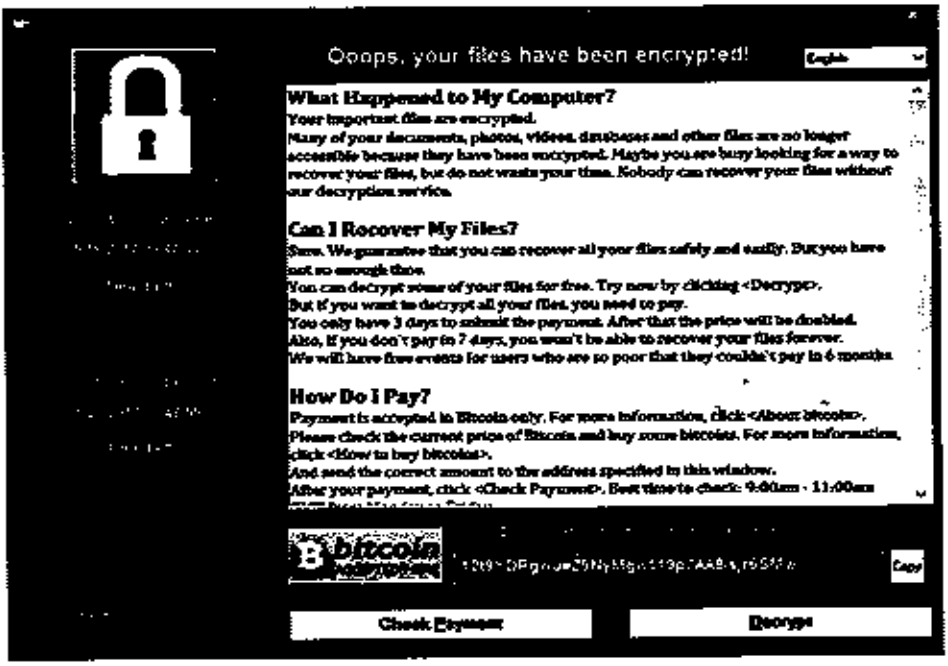

Figure 3.Displaying the ransom message

The recent attacks has set the time limit that means after certain period of time the ransom may increased if it is not paid at time. Due to this advanced technique used in this recent attack the profit has also increased by 67% than the usual previous attacks which made it most disastrous attack in the cyber world.

REMEDY

The most recent pattern in cybercrime is the Ransomware assault—programmers bring an infection into a framework which closes down the objective's PC, at that point the programmers request cash to discharge the framework. Ransomwares mostly targeted individual's pc as they don't have backup of their files. They also target institutions like school, colleges, hospital to retrieve the data and encrypt it to get ransom. They attack on home users due to lack of cyber knowledge, more prone to manipulation of attackers, less online safety awareness, no updated softwares, rely exclusively on antiviruses and rely on luck to keep them on internet. They attack on organization's data due to that's where money is. They know successful attack can destruct the organization due to which they can easily pay the ransom. Their systems are more prone to vulnerabilities which can be exploited easily. They know that organization will not file case in cyber security as their loss and brand name will get affected. Staff is not trained to spot the attack at public institution Ransomware does not only affect system but also servers and cloud based file sharing system causing huge damage. The current WannaCryransomware

assault brought down PCs in Europe, America, and Asia, before being thwarted by a malware pro.[248] Regardless of critical notices from the FBI and cyberwarfare masters that "there is no hope" against ransomware assaults, organizations and individuals can find a way to limit harm and constrain introduction to these new dangers to keep up information security In order to prevent such damages following things can be done:

1. Keep up malware/spyware consistence. Ransomware is commonly brought into PCs as a trojan infection, by downloading tainted malware or spyware. Guaranteeing that representatives obey organization prerequisites against downloading any outside projects that could contaminate the corporate intranet.

2. Debilitate or keep workers from exchanging information from outside PCs through blaze drives or other USB gadgets, particularly business gadgets. Streak drives are typically not encoded, and are effortlessly contaminated with malware and spyware. In the event that remote access is fundamental, representatives ought to be given organization USB document sharing gadgets, or other encoded frameworks.

3. Move down all records routinely and in different organizations. Despite the fact that reinforcements are not really secure from a trojan assault, a disconnected reinforcement will keep organization data in a safe area that will permit a brisk reestablish if the framework is traded off.

4. Encourage correspondence amongst representatives and IT. One of the quickest approaches to address conceivable information interruption is for representatives to will and ready to admit to IT they have coincidentally downloaded an amusement, or got to a website they ought not to have. In the event that representatives fear conceivable disciplinary activity by revealing potential breaks, the IT division will never know about it until the point that it is past the point of no return.

5. Ensure updating your operating systems and softwares around the date. Spam messages should not be opened and backup of the data should be done to prevent giving the ransom.

6. Abstain from visiting unsafe and non reliable websites: also be cautious while clicking on harmful links. Do not visit unsafe and unreliable websites. Use reputable security suites.

248 INDIAN CONST. Art. 19(1)(a), All citizens shall have the right to freedom of speech and expression.

CONCLUSION

Considering that the universal group respects the right to privacy and security as a fundamental right, the country might be under a good and additionally lawful commitment to authorize protection and informarioo insurance controls. There exist two ways through which controls are received: "Self-direction and Government direction"

- ***Self-direction*** – The country will consider advancing an activity in the midst of its ventures, particularly the ones keen on development of web based business. Self-control by the business guarantees upside of an adaptable approach prepared by the individuals who are aware about the exchange hones and are roused by the want of clients. Self-control is additionally fetched effective to the administration, as implementation components require not be built up. Iu any case, a vast and heterogeneous gathering of operators may make self-control troublesome. In any case, there is likewise the hazard that self administrative arrangement is set the most reduced standard.
- ***Government Regulation*** - Alternatively, the government can receive particular enactment to deal with security and information insurance problems. Indeed, even nations like the US that have principally adopted a self-administrative strategy in order to achieve secure internet usage nationwide.

Ransomware has resemblance to the false applications stating themselves as antivirus applications which are mostly fake in nature. This has subjected the end users in the past few years to believe in misleading antivirus applications making their estimated earning to millions of dollars. The spread and expansion of Ransomware has begun from the Russian speaking nations and it further evolved in the Western Europe, Canada and United States. The established criminal gangs have played a vital role in its expansion over the years.

Therefore the profitable market of this fraudulent malware is likely to increase. It is probable that there might be clashes between the conventional malware distributors and Ransomware gangs. Ransomware being an evident malware forces the computer user to reboot the machinery severely in order to eliminating any sort of malware. With the evolution of more sophisticated mechanism for the prevention and detection of such malwares in form of Ransomware the operational business model will experience a dent.

GOOD GOVERNANCE AND TECHNOLOGY: THE STORY OF CONVERGING FACTORS AND INDIAN DEVELOPMENT

Siddhant Asthana[*] and Vanya Chaturvedi[**]

ABSTRACT

'Governance', in its broadest and truest sense, is a word profoundly and prominently used and yet seldom correctly comprehended. It is the hallmark of an ideal democracy and the foundation stone of a great nation. Add to it the phenomenon of technology and you beget a nation unprecedented and unparalleled. Ideal governance has been the catchphrase for development across the world and no nation has impeccably equipped itself for the contemporary times without the aid of technology. India is no exception to the same. For a booming nation of 1.324 billion, ideal governance is the key to stand out in today's international front.

This article is an attempt to highlight the due importance of technology in the modern day governance system of India. It seeks to analyse the intrinsic relation between technology and good governance in the modern-day Indian governmental setup. Through the analysis of vital statistics, data and recent case studies, the article seeks to put forth the successes and failures of India's technological advancements in the light of e-governance. Varied facets of governance like law and order, health services provided by the government, tax related systematization, educational and awareness related technological advancements would also be significantly dealt with. The article will also highlight how the technological developments and innovations have raised concerns like ethical issues and threat to privacy and need for more stringent action by the government. After analyzing the key shortcomings and successes of governance mechanism, the article would outline the future course of action to be contemplated and implemented in this regard. Doctrinal mode of research is to be used to substantiate the study and outline recommendations in this regard.

KEYWORDS: India, governance, e-governance, technology, recommendations

INTRODUCTION

"Technology plays a critical role in modern society. Everyone is touched by the power of technology in some way, large or small, good or bad, everyday."

-Mackenzie and Wajcman (1999)

* 4th YEAR STUDENT, B.A. LL.B. (HONS.), AMITY LAW SCHOOL, DELHI

** 4th YEAR STUDENT, B.A. LL.B. (HONS.), AMITY LAW SCHOOL, DELHI

Technology in today's fast-paced era is not merely a word, but indeed, a way of life. It is that indispensable force that has transformed lives and connected every nook and corner of the world. Nothing seems to be a distant dream now as a mere click can open up varied arenas for one. Be it Face time with your near and dear ones or shopping the latest fashion trend. Technology has got one's back anytime, always. You game, you chat, you laugh on memes and you book tickets to the most exotic destinations. All of this has become possible courtesy the leaps and bounds taken in the advancement of technology.

It remains undoubted now that no modern day governance system can be said to be effective and complete without the aid of technology. Information and Communication Technologies (ICTs) play a pivotal role in the development & economic growth of India. Political, Cultural, and socio-economic developmental and behavioural decisions today rest on the ability to access, gather, analyze and utilize information and knowledge. ICT is the conduit that transmits vital information and knowledge to the individual to widen their perspectives thereby transgressing economic and social empowerment. India is the fastest growing economy of the world; as a government it has an ambitious objective of converging the citizen-government interaction from mere snail-paced and paper-based methods to electronic modes of governance (e-Governance) by the year 2020.

The idea of governance is not only to rule the masses and strengthen the state against foreign enemy as it used to be in the ancient times. The ideals of democracy, social and economic justice and mixed economy are those which have been changing the contours of governance over the years. Citizens all over the world wish a high-quality governance with expectations of enrichment in their personal and general pursuits. The concept of "governance" is not new. It is as old as the human civilization and spans centuries. It has transcended into varied manifestations with the changing times. India is a country of villages and much of its population dwells in rural India. Thus, to improve and sustain the overall ptosperity, growth and development in the global competitive regime, there is a need to bridge the gap between the urban and the rural India. Sevetal e-governance plans over the years have been demonstrating the role of Information and Communications technology in providing the best of development in India. Some of the schemes undoubtedly have improved the services and the shift towards an e-government has proved to be boon for the government and the citizens.

The concept of "governance" is not new. It is as old as the human civilization and spans centuries. It has transcended into varied manifestations with the changing times. Simply put "governance" means: the process of decision-making and the process by which decisions are implemented (or not implemented). In this new era,

governance is not only limited to the state players and the citizens and communities are equally involved in changing the landscape of governance.

A government is said to follow the path of good governance when it is transparent, accountable, effective and efficient, equitable and inclusive, participatory and consensus oriented, equal opportunities to every majority and minority communities, low level of corruption and rule of law is followed. ICTs are crafted to enable Electronic Governance through wireless communication and are intrinsically interlinked and knitted. A successful ICT application in e-Governance giving one-stop solutions for rural community is the need of the hour.

Thus, in the changing times, it is important for an ideal governance system to adapt to the needs of the era and only then can it sustain a great nation. The convergence of governance and technology is a vital one and without a union of the two, development would still be a far-fetched dream. The onus thus being not merely being reaching out to the urban, but, being essentially on amalgamating the rural alike.

This paper further expatiates and elaborates upon the interface between the information and communication technology and the governance.

E- GOVERNANCE: REVAMPED OUTLOOK TO GOVERNANCE

Globalisation and technophile behaviour of the world population led to a change in how the population is to be governed. The use of computer technology not only helped in governance but also helped in eradicating a few issues that piled up because of the advancement of crimes by the use of technology. For the fulfilment of the goal of good governance we resorted to an offspring of Information and Communication Technology and governance which came to be known as E-governance.

Basically E-governance, stands for 'electronic governance', which means using information and communication technologies (ICTs) at various levels of the government and the public sector and beyond, for the purpose of enhancing governance.[1] According to Keohane and Nye (2000), "Governance implies the processes and institutions, both formal and informal, that guide and restrain the collective activities of a group. Government is the subset that acts with authority and creates formal obligations. Governance need not necessarily be conducted exclusively by governments. Private firms, associations of firms, nongovernmental organizations (NGOs), and associations of NGOs all engage in it, often in association

1 K BEDI, P.J. SINGH, S. SRIVASTAVA, GOVERNMENT @NET: NEW GOVERNANCE OPPORTUNITIES FOR INDIA, Sage Publishers, New Delhi (2001).

with governmental bodies, to create governance; sometimes without governmental authority." Clearly, this definition suggests that e-governance need not be limited to the public sector. It implies managing and administering policies and procedures in the private sector as well.[2] "Governance refers to the exercise of political, economic and administrative authority in the management of a country's affairs, including citizens' articulation of their interests and exercise of their legal rights and obligations. E-Governance may be understood as the performance of this governance via the electronic medium in order to facilitate an efficient, speedy and transparent process of disseminating information to the public, and other agencies, and for performing government administration activities."[3] Dr. APJ Abdul Kalam, former President of India, has visualized e-Governance in the Indian context to mean: "A transparent smart e-Governance with seamless access, secure and authentic flow of information crossing the interdepartmental barrier and providing a fair and unbiased service to the citizen."[4]

It has now become a very indispensable part of governance in any of the world economies. Due to the globalisation process there was a demand of clarity in administration and rapid/instant data and information exchange by the people and organisations were pushed to change to electronic means for the success in their endeavours. In consonance with the same there emerged a need to innovative use of technology in governance as well. The advantages attached to e-governance are manifold, like improved access to services, data management, easier data mapping, decreased operational costs, enhanced co-operation between government agencies and other organisation or the people of the country. The application of ICT in governance generates huge potential for interplay between different organisations in the developing countries. The whole idea is to simplify the administration of the country for all parties- government, citizens and players and acts as a support for achieving good governance and often termed as smart governance.

According to an administrative reforms commission report e-Governance initiatives[5] implemented in past few years can be categorized into the following:

- Government to Citizen (G2C) is an initiative which aims at extending the reach of governance to have a major impact on the people at large.

2 Shailendra C. Jain Palvia and Sushil S. Sharma, *E Government and E-Governance: Definitions/ Domain Framework and Status around the World*, http://www.iceg.net/2007/books/1/1_369.pdf.

3 *Defining E-governance*, UNESCO Web Archives, http://webarchive.unesco.org/20161021003528/http://portal.unesco.org/ci/en/ev.php-URL_ID=4404&URL_DO=DO_TOPIC&URL_SECTION=201.html.

4 Inaugural address at IIT Delhi during International Conference on e-Governance.

5 *E Governance Initiatives in India*, The Hans India,http://www.thehansindia.com/posts/index/Young-Hans/2016-02-01/E-Governance-Initiatives-in-India/204109.

Projects taken in this direction are Computerization of Land Records (Department of Land Resources, Government of India), Bhoomi Project: Online Delivery of Land Records, Gyandoot, Lokvani Project, e-Mitra Project, Project FRIENDS, eSeva, Revenue Administration through Computerized Energy (RACE) Billing Project, Admission to Professional Colleges – Common Entrance Test (CET) etc.,

- Government to Business (G2B) is an initiative which deals with activities of government which impinge upon business organizations. The objective of bringing activities like registrations, licenses and exchange of information between government and business under e-Governance is to provide an amiable legal environment to business, speed up processes and provide relevant information to business. Some of the projects are e-Procurement Project, e-Procurement, MCA 21, etc...

- Government to Government (G2G) is an initiative which deals with large scale processing of information and decision making within government systems. This initiative has been taken to help in making the internal government processes more efficient. Some of projects are Khajane Project in Karnataka, SmartGov (Andhra Pradesh), etc... [6]

ICTs: SECTORAL ANALYSIS

Education Sector

The incidence of technology in the education sector has been a premier addition and has also emphasised that learning is not that difficult as it seems to be. Introduction of methods and tools which advance student learning in the education process has been helping the people since long.

One can recall of the cave paintings that were used as a method of teaching during early civilisation. Few decades earlier also documentaries and educational films have been used to educate people. The use of audio-visual learning techniques like streaming of videos, power-point presentations have taken away people from books to a large extent by providing ease and the influential learning effect they have. Just like everything else has been affected by the advancement of technology, the education cannot be indifferent to it. The education shifted from books to computer and now from computer to smart-phones and one cannot deny that these mind-hacking devices have expurgated the need of books and note-books to a substantial extent. India has become the second largest market for smart-phones

6 *Ibid.*

trailing just behind China[7] which shows the extent to how influenced the Indian minds are with technology.

But all of this has barely helped India achieve a feet in the education rankings. The poor condition of education can be understood by the fact that India came 92nd among 145 countries when it comes to education. This shows that there is a lot to be achieved. Even as the previous government tried to bridge the digital divide, Modi's masterstroke offers a lot of positivity for the Indian education market which is estimated to be worth Rs 5.9 trillion in 2014-15 against Rs. 3.33 trillion in 2011-12. With nearly half the population of India below the age of 25 and increasing penetration of Internet and mobile devices in this demography which is expected to reach 250 million soon, rivalling the US and second only to China, India's potential as a huge market for e-learning is enormous.[8]

Given below are some of the uses of technology in the Education sector:

1. **Distance Education-** The students or working professionals can learn courses through online access and can even interact with the faculty from far distance remote locations For people in remote areas where education is a dream this can be of help. A report released by the Ministry of Human Resource and Development states that the total enrolment of students for Distance education constitute of 11.7% out of which 46% are female students.[9]

2. **Classroom based learning-** nowadays even the classroom study is not limited to books and notebooks. The classes are now turning into smart classes with the use of projector blackboards. Gadgets like the laptops and the tablets are being used to take down notes and the handwriting of the teachers are replaced with the power-point presentations.

3. **Learning through mobile applications-** nowadays there are a lot of e-learning services which can be availed on your mobile phone by just downloading an application in your Android/IOS/Windows phone. Newspapers, IAS preparation Classes, dictionary, NCERT books are just a click away when you have the applications installed in you phones. One can access them anytime and at any place without many hassles.

7 The Hindu Net Desk, *India now second-largest smartphone market in world*, The hindu(OCTOBER 30, 2017), http://www.thehindu.com/sci-tech/technology/india-now-second-largest-smartphone-market-in-world/article19926744.ece.

8 Ms. Swati Yadav, Dr. Anshuja Tiwari, *E-Learning in Rural India* , IJSET, http://www.ijset.in/wp-content/uploads/2016/06/P-10.pdf.

9 Dept. Of Higher Education, MHRD, *All India Survey on Higher Education 2015 16*, http://mhrd.gov.in/sites/upload_files/mhrd/files/statistics/AISHE2015-16.pdf.

There are many more contemporary ways in which technology is bringing a change in the education system but that is sort of out of the scope of this paper.

The Indian Government too has come up with the Digital India Initiative. Almost every sector has high hopes from the Digital India initiative, which is extensively based on faster communication facilities such as National Optical Fibre Network and adoption of Internet enabled devices such as smart-phones and tablets. The government of India focussing upon Digital India initiative is trying to put in the E-model of education in the higher Education. "When the country is adopting digital in most sectors, keeping education away is not the right approach. Pure online courses—adopted and aided by Indian institutes—will push quality higher education to the masses," said a human resource development ministry official.[10]

The official said the promotion of massive open online courses (MOOCS) was the first step and it was time to take the initiative forward. In the past year-and a- half, the government has asked top Indian institutions to develop MOOCS on various subjects for supplementary knowledge. These are in the nature of short-term, subject-specific capsule courses, available online to all.[11] Indian has 799 universities, 39,071 colleges and 11,923 stand-alone institutions catering to around 30 million students. Despite the size of the sector, the gross enrolment in higher education is just 24%, way below leading economies. With limited government spending on education, online education could spur the sector.[12]

Health Care Sector

"The health of people is the foundation upon which all their happiness and all their powers as a state depend"

-Benjamin Disraeli, British Prime Minister

In the health sector, we have observed many changes over the past few years. The hospitals and the clinic are getting more and more digitalised to provide the best of services to the patients and other stakeholders. This portion of the paper does not focus upon the role of technology in inventing equipments and devices which are used in surgeries and other medical processes but focuses upon the role of information and communications technology (ICT) in the health sector and how beneficial it has proved over the years.

The storing of information in the digital form, the accessibility of the same, and

10 Prashant K Nanda , *Govt framing policy to push online education*, Livemint (Wednesday, Jul 05 2017), http://www.livemint.com/Education/nxBcHtzdIEC3fhA3P25f3J/Govt-framing-policy-to-push-online-education.html.

11 *Ibid.*

12 *Ibid.*

the amount of ease that it provides can't be denied The data and the systems once digitalised are helpful to the people from outside the conventional care centres to fulfil some basic needs like fetching various test-reports. Rapid communication via e-mails and patient portals, retrieving of lab-reports via websites, online consultation, online medical records, online medicine supply, pan-India exchange for patient information, etc, are all a part of the E-healthcare scheme.

Worldwide use of computer technology in medicine began in the early 1950s with the rise of the computers. In 1949, Gustav Wagner established the first professional organization for health informatics in Germany. Health informatics also called Health Information Systems is a discipline at the intersection of information science, computer science, and health care. It concerns with the resources, devices, and methods required for optimizing the acquisition, storage, retrieval, and use of information in health and biomedicine.[13]

Tele-healthcare can be defined as the use of ICT to support the delivery of health care directly to people outside the conventional care centres. This can enable health related information in the web, create PPP model, help customer contact, allocate patient to different level of health care, provide electronic forum for patient interaction and build e-prescription system. It is high time to explore how doctors and IT personnel can work together to reduce health care cost, deliver high quality service and cover rural mass.[14]

The introduction of the telemedicine hubs in the health-care sector to provide medical facilities to people in the remote areas has been a very crucial move. The World Health Organization (WHO) defines Telemedicine as, "The delivery of healthcare services, where distance is a critical factor, by all healthcare professionals using information and communication technologies for the exchange of valid information for diagnosis, treatment and prevention of disease and injuries, research and evaluation and for the continuing education of healthcare providers, all in the interests of advancing the health of individuals and their communities."[15] This came as a boon for people covering long distances and spending money on travelling and accommodation for the treatment. In the past the Union ministry also signed a memorandum of understanding (MoU) with ISRO to expand its telemedicine

13 Asian Hospital Healthcare And Management, https://www.asianhhm.com/articles/role information-technology-medical-sciences.

14 Subash Chandra Mahapatra , Rama Krushna Das and Manas Ranjan Patra, *Current e Governance Scenario in Healthcare sector of India, Computer Society of India(E-journal)*, http://www.csi-sigegov.org/egovernance_pdf/15_121-127.pdf.

15 Aparajita Dasgupta and Soumya Deb, *Telemedicine: A New Horizon in Public Health in India*, Indian Journal of Community Medicine, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2782224/.

network to remote places and pilgrimage centres.[16] Initially this tele-health service was proposed to be in the field of medicine, orthopaedics, respiratory and cardiology disciplines. Some states have also individually tied up with private players under the public-private partnership (PPP) model. "Himachal has tied up with the Apollo Group and they have nodes running successfully in Lahaul and Spiti. They consult their own specialists and the model is working fine", said Jitendra Arora, director (E-Health), Health Ministry.[17]

Health Sector is one of those sectors which is most impacted by the Digital India move of the Indian Government. Technology can solve a lot of problems that exist in this sector like- lack of Information/knowledge about various health schemes, access to various health services, transparency in the implementation of various schemes, knowledge about the stocks in the hospitals, etc. Recently the Uttar Pradesh government announced the digitisation of some government hospitals where registration to all reports will be available online, also keeping an eye upon the stocks of oxygen and medicines available at each hospital. The Digital India move fosters the goal of a healthy India.

With the storage of information of the patients, the pattern of a particular disease/ health in a particular area can be easily assessed and essential steps can be taken to eradicated the problem or improve the situation. But, it's not always a positive impact. There are also various issues that have arisen with the increasing technological shift in the health sector. This will be discussed later in the paper. The government is also planning to bring a legislation regarding the e-health services which will include provisions for data privacy, security, comprehensive remedies (civil and criminal) for data breach and enforcing nodal body.[18]

Law Enforcement Sector

The enforcement of law in a State majorly depends upon the functioning of the Police of the State. The Police department is the one which provides security to the people from the crimes and criminals and maintains Law and Order in the society. So, they need to be trained in such a way and equipped with such tools and technologies that they can identify, restrain and regulate the activities of the people in order to promote the peaceful living in the society. With the crimes getting more

16 Rythma Kaul, *With 105 centres, govt spreads telemedicine network across country, Hindustan Times*, http://www.hindustantimes.com/india-news/with-105-centres-govt-spreads-telemedicine-network-across-country/story-U1OwyqZRniQOjzJg9MOzk8I.html.

17 *Ibid.*

18 *Government set to bring out e-health legislation*, Economic Times, https://economictimes.indiatimes.com/news/politics-and-nation/government-set-to-bring-out-e-health-legislation/articleshow/55620788.cms.

complex with involvement of several technological instruments and methods, the importance of technology in policing cannot be overlooked.

Information and communications technology has caused everything from business to governance to change and so policing cannot be kept far from its influence. With the increase in awareness and role of media in today's society and increased pressure from all the stake-holders in the society for prevention, detection and investigation of crimes, the only resort is to shift to more innovative policing methods by the inclusion of information and communications technology. The use of wireless radio, CCTVs, tracking soft-wares and tools, and phone-tapping are well known instruments used for modern day policing. Police can use a number of other methods for detecting crimes and identifying criminals, like-

- Any electronic communication by the person can be used for his electronic identification. E.g.- Digital signature of a person, bank account, PAN, e-mail accounts, IP addresses etc.
- The Biometric technologies and fingerprint readers can be used to identify and trace the criminals and suspects. Even a lot of online verifications these days use the fingerprint scans.
- Social networking sites and mobile application like Twitter, Whatsapp and Facebook and others are being resorted to connect with people for giving information about crimes and trace the criminals.
- In a large geographical area which is very hard to check and administer, the Global Positioning System (GPS) and Geographical Information System (GIS) are used to track the information about a particular area and movement of suspected persons and terrorists etc. with the available data and video. The available information provides the ability to coordinate all the activities for better tracking, reporting, and taking action[19].
- E-Police will help to built citizen confidence. The first step to using ICTs would be in the interface of police with the public. Police is the body to secure the life and property of the public. Through ICT public will be able to view information regarding status of their complaints and the police will be able to provide feedback on the same.[20] The feature of Online FIRs has been a boon to people for reporting incidents of mobile, laptop, and other small thefts and lost cases.

19 Balbir Kumar, *Role of Information and Communication Technology In Indian Police*, 1 GIAN JYOTI E-JOURNAL, Issue 2 (Jan – Mar 2012) , http://www.gjimt.com/N6.pdf.

20 Ibid.

- The use of Big Data and increased interest in crime analytics, which involves storing and analyzing huge volumes of information in real time, helps in identifying the areas which are prone to crimes.

Several initiatives have been introduced in the past to leverage IT in police functioning. Some of these initiatives include centrally initiated programs such as the NCRB-led CCIS (Crime and Criminals Information System) and CIPA (Common Integrated Police Application), and State-led initiatives such as e-COPS (in Andhra Pradesh), Police IT (in Karnataka), Thana Tracking System (in West Bengal), CAARUS (in Tamil Nadu) and IID ITTS (in Gujarat).[21]

CCTNS Crime and Criminal Tracking Network & Systems (CCTNS) is a plan scheme conceived in the light of experience of a non-plan scheme namely - Common Integrated Police Application (CIPA). CCTNS is a Mission Mode Project under the National e-Governance Plan (NeGP) of Govt. of India. CCTNS aims at creating a comprehensive and integrated system for enhancing the efficiency and effectiveness of policing through adopting of principle of e-Governance and creation of a nationwide networking infrastructure for evolution of IT-enabled-state-of-the-art tracking system around 'Investigation of crime and detection of criminals'.[22]

Further, the Cyber Cells have been established to put a check upon the cyber-related offences as there is a substantive increase in the cyber offences and Police Personnels and specially trained to tackle these new generation crimes.

CONCERNS/CHALLENGES FOR E-GOVERNANCE

Through this paper the idea is to present the cons of the introduction of technological instruments and methods. But, there are always two sides of a coin. So there are also many issues or concerns that have arisen due to the dependence of the government departments upon the information and communications technology. Some of the issues or challenges are enlisted as under:

Trust Deficit-India as a country has a very tarnished image in the field of corruption and misuse of power or authority among its own population and citizens. For a government to implement its e-services there are two stages involved. First is the coming up with schemes and the second is the participation of the masses towards the successful implementation of the schemes. The user must be confident in, trusting and comfortable with the different tools and techniques the government is coming up with that any information that is provided to the government can't be

21 *Crime and Criminal Tracking Network & Systems (CCTNS)*, National Crime Records Bureau, http://ncrb.gov.in/BureauDivisions/cctnsnew/index.html .

22 *Ibid.*

used for any fraudulent transactions which can be of a detriment to the user in any way. Recently, the making of Aadhaar compulsory has been criticised upon by a large amount of Indians as Aadhaar is not being a fool-proof method of storing information by the government. The fear of misuse of data is still keeping away people from the Aadhar project.

Resistance to change- In a country where lynching happens over carrying meat, opposition to sex education for preservation of culture are a common, a change in the mindset of people is very difficult to be brought to shift to an electronic mode of working

Digital divide- Digital divide refers to a substantial symmetry between two or more population in the distribution and effective use of information and communication resources.[23] TRAI data recognises that while urban India has 61.9 Internet subscriptions per 100 people, rural India gets by with just 13.7.[24] India being the country with highest number people living below the poverty line this divide seems a very difficult one to be bridged. Not only financial problems but also the unawareness among the people of various government initiatives and schemes keeps the divide alive.

Privacy and Security-There will be three basic levels of access exists for e-government stakeholders: no access to a Web service; limited access to a Web-service or full-access to a Web service, however when personal sensitive data exists, the formation of the security access policy is a much more complex process with legal consideration. With the implementation of e-government projects, effective measures must be taken to protect sensitive personal information. A lack of clear security standards and protocols can limit the development of projects that contain sensitive information such as income, medical history.[25]

Inadequacy of technical advancement- It is a general connotation that the criminals/wrongdoers stay one step ahead of the police and the enforcement authorities. Even newly brought up project of Aadhaar has got frauds accorded to its profile.[26] The crime can be detected and the criminals can be busted but the effects of the crime cannot be erased once the crime has been committed. The

23 Ipsita Panda , Durlav Charan Chhatar , Bulu Mharana, *A Brief View to Digital Divide in Indian Scenario,3* International Journal of Scientific and Research Publications (Issue 12, Dec. 2013), http://www.ijsrp.org/research-paper-1213/ijsrp p2471.pdf.

24 Aarati Krishnan , *How many Indians have Internet?,* The Hindu, http://www.thehindu.com/business/how-many-indians-have-internet/article17668272.ece.

25 *E-governance in India: Concept, Initiatives and Issues,* http://www.insightsonindia.com/2014/11/23/e-governance-india-concept-initiatives-issues/.

26 Omar Rashid, *Fake Aadhaar card network busted in Kanpur,* The Hindu, http://www.thehindu.com/news/national/uttar-pradesh-police-busts-fake-aadhaar-card-network/article19660140.ece.

government initiatives need to compulsorily equipped with clear security standards and protocols so that the sensitive information like the medical history, bank account details, biometrics of the people can be safe.

Aadhaar: An exemplary case study

Aadhar has been one of the most controversial steps of the present government in the field of storage of citizen's information with the government authority (the UIDAI). Reason for selecting this project was that apart from being a very positive step of the government towards the good governance goal, this project has raised a lot of security issues in the minds of Indians. As a result a lot of opposition to making Aadhar compulsory and linking it with other systems has been observed.

The whole idea behind the linking of aadhar is to keep a track of the financial activities of each and every individual to keep a check upon the frauds, corruptions and illegal activities. It was used as an identity proof for getting benefit from a lot of government schemes such as:

- Aadhaar based Direct Benefit Transfer (LPG Subsidy)
- Jan Dhan Yojana
- Passport in 10 days
- Digital Locker
- Voter Card Linking
- Opening new bank account
- Digital Life Certificate

But it raised a grave *Privacy Concern*; the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Bill, 2016 was passed with no public consultation about the privacy safeguards for the information stored as database. A lot of Aadhar based transactions are dependent upon the thumbprints and in the past we have heard of people creating replicas of thumbprints for illegal activities[27]. Then the next concern is over 'personal integrity' which is under threat when one has to share his information which will be available to institutions with which they don't want to share with. The databases which are stored with the UIDAI can be used for permanent surveillance of the residents without invoking any special powers. This impedes upon the right to privacy of individuals guaranteed by our

27 Musab Qazi , *You will be glued to this: Mumbai college's students trick biometric system*, Hindustan Times, http://www.hindustantimes.com/mumbai-news/you-will-be-glued-to-this-mumbai-college-s-students-trick-biometric-system/story-W64f1jdMtccxKDml2Dakel.html.

constitution. Repeatedly the Aadhar data breaches have been occurring[28] and the Act is very weak to tackle the issues arising.

This project is an example of how the glitches occur in an E-governance mechanism and the need to be more cautious with the data storage and transfer in every e-scheme the government is coming up with. The mere resort to e-governance is not the solution but also there should be thoughtful analysis of possible issues that may arise. A whole fool-proof mechanism is needed for such projects to be functional and successful.

CONCLUSION

With E-governance mechanisms being built in the India the call for 'minimum government and maximum governance' is getting louder. As mentioned in the article the importance of Information and Communications Technology (ICT) in governance is increasing day-by-day. India's efforts towards reaching even the most remote areas and successful implementation of its policies needs a lot of more efforts to be put in to remove the hurdles like the Digital Divide. In a country where education is a distant dream in many remote areas, the internet facility is still not available in many places, and e-governance preparedness is less, lot more efforts need to be put in, As earlier mentioned, there also needs to be certain level of protection and cyber security that has to be assured before any more e-governance policies are brought in. Absence of the privacy laws and data protection laws has already raised concerns over many e-government initiatives. Apathy towards these issues cannot lead to a good-governance system and for development of a country like India, every effort put in towards improving governance has to coincide with the general concerns of the population.

28 *Right to privacy a fundamental right: 7 Aadhaar controversies that raised concern,* Hindustan Times, http://www.hindustantimes.com/india-news/right-to-privacy-a-fundamental-right-7-aadhaar-controversies-that-raised-concerns/story-UGTtXhgJDtaWrmyuli2LwO.html.

ISSN 2249-4421 UGC Approved Journal No. 42016

ROLE OF TECHNOLOGY IN FACILITATION OF COMMERCIAL ARBITRATION

Vivek Sharma*

ABSTRACT

International commercial arbitration is considered to be El Dorado for lawyers all over the world. When issues, irrespective of their complexities, arise between parties, they essentially want to put an end to all the disputes and in order to do so, submit them to arbitration, usually because of the binding nature of the arbitration agreement, which was entered into before the parties started dealing in business. This paper succinctly describes the relationship between humans, technology and dispute resolution mechanism. It also throws light on the dynamic aspects of human interactions with innovations and making the reader realize the indomitable spirit of innovations that the people are believed to have in all the previous generations.

As disputes are ever-arising, the alternate dispute resolution mechanism is described in detail. It entails the reason and procedure as to why people go for arbitration and what is the procedure to do the same. The differences are also noted between litigation and arbitration with a special focus on the party autonomy. The way the two proper laws and the curial law works in international commercial disputes is explained by keeping in mind the categorisation of arbitration into domestic and international.

The research paper discusses in detail the merits of using technology in arbitration and also how it facilitates the whole process. Video conferencing and quick chat applications are examples discussed in the research paper which can substantially reduce the cost of arbitration and also ease the whole process of communication between the concerned parties. The benefits of transferring of data through the medium of internet are discussed. Author describes how super-fast translations can reduce the cost of arbitration and would make it less time consuming

The research paper also discusses the demerits of using technology in arbitration by giving various real life examples of cyber-attacks, data breach and round the clock surveillance by wire-tapping. The risk of losing confidential data by the use technology is articulated by discussing the case of China's planted code of data breach at the website of the Permanent Court of Arbitration. The author concludes by remarking the importance and the need of the hour of using technology to resolve disputes between the parties but also makes it clear that the substantial ease which technology provides may come at a cost of losing confidential information.

* 2nd YEAR B.A.LL.B. (HONS) STUDENT, AMITY LAW SCHOOL, DELHI.

INTRODUCTION

The very basis of any creation by humans is technology. Technology has been known to humankind as a measure through which lives of the people become smooth and efficient. Initially, technology was developed when humans started interacting with their environment and using the available materials in a sharper and accurate manner through which the daily life became very well-organized. However, with time the humans started experimenting with creativity and invented magnificent entities. This is the reason why in every century people thought that they are living in the most advanced centuries of all time as they inherited the already invented items and started working with the available resource (technology) to help bring in more progressive and proficient entities into being. That is why they say that technology is anything that wasn't around when you were born.

WHAT IS ARBITRATION

Arbitration is one of the mechanisms through which disputes are resolved between two parties. It is essentially different from litigation in terms of the autonomy given to the parties when the disputes are either anticipated or are being arbitrated upon and also on the basis of appointment of the adjudicatory body. These are the main reasons why arbitration is known as an alternate dispute resolution mechanism. Many important practices of litigation are not followed in arbitration. However, the principles on which these practices or procedures of litigation developed, are followed in arbitration and at times these principles are of indispensable nature.

Arbitration is purely based on mutual understanding and cooperation. It requires a formal agreement which has to be entered into before the arbitral proceedings start and that is the reason why arbitration is of contractual nature, unlike litigation, where there is not an agreement to settle the disputes. Both the parties agree to arbitrate only when they both find some benefit in doing so and this is the reason why arbitration leads to a win win situation, not in terms of its end result or final order like in mediation but it may so happen that the parties do not want to litigate the matter and want the dispute to be resolved in a manner where the parties weak points or strategies are not set to be known to the public. In international commercial arbitration, very often than not, the companies which agree to arbitrate are facing stiff competition from other companies in the market and they want to resolve the dispute without making their strategies or weak points known to their competitors.

Arbitration is less formal than litigation and the parties have the freedom to choose the laws which would govern the whole process. Essentially, commercial arbitration agreement specifies three kinds of law which would govern the whole process. Firstly, proper law of the contract, which is the law that governs the contract

entered into between two parties. Second, the proper law of the arbitration agreement, which is the law that governs the arbitration agreement alone and not the contract even if the arbitration agreement is in the form of a clause entered in the main contract. Thirdly, the curial law or *lex arbitri* which is the procedure which governs the arbitration proceedings.

According to the Arbitration and Conciliation Act, there are two types of arbitration – domestic and international. The domestic arbitration is done between two parties when both the parties are Indian and when either of the parties is non-Indian then that arbitration is termed to be international in nature.

Hence, the three laws mentioned in the arbitration agreement gains importance in international commercial arbitration as the party of one country may not want the disputes to be resolved through the laws of the country where the other party is situated, and they can choose the law which suits both of them. This the reason why party autonomy is given due recognition and acceptance in arbitration as it helps to resolve disputes according to the mutual understanding of the parties. Moreover, the parties can also choose a law that none of the countries in which the companies are situated follows. For instance, a French and a German company may make an arbitration agreement where the law agreed upon to be followed is British.

Party autonomy is the guiding principle in determining the procedure to be followed in an international commercial arbitration. It is a principle that has been endorsed not only in national laws but by international arbitral institutions and organizations[1]. The parties' freedom to agree on an arbitration regime of their choice and to prescribe the procedure to be followed is subject to few limitations. The arbitration agreement must be a valid one according to the law which governs it. This will usually be the law governing the substantive contract, in which the arbitration clause is embedded, but is not necessarily that law. The possibility of dépeçage arises because the arbitration agreement is regarded as a separate agreement to the substantive contract in which it is contained[2].

Efficiency and feasibility of using technology in arbitration

The innovations made by humans have helped technology to be considered as an ever-growing field. The truth which everyone is aware of is that ever-evolving technology has both merits and demerits. Merits of using technology are that it is

1 REDFERN AND HUNTER, WITH BLACKABY AND PARTASIDES, LAW AND PRACTICE OF INTERNATIONAL COMMERCIAL ARBITRATION, 4th Edition.

2 FOUCHARD, GAILLARD, GOLDMAN, INTERNATIONAL COMMERCIAL ARBITRATION 212 (Edited by Gaillard and Savage)(1999).

cost efficient as less labour needs to be employed for the production of the desired output by the producer.

It leads to easy access to information as today the internet provides humongous data on almost everything and it also influences behaviour and reactions of the majority community by providing cheap access to information. It encourages innovation and creativity as more and more people use the available technology to create more and to create it efficiently. This is evident from the fact that the new sector of the economy, which is tertiary, is essentially based on skills which can only be demonstrated, exhibited and honed only by using technology which is created in the recent past.

Improved communication

Improved communication is again a merit of using technology. The considerable improvement of communication is purely based on the will and desire of the people who innovate and also on the demand for it. In today's world, a person can easily communicate to another person with substantial ease and convenience. Quick chat applications such as WhatsApp and Facebook messenger have made Email to be considered as an old technology used as a means of communication, which is now mainly used in formal communications.

Convenience of travelling

Another merit is the convenience of traveling both physically and virtually. The longest flight in terms of distance covers 14,200 km and takes about 17 hours which is again an achievement[3]. Virtually a person can be present anywhere in today's world because of video conferencing. The first concepts of video conferencing were developed in the 1870s, as part of an extension of audio devices.

The first actual developments of the video telephone began in the late 1920s with the AT&T Company, Bell Labs and John Logie Baird. AT&T expetimented with video phones in 1927. Early video conferencing expetiments took place in the late 1930s in Germany. This early video technology over phone lines included image phones that would send still photos. AT&T began using video conferencing for its picture phone service in the early 1970s[4].

The above-mentioned merits of technology can also be realized when latest technology is used in arbitration for dispute resolution. From the beginning when

3 *Emirates A380 from Dubai to NZ makes longest non-stop flight*, BBC NEWS, Mar. 3, 2016.

4 *The history of Video Conferencing*, BUSINESS MATTERS, Jan. 8, 2015.

the agreement of arbitration is entered into to the final award given by the tribunal, latest technology usage would result in efficient and convenient arbitration for both the parties as well as the arbitrators.

Travelling to a different country is expensive. It becomes a burden on the company to first hire a lawyer for the adjudication of disputes and then to send the lawyer as well as the other persons of the company to witness the arbitral proceeding. It doesn't stop there. It includes the expense of living in a different country and many times the tribunal sits in intervals of months due to which the company has to bear the expense of traveling and living in a different country. This is of course only possible in international commercial arbitration when the parties have decided to go to a neutral place to arbitrate or when one of the parties is at the venue of the arbitration.

The above-mentioned problem can be solved to a reasonable extent by using video cooferencing for certain people who are expected to be present in the arbitral proceedings. For example, if two parties are arbitrating and both the parties don't live at the venue of the arbitration, then they can send their lawyers and legal consultants to the arbitration venue and can view the arbitral proceedings through video conferencing. Such a move can be of immense benefit to the parties whose arbitration is happening with long intervals. This will substantially reduce the cost of arbitration for the parties. Almost all the institutional arbitration centres have audio and visnal conferencing facilities including the MCIA[5] and DAC[6] in Mumbai and Delhi respectively.

The testimony of witnesses can also be taken through the above technology which again has the potential to reduce the cost to a substantial extent. This may happen when two parties have many disputes lined up before the arbitral tribunal and the reasonable step in such a situation is not to send the witnesses to the venue of the arbitration to record their testimony, but to make use of the easily available technology that is audio and video conferencing by which the testimonies can easily be recorded.

Transfer of files and data through software

The tribunal which sits for the arbitration of the dispute may not necessarily be qualified in the field in which the dispute lies. This is because customarily the tribunal is more of a judicial body and looks into whether the essentials of dispute resolution mechanisms and the rules of arbitration of an institute are followed or not.

5 http://mcia.org.in/premises/facilities/.

6 http://www.dacdelhi.org/topics.aspx?mid=1.

Hence, the tribunal appoints professional analysts, who try to quantify the damage or loss to a party and make it more understandable to the tribunal as to what are the intricacies involved in the process of quantifying such damage.

However, this is not the only job of the analysts as they also help the tribunal to comprehend complex practices which are undertaken by the parties to do business, of which, some are intrinsic alone to a particular field or task. The analysts make use of the technology available to simplify the complex problem and present it in a manner which is easily comprehensible.

Many disputes which go for international commercial arbitration are complex in nature and require gigantic files to be transferred to both the tribunal and the other party in the dispute. To print all the relevant files would be time-consuming and costly as they have to be couriered to the party. Technology can help make this task easier and less time consuming as there are numerous websites which help in transferring these files through a software for a nominal charge.

DETRIMENTAL EFFECTS OF TECHNOLOGY ON ARBITRATION

Cyber-attacks

Law firms and chambers of the lawyers have an enormous amount of information about the clients and act as repositories of their clients' data and documents. Customarily, a law firm is expected to follow a code of conduct while dealing with clients and which is the reason why communications that a law firm has with its clients are ordinarily covered by privilege or a duty of confidentiality.

As the people who deal in arbitration are often associated with a law firm as well, it is expected that these people would keep the conversations private and confidential which they have with their clients including the conversation which happens not face to face but through some other medium with the help of technology such as email, telephone and text messages.

When the lawyers deal in arbitration it is very likely that they are a target of cyber-attacks. This is done in order to get controversial and confidential information. Cyber-attacks usually happen when the arbitration is about to end and the final order has to be given by the tribunal. This is because over the period of arbitration all the information which is collected is examined by the tribunal and a draft award is drafted. This way only the most confidential, dispute irking and controversial information is separated from the rest and that the hackers have to attack once to steal the draft award. Hence, arbitrators have to be careful before opening any particular site or even an email when using their official laptops.

A 200 law firm study[7] released by Logic Force (a cybersecurity consulting firm) found that all firms had been subjected to hacking attempts. The Logic Force survey revealed that 40% of firms were actually unaware of the hacking attempts until the study was conducted and corresponding investigations made. Further, 95% of firms were not fully compliant with their own data governance and cybersecurity policies and only 23% had an adequate cyberattack insurance policy in place.

However, lawyers and their law firms are not the only targets of cyber-attacks. The arbitral institutions which are now present in almost every commercial hub of the world are also the prime victims of cyber-attacks. These institutions do not upload anything on their websites such as the names of the parties, nature of the dispute or the arbitrator's name. However, they still remain prime targets. This is because the website of these institutions have other important information which the lawyers regularly have to check and keep themselves updated.

The hackers plant technical codes to get all the available data on the person's laptop whenever he visits the website. As the depository of sensitive data, institutions are highly exposed to cybersecurity risks, including in terms of reputation management and compliance with the rapidly evolving regulations. In July 2015, the website of the Permanent Court of Arbitration in The Hague was hacked during a hearing of a sensitive maritime border dispute between China and the Philippines. The website was implanted with a malicious code that posed a data breach risk to anyone who visited a specific page devoted to the dispute[8].

An interesting case which happened in the International Centre for Settlement of Investment Disputes arbitration was that one of the parties was the Republic of Turkey and had contracted with a private entity. In the duration of the arbitration, the Republic of Turkey started using its police and intelligence agencies to tap the phone calls of the lawyers and the directors of the private entity. The matter got wide attention from around the world and showed that technology can also be used in a manner which is prejudicial to the interests of the other party. When the issue of wiretapping and surveillance was raised before the tribunal, the tribunal started investigating the matter. In the circumstances, the tribunal observed:

like any other international tribunal, [the Tribunal] must be regarded as endowed with the inherent powers required to preserve the integrity of its own processes — even if the remedies open

7 Law firm cyber security scorecard, https://www.logicforce.com/reports/detail/cyber-security-q1.

8 Claire Morel de Westgaver, Kluwer Arbitration Blog, *A Necessity And An Opportunity For Arbitral Institutions, Cybersecurity In International Arbitration*, http://arbitrationblog.kluwerarbitration.com/2017/10/06/cyber-security/.

to it are necessarily different from those that might be available to a domestic court in an ICSID Member State . . . . Parties have an obligation to arbitrate fairly and in good faith and . . . an arbitral tribunal has the inherent jurisdiction to ensure that this obligation is complied with; this principle applies in all arbitration, including investment arbitration, and to all parties, including States (even in the exercise of their sovereign powers)[9]

Nevertheless, the tribunal declined to grant the draconian sanction of "summary judgment" requested by the claimant. Instead, it accepted the host government's assurances that no privileged information had been misused, and fashioned a series of orders essentially intended to ensure that this remained the case[10].

Job Loss

New technology is thrilling, but we shouldn't let that veil the fact that we work in an industry built on people. In a law firm, apart from representing the case before a court or tribunal, there are numerous other things that a lawyer does and that makes the profession more competitive, difficult and bustling. The life of a lawyer is considered to be difficult and busy because the very essence of honing one's skills in the field of law is to research, debate and articulate which is not only time consuming but also requires a long span of attentiveness.

However, with developing technology the work of a lawyer is anticipated to decrease and with a decrease in work, the very demand for the workforce will also decrease, rendering many people jobless. Around 114,000 jobs in the legal sector are likely to become automated in the next 20 years as technology transforms the profession. Automation, changes in the demands from clients and the rise of millennials in the workplace will alter the types of skills sought after by law firms, according to the new study by Deloitte which predicts a tipping point for law firms by 2020. Technology has already contributed to a reduction of around 31,000 jobs in the sector including roles such as legal secretaries, the report said, as it predicted that another 39 percent of jobs are at "high risk" of being made redundant by machines in the next two decades"[11].

Yet with rising legal costs and clients who are increasingly unhappy with the length of time an instruction may take to complete, new technology is paving the way for the use of artificial intelligence in law, promising to produce answers to legal questions in half the time and at half the cost to clients. Artificial intelligence can perform tasks which save the average associate solicitor hours in billable time—

9 Libananco Holdings Co Limited v. Republic of Turkey, ICSID Case No ARB/06/8.

10 Mealey's International Arbitration Report, Sept. 2008.

11 Jane Croft, *Deloitte report predicts machines will displace legal low-skilled jobs*, FINANCIAL TIMES, Mar. 16, 2016.

such as automating the drafting of lengthy commercial contracts and undertaking due diligence and other time-saving processes—allowing them to get on with the important legal work. While such innovative breakthroughs in artificial intelligence are ground-breaking in today's legal context, new technologies quickly become the indispensable norm[12].

Impact on economy

The most experienced phenomenon recently in India is that of case law reading. All the lawyers who have spent a substantial portion of their life studying in the libraries, reading voluminous commentaries and then looking for the relevant year's AIR still believe that the best way to find a case law is through commentary. However, that perception is fast changing as the new tech-savvy lawyers in India find their case laws on the internet using paid websites such as Manupatra and SCC Online. It is easy, convenient and time-saving. Even the courts provide the judges with the latest technology to make their work less hectic especially considering the backlog of cases before the Indian Judiciary.

However, amidst the time saving and convenient environment people have failed to notice that when AIR was being used in full swing or rather were the only resource available, it employed many people for its research, production and transportation. The money circulated from the hands of the lawyers to the printer, researcher, binders, papermakers, transporters and booksellers. One of the essential roles it played was to keep the library up and beaming with life. All this has declined to a major extent because of computerization of legal research and this way the economy of the particular sectors of the country has also been affected.

Impact on environment

The technology that will facilitate the process of arbitration is most likely to be charged by lithium-ion batteries. The lithium-ion batteries are also known as Li-on batteries. These are the batteries which are rechargeable and are found almost in every gadget such as cell phone, laptop, and tablets. These batteries are known to pollute the environment when not disposed of properly. The best way to dispose of these batteries is to recycle them.

If one promotes mass usage of latest technology in arbitration, in a sense, that person is also encouraging the use of Lithium-ion batteries which more often than not land in a garbage dump area and are not recycled. This leads to sparks and fires in garbage dump areas and is hazardous for the people who enter the area to

12 Charles Kerrigan and Isabel Parke, *Lawyers and Robots*, LEXISNEXIS REPORT, http://www.lexisnexis.co.uk/pdf/lawyers-and-robots.pdf.

clean it. Cities like Dhaka, New Delhi, Mumbai and Manila where arbitration centres are expected to grow do not have adequate infrastructure to recycle these batteries and this way the electronic waste pollutes the city and the neighbouring areas as well.

TECHNOLOGY AND TRANSLATIONS IN ARBITRATION

A challenge which any cross-national company dealing with alternate dispute resolution mechanism is bound to face is that of translation. When parties who deal in business have different languages mostly make an agreement about the language which would be used in arbitral proceedings. A language clause in arbitration agreement vitiates the possibility of a dispute over language usage or the situation where the parties want to arbitrate in different languages.

As arbitration can be costly if every word and document, said and produced in arbitration proceedings is translated, a language clause helps in this respect. However, even if a language clause is inserted in the arbitration agreement, translators are still required to translate evidence and other materials produced on record. This is because the evidences may be in a language which is different from the language agreed upon by the parties for the arbitration of disputes.

An inherent challenge of cross-national business endeavours is that, once a deal or business relationship is in place, the actual terms of the contract will be carried out in different countries. Despite the fact that the trans-national agreement or contract was written in one language and that the terms of the agreement likely specify that such language is the "controlling" language in the event of a dispute, the execution of the terms of that contract will, in almost all cases, be carried out in different languages.

For example, a Chinese company may have a contract to provide certain gadgets to a German company, which will then add value to the product and then sell them in Germany. Let us say that the contract was negotiated in English and also written in English. However, once the negotiations are complete and the Chinese company starts supplying the product to the German company, the German company's re-sale efforts will not be conducted in English. The German company is servicing German customers on German soil. Thus, the transactions will be conducted in German and the documentation will reflect that - the invoices, receipts, customer agreements, website, terms of use, and every other conceivable document will be in German.

If the Chinese company and the German company in this example ever become embroiled in a contract dispute that relates, for example, to what the German

company represents to its own customers about the Chinese products, it is likely that most of the documentary evidence, in this case, will be in German. Both sides are left with a problem. A dispute between a Chinese company and a German company with a governing contract that is written in English will almost certainly be tried by an English-speaking judge, arbitrator, or tribunal. The challenge will be in how documentary evidence, which almost certainly is written in German, is presented.

Having two or more languages of the arbitration will normally increase time and cost. Consideration should be given to whether the use of two or more languages truly justifies the additional time and cost. On the other hand, where there is a single language of the arbitration, the use of an additional language should be considered if it would reduce time and cost.

For example, where appropriate, the parties can agree that documents, legal materials and witness testimony in a particular language need not be translated into the language of the arbitration. If the parties have agreed, or the arbitral tribunal has decided, that the arbitration will be conducted in two or more languages, the parties, and the arbitral tribunal should consider agreeing upon practical means to avoid duplication. In cases where the members of the arbitral tribunal are fluent in all applicable languages, it may not be necessary for documents to be translated. Consideration should also be given to avoid having the Terms of Reference, procedural orders, and awards in more than one language. If this cannot be avoided, the parties would be well advised to agree upon the language that will prevail[13].

As is evident, arbitral proceedings which require translations of speeches and documents still are heavily dependent on humans to translate. The need of the hour is to have a super-fast translation software which can expedite the whole process of arbitration in cases where the parties have wished to arbitrate in two different languages or the evidence produced is in a language different from that of the language agreed upon by the parties. The problem the software makers will face is how to make the material an input for the software where the files are in hardcopy. But as they say, science fiction is nothing but a prediction of what will be invented in future. The case of super-fast translation software also seems to be of such a nature and would be invented hopefully than not in the near future.

CONCLUSION

Technology and innovation are ever-growing and ever-evolving. The daily life of

13 *Proceedings involving two or more languages, Controlling time and costs in arbitration*, ICC COMMISSION REPORT, (2 ed.).

human is heavily dependent on technology and soon the arbitration which happens in areas which are not comparatively economically powerful, would soon be highly tech savvy. This is what technology does to humans, it serves them initially and later it becomes their master. Similarly, we see examples of how most of the work which needs to be done in today's world, can't be done without using the latest technology and software.

In arbitration, the parties come to resolve disputes and the whole process gets easier with using gadgets to explain how the cost is evaluated, how the damage is calculated and other things of same nature. In future, it is very likely that we have super-fast translations software which would decrease the cost of arbitration. The dependency on technology today is frightening but at the same time can't be dispensed with. Therefore, with such an ever-evolving and indispensable nature, humans tend to experiment with technology as when the latest arrives. And in doing so realises that loopholes just can't be done away with. Hence, issues of data breach and leakage of confidential information are bound to arise. In the end, one has to make the decision about using technology in arbitration as the substantial ease which technology provides may come at a cost of losing confidential information.

CASE COMMENT: SHREYA SINGHAL V. UOI

Lubhanshi Rai*

INTRODUCTION

The Supreme Court of India on March 24, 2015, delivered a landmark verdict in the case titled "Shreya Singhal V. Union of India" (writ petition (criminal) no.167 of 2012). This event happened to be, as a high point in the legal enlargement of the Freedom of Speech and Expression[249] and primarily the constitutional scope of its restriction[250]. The leading gist of the judgment is that it has interpreted the scope of the fundamental right guaranteed to us by the constitution of India to express ourselves freely, and limited the exercise of a right available to the state in curtailing this freedom to absolutely necessary circumstances.

In this case, Shreya Singhal, the petitioner, filed a writ petition in the Supreme Court, under article 32 of the Constitution of India, challenging the constitutional validity of Section 66A, 69A and 79 of the "Information Technology Act, 2000" and Section 118(d) of "Kerala Police Act, 2011", on the grounds that the drafted sections are overbroad, have not been adequately specified for its proper application and the overbroad terms of the Section 66A of IT Act and Section 118(d) of Kerala Police Act, are not covered within the scope of Article 19(2), thus, the said sections are in violation of the right to Freedom of Speech and Expression. Thus, these sections are liable to be declared *void* and *ultra vires* of the constitution of India.

In the judgment, the Supreme court declared Section 66A of the Information Technology Act, 2000 and Section 118(d) of the Kerala Police Act, 2011, as *void*, in their entirety, being repugnant of Article 19(1)(a) and not saved within the scope of

* 2nd Year, Amity Law School, Delhi (Affiliated to GGSIPU)

249 INDIAN CONST. Art. 19(2) - Nothing in sub clause (a) of clause (1) shall affect the operation of any existing law, or prevent the State from making any law, in so far as such law imposes reasonable restrictrictions on the enjoyment of the right guaranteed by the said sub clause in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence.

250 Central Government is armed with the right to issue directions for blocking the content under certain circumstances, read with section 87(2)(z) of the Act, in exercise of which, Procedure & Safeguards for Blocking for Access of Information by Public, Rules 2009, were laid down.

Article 19(2). However, "Constitutionally valid" status was given to the Section 69A[251] and 79[252] of IT Act.

Whole essence of the case moves around striking down of Section 66A, the most deliberated, argued and analyzed by the division bench, comprised of J. Chelameswar and J.R.F. Nariman, due to its nature of restricting the freedom of speech made through computer resources (covered the opinions expressed through social media on internet). In this comment as well, the very same Section in context of the main issue the scope of restriction of freedom of speech and expression is going to be discussed primarily.

BACKGROUND

IT Act, 2000 confers legal recognition upon the transactions made through the computer resources. This law was made, to elevate the IT industry, administer e-commerce, promote e-governance and anticipate cybercrime. In 2009, Section 66A was inserted into the Act to penalize offensive texts made through computer resources or other communication tools. Provision: any person who sends any information, by means of a computer resource or a communication device, which-

A. is grossly offensive or has menacing character

B. he knows to be a false and meant for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device; or

C. any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine[253].

251 Section 79 was held valid by the bench, subject to Section 79(3)(b) has to be interpreted, to mean that an intermediary upon receiving actual knowledge from a court order or on being notified by the appropriate government or its agency that unlawful acts relatable to Article 19(2) are going to be committed then fails to expeditiously remove or disable access to such material. Similarly, the Information Technology (Intermediary Guidelines) Rules, 2011 are also valid subject to its Rule 3 sub-rule (4) has to be interpreted in the same manner.

252 The genealogy of this Section may be traced back to Section 10(2)(a) of the U.K. Post Office (Amendment) Act, 1935, which made it an offence to send any message by telephone which is grossly offensive or of an indecent, obscene, or menacing character. Section 66 of the UK Post Office Act, 1953, was essentially the reproduction of the earlier provision. Later, this Section was replaced by Section 49 of the British Telecommunication Act, 1981 and Section 43 of the British Telecommunication Act, 1984. In the UK, currently it is Section 127 of the Telecommunication Act, 2003.

The arrests that were made using the power of Section 66A of IT Act, sparked the debate on the scope of the section and its application, finally leading to challenging the constitutional validity of the said section.

Some of the incidents which were significant enough to pose the challenge to the section: when two Palghar girls, Shaheen Dhada and Renu Srinivasan, were allegedly arrested under this section in November 2012 for posting on their facebook, critically questioning why the entire city was closed down for merely the funeral of Shiv Sena leader Bal Thackeray: same when a businessman from Puducherry, Ravi Srinivasan, was arrested in October 2012, for allegedly posting 'offensive' contents on Twitter about Karti Chidambaram, son of Congress leader P Chidambaram, and when the Police arrested CPI-M worker Rajeesh Kumar in August 2014, for posting offensive comments and pictures on facebook about Prime Minister Narendra Modi. And, so many cases of the same nature actually did take place.

Most of the arrests, in fact, were made for commenting on the political leaders or prominent personalities, which posed a serious doubt on the objective and legality of the section.

Accordingly, certain rules of procedure were issued by the central government,[254] aimed to check such arrests, including that advance permission from the Deputy Commissioner or Inspector General of Police is necessarily to be taken before recording a complaint under Section 66A. And, Supreme Court too endorsed these directives in May 2013. Since, the matters related to 'police' and 'public order' lie in the state list, a Supreme Court mandate was required for the application of these guidelines across the country. However, the Section could not be modified.

In 2013, a Private Member Bill[255] was brought in Lok Sabha, suggesting some amendments to the Section. The Bill, aimed to make impugned section parallel with the available provisions of the Indian Penal Code (IPC), 1860 on certain aspects, because disparities between the provisions of two acts had led to double penalties for the same, single offence. As per the statement of the Bill, there were even inconsistencies and disparities between the two laws in respect of duration of

253 On Nov. 29, 2012 the Minister for IT, Mr. Kapil Sibal called for a meeting of stakeholders with representatives of government, businesses and civil society to break the deadlock on Section 66A of the IT (Amendment) Act of 2008.

254 **The Information Technology (Amendment) Bill, 2012** By Shri Baijayant 'Jay' Panda, M.P., *A BILL further to amend the Information Technology Act, 2000.*

255 A private members resolution was moved by M.P. P. Rajeeve on Dec. 14, 2012 to amend the draconian section 66(A) of IT act, but it was withdrawn on the assurances from Telecom Minister Kapil Sibal that the resolution will be taken up after the Supreme Court of India rules on it.

imprisonment for the same offence, as two years punishment has been prescribed in IPC for the offence of threatening someone to injure through email, while it's three years under the IT Act for the same offence. But the Bill was eventually withdrawn.

The very same year, again an attempt was made as "Private Members resolution"[256] was moved in the Parliament, which recommended certain changes in the Act, which were:-

- To make Section 66A consistent with part III of the Constitution,
- To limit the operation of the Section to communication between two persons only,
- To accurately demarcate the offences covered by the Section, and
- To lower the penalty and make the offence a non-cognizable one, so that any arrest could not be made without a warrant.

However, this resolution also could not be taken further and was eventually withdrawn. By then, PIL had already been filed by Shreya Singhal in the Supreme Court challenging the constitutionality of the Section.

ANALYSIS

In this milestone judgment, the Supreme Court enlarged the scope of right to speech on social media and limited the grounds on which, this precious right can be curtailed, by abolishing the draconian, stringent Section 66A of the IT Act, calling it open-ended and unconstitutionally vague, and further expressed that the impugned Section "arbitrarily, unnecessary and disproportionately" interrupt with the right to free speech, right to dissent, right to know, and had a "chilling effect" on the constitutional mandates.

Decision of the Court was quite appropriate with the all legal reasoning behind the unconstitutionality of the impugned Section, as this section had been widely misused for merely a political purpose by police in various states to arrest innocent persons for posting critical comments about social and political issues. In many cases, section 66A was just used as a tool to punish the political opposition for remarking upon political and notable personalities.

This drew the attention of the Court. The scope of this section is too wide that even innocent persons can be easily trapped within its requirement, and thus this section is highly vulnerable to its misuse. Respective bench in the same context

touched upon the point that the terms of the Section are such, not even capable of guiding the implementing authorities properly.

Thus, it was expressed by the respective bench, that for proper application of any law, language and the terms of the particular provision should be comprehensive enough that- *firstly,* people, who all are to be governed, should be able to draw a line between legal and illegal acts and should be able to comprehend the prohibited acts as per that particular law and *secondly,* the concerned law should be able to provide proper guidance to the administering authorities in regard of procedures and safeguards to be undertaken, while applying the law[257]. And section 66A is actually in a defect on both the aspects.

Term 'liberty' has been embraced in our Constitution and happens to be of paramount significance. In this judgment, Supreme Court has reiterated the importance of Freedom of Speech and Expression citing the previous judgments[258].

Bench concluded that the content of the speech has to be analyzed for determining the role of Article 19(2), as any speech can be of three types, first merely discussion,

256 In the present case, bench took an American case for reference "Musser v. Utah, 92 L. Ed. 562(1948)" and analyzed the concept of U.S.A- The U.S. Supreme Court has repeatedly held in a series of judgments that where no reasonable standards are laid down to define guilt in a Section which creates an offence, and where no clear guidance is given to either law abiding citizens or to authorities and courts, a Section which creates an offence and which is vague must be struck down as being arbitrary and unreasonable. Same rule being applied in present case, however this concept is not absolutely applicable in India, was admitted by the bench.

257 Romesh Thappar v. State of Madras, [1950] S.C.R. 594, In Sakal Papers (P) Ltd. &Ors. v. Union of India, [1962] (3) S.C.R.842.

258 Kameshwar Prasad & Ors. v. The State of Bihar & Anr., 1962 Supp. (3) S.C.R. 369, and Indian Express Newspapers (Bombay) Private Limited &Ors. v. Union of India & Ors., (1985) 2 SCR 287, The pattern of Article 19 (1) (a) and of Article 19 (1) (g) of our constitution is different from the pattern of the First Amendment to the American Constitution which is almost absolute in its terms, appears to has conferred no power on the Congress to impose any restriction on the exercise of the guaranteed right, still it has always been perceived that the freedom assured, is subject to the police power - the scope of which however has not been demarcated with precision or uniformly. It is due to this police power to curtail the freedom, that the laws interdicting libels, and those relating to sedition, or to obscene publications etc., have been sustained constitutionally. The resultant flexibility of the restrictions that could be validly imposed renders the American concept or courts' decisions inapplicable to Indian cases. In the present case as well, bench has cited some American judgments to emphasize the significance of this Fundamental right, but at the same time has also expressed that the American concept can't be applied absolutely in present case, as in America, the concerned right has been interpreted in subject to "general public interest", while in India, there are only eight conditions provided in article 19(2), and nothing apart from or above these conditions has been recognized in India by the Courts.

second argumentative, these two are saved within the scope of Article 19(1)(a), while third one is instigative where article 19(2) comes into picture.

Now, It can be concluded from the previous applications of the concerned provision that section 66A is not capable to demarcate the speeches of these three kind, as any discussion or argument may be sometimes annoying, highly offensive or may cause inconvenience or even insult someone, but ultimately all these are saved within the ambit of "freedom of speech and expression" and can only be restricted if it falls within the meaning of those terms, incorporated in article 19(2), which are- sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality or in relation to contempt of court, defamation, or incitement to an offence. Thus, the bench rightly said that the section violates the people's right to know as well.

It can be easily interpreted that the terms, such as security and integrity of India, security of state, and relation with the foreign states, have got nothing to do with the section 66A of the IT act. Now the remaining four terms- public order, decency and morality, defamation, incitement to an offence, mechanically fall within the ambit of the terms used in the Section 66A due to its open ended scope. But words of section 66A do not fall within the scope of article 19(2). It can easily be explained in a way: there are two circles, one small circle of article 19(2) which lies within the bigger circle of section 66A.

So, this Section just paves the way for the state authorities to deprive people from their fundamental right on unreasonable grounds. Even if this section tries to create some offences like insult, for which the section has not been framed properly, with the wrong choice of words, lack of specifications, without any stipulations and safeguards.

Supreme Court went on to pronounce, citing a judgment of Sakal Papers (P) Ltd. &Ors. v. Union of India, [1962] 3 S.C.R. 842, that apart from the constitutional grounds, there can't even be 'general public interest' an acceptable ground to restrict the right to speech[259] Kameshwar Prasad & Ors. v. The State of Bihar & Anr., 1962 Supp. (3) S.C.R. 369, and Indian Express Newspapers (Bombay) Private Limited & Ors. v. Union of India & Ors., (1985) 2 SCR 287, The pattern of Article 19 (1) (a) and of Article 19 (1) (g) of our constitution is different from the pattern of the First Amendment to the American Constitution which is almost absolute in its terms, appears to has conferred no power on the Congress to impose any restriction on the exercise of the guaranteed right, still it has always

259 Information disseminated may be to one individual or several individuals, This Section makes no distinction between mass dissemination and dissemination to one person.

been perceived that the freedom assured, is subject to the police power - the scope of which however has not been demarcated with precision or uniformly. It is due to this police power to curtail the freedom, that the laws interdicting libels, and those relating to sedition, or to obscene publications etc., have been sustained constitutionally. The resultant flexibility of the restrictions that could be validly imposed renders the American concept or courts decisions not applicable to Indian cases. In the present case as well, bench has cited some American judgments to emphasize the significance of this Fundamental right, but at the same time has also expressed that the American concept can't be applied absolutely in present case, as in America, the concerned right has been interpreted in subject to "general public interest", while in India, there are only eight conditions provided in article 19(2), and nothing apart from or above these conditions has been recognized in India by the Courts.

With this judgment, The Supreme Court, in order to save the precious fundamental right of citizenry from getting violated and to maintain its spirit, very well narrowed down the power of the government to restrict the right to speech, only to extreme circumstances.

As connection was being tried to establish between the impugned Section and the terms of article 19(2) by the respondent, court very finely demarcated the boundaries of these terms, analyzing the landmark judgments in this regard. Out of all concerned terms, Public Order was the huge issue and most analyzed one, by the bench.

It is nowhere mentioned in section 66A whether this section aimed to punish the acts directed against general public or individual[260], and that has maintained a high vagueness of objective of this section. Here bench, referring the judgment of Arun Ghosh v. State of West Bengal, [1970] 3 S.C.R. 288, declared that restrictions on the right, provided in the Section has not been covered within the ambit of Public order. Public Order is in fact a very narrowly interpreted term as described by the bench that, "One has to assume three homocentric circles. Largest circle represents law and order, within which, the next circle is depicting public order and the smallest circle represents security of State. It is then comprehensible, that an act may affect law and order but not public order and similarly an act may disturb public order but not security of the State[261]."

Acts causing disturbance to public order needs to be separated, from acts directed against individual persons, which do not disturb the society to the extent of causing a disturbance to public tranquility[262].

260 Dr. Ram Manohar Lohia v. State of Bihar & Ors., [1966] 1 S.C.R. 709.

261 Arun Ghosh v. State of West Bengal, [1970] 3 S.C.R. 288.

262 State of Bihar v. Shailabala Devi, [1952] S.C.R. 654.

So, the test here is, does a speech prohibited, leads to cause disturbance to current, normal life of the community or society or does it merely interfere with an individual's life, leaving the society peaceful and undisturbed. Another test is that does a message tend to bother the public order[263]. Section 66A has failed to answer both the questions.

It was intended to create an offence of defamation through the Section, but in its language Section is not even concerned with injury to reputation at all, which is an essential ingredient of the offence defamation.

Even if it was tried to bring the section within the ambit of "Incitement to an offence" or "Decency and Morality", it could nor be done as Section has failed to characterize the information which has a tendency to incite and the information under the Section is not required to be obscene at all.

The apex court provided all the legal and logical reasoning that why the Section 66A could not be covered within the scope of article 19(2) and thus, is altogether "*ultra vires*" of the Constitution of India.

And these offences like criminal intimidation, defamation have already been included in IPC in a proper way, which are enough to deal with the cases even committed through computer resources.

And moreover, terms like annoyance, inconvenience, grossly offensive, etc, which all have been incorpotated in the section 66A, can't be the offences in themselves, however, they collectively do form some of the offences, as ingredients in IPC. If they are made offences in themselves, it would be highly offensive to the basic rights of the people.

The fact, that the social media is more vulnerable to the abusive information or is more convenient way to abuse people, should not be a reasonable or satisfactory ground to curb the freedom of speech and expression of the citizenry on social media.

Though, The Supreme Court has abolished the Section 66A, but it has recognized an intelligible differentia between internet and other mediums as the platforms to share information, and upheld that parliament is very much empowered to make new law or amend the IT act to add new provisions with proper safeguards and procedures in this regard.

263 Penalty for causing grave violation of public order or danger.- Any person who,- Causes annoyance to any person in an indecent manner by statements or verbal or comments or telephone calls or calls of any type or by chasing or sending messages or mails by any means; shall, on conviction be punishable with imprisonment for a term which may extend to three years or with fine not exceeding ten thousand rupees or with both.

It also outlawed a provision: "Section 118(d) of the Kerala Police Act[264], parallel to section 66A, on the very same grounds, being inconsistent with Article 19(1)(a) and nor saved by Article 19(2)".

But it upheld the validity of Section 69A and Section 79 of the IT act, stating that unlike section 66A, these provisions are narrowly drafted, with the proper safeguards and procedures, with the condition that section 79 to be read down as the "knowledge" referred of in the section 79(3)(b), must be acquired through the means of the court order.

CONCLUSION

Here in this case, the constitutional validity of the four major provisions, was challenged which are section 66A, 69A and 79 of the Information Technology Act, 2000 and section 118(d) of the Kerala Police Act. In which, Supreme Court has struck down the section 66A of I'T Act and section 118(d) of the Kerala Police Act, on the same grounds of "Overbreadth and Chilling Effect", while it upheld the validity of other two provisions of the IT Act, thus it maintained the balance between the parties.

Moreover, it acknowledged, analyzing the American case laws, that unlike USA, vagueness is not an absolute ground for declaring a law invalid in India but Indian courts are required to narrow down and specify the language of the provision or law under consideration, to an extent, it is possible. And, this rule is actually being applied here by the court, as it can be understood from the all reasoning that it provided for striking down the section 66A and even "why" it can't be saved anyhow, giving a reason that, if a law which is otherwise invalid, can't be saved by the undertaking from the Government.

While the bench specified the interpretation of Section 79(3)(b) on its own, declaring it as constitutionally valid, because it was possible in this case as the whole section was otherwise constitutionally valid, so could not be declared *void* just for minute vague thing which was actually very much capable of getting corrected and so the court did, standing up to the expectations and its duties.

The verdict of the Supreme Court is of colossal significance in protecting online free speech against arbitrary powers of the state. But unfortunately, the Section 66A, which was declared unconstitutional, still has been used in many cases as a punitive measure against online speech, discounting the value of the Supreme Court.

264 Section 79 belongs to Chapter XII of the Act in which intermediaries are exempt from liability if they fulfill the conditions of the Section.

About Amity Law School

The School has been consistently ranked as one of the Top Law Schools in the Country since 2006. In the survey of the India's Best Law Colleges by India Today (THE INDIA TODAY NIELSON SURVEY), the National Magazine, Amity Law School Delhi(ALSD) bagged 4th rank in India in 2017 moving up in ranks from Rank 11 in the same in 2016. In THE WEEK (HANSA RESEARCH SURVEY) ALSD was ranked at 12th in 2016 and 11th in 2015. THE OUTLOOK (OUTLOOK GFK MODE SURVEY), ALSD was ranked 10th in 2016.

The Amity Law School, Delhi(ALSD) has the unique distinction of being the first Law School in Delhi to start a 5-year integrated LL.B (H) programme in 1999. The School was established under the Ritnand Balved Education Foundation (RBEF) to achieve world-class legal education in the country. Dr. Ashok K. Chauhan, the Founder President of the Law School is a great philanthropist and a man of extraordinary vision. This great vision has been translated into practical reality through the establishment of various educational institutions including the Amity Law School. His vision for the Law School is to provide excellence in legal education and to produce quality lawyers with good moral principles and great human values. The President RBEF, Dr. Atul Chauhan has been providing dynamic leadership intervention in strengthening the vision of the Founder President. Presently the academic values are being inculcated by Prof. (Dr.) D. K. Bandyopadhyay, (Former Vice-chancellor, GGSIPU) Chairman, Amity Law Schools.

Amity Law School Delhi has been granted affiliation by the Guru Gobind Singh Indraprastha University, Delhi for running a 5-year Integrated LLB (H) programme and the affiliation has been approved by the Bar Council of India. The programme is designed to incorporate teaching methods for realizing holistic legal education.

The programme offered by Amity Law School Delhi seeks to promote multi-disciplinary analysis of the socio-legal problems by designing/pursuing/giving effect to its course-structure and teaching methods to realize these objectives. The methods of teaching in the Law School include lecture, discussions, case law analysis, moot court training, project assignment and placement programmes. In addition, the School organizes seminars on contemporary legal issues, conducts clinical courses and train students in legal research and legal writing. By the time a student completes the 5-year programme he/she will be fully equipped with the required theoretical knowledge and practical experience in the field of law to become a full-fledged responsible member of the legal profession.

AMITY LAW SCHOOL (DELHI)
(An Institution of Ritnand Balved Education Foundation)
Affiliated to Guru Gobind Singh Indraprastha University, Delhi)
F-1 Block, Amity University Campus, Sector-125, Noida-201313 (Uttar Pradesh)
Tel: 0120-4392681 E-mail : alsdelhi@amity.edu Website: www.amity.edu/als
Printed at : K. S. Enterprises, Delhi