ROLE OF CYBER LAW IN E-GOVERNANCE

Written by ***Yatharth Chauhan***

3rd Year BA.LLB Student, Gautam Buddha University, Greater Noida, India

ABSTRACT

Certainly, the advent of Information and Communication Technology has resulted in expeditious and effective communication, better data storage, processing of data as well as information, accountability, transparency and so forth. Electronic governance, digitization of government's service, is linked with administering the functions and procuring the ends of governance via Information and Communication Technology. In other words, e-governance is a modus operandi to dispense the service of government with the assistance of Information and Communication Technology. Electronic governance is primarily an initiative to make governance citizen-oriented only. Late Abraham Lincoln has rightly asserted that government is by the people, for the people, and of the people. Given the increase in consciousness concerning fundamental rights among the people and in supposition from the government, the prospect of governance has affected significantly. To be more answerable as well as transparent is expected from the government in the present time. This has spurred the need to advance the application of Information and Communication Technology. Information and Communication Technology, beyond doubt, is a boon to businesses since it embraces all types of digital technologies that aid businesses and companies as well in respect of design, sales, manufacturing, response and makes businesses more coherent and effective. To substantiate the consummation of e-governance, indispensable is that security features should be stringent because e-governance involves the flow of personal data. The privacy of common people in any respect cannot be compromised therefore it is the need of the moment to shield the whole system from cyber-attacks. The instant research paper is divided into four parts namely the first part deals with the general introduction pertaining to cyber law as well as e-governance which also includes celebrated definitions, the second part deals with major cyber threats in respect of e-governance, the third part deals with the relationship between cyber law and e-

governance which is supported by landmark cases of Hon'ble Supreme court and the last part covers the significance of cybersecurity followed by the Conclusion.

***Keywords*:** Accountability, Transparency Privacy, Cyber law, Security Features and Personal Data

INTRODUCTION

Men has continuously been stimulated by necessaries, since the advent of civilization, to institute productive changes and ameliorate the existing technologies. This has resulted in the prodigious advancement which has been a propelling cushion for the further development and one such significant development is Information and communication Technology (hereinafter referred to as ICT). According to World Bank, ICT refers to variety of activities that stimulate the processing, transmission and Display of Information via electronic means. Certainly, ICT are ubiquitous in nature and the scope of digitization has been considerably expanded. Even though, the introduction of ICT, specifically in western nations, centered on realizing the consumer needs, but developing nations too may reap benefits of such advanced technology[i]. Through the Long-Distance Remote Conversation Technology namely WiMAX (Worldwide Interoperability for Microwave Access), numerous Individuals in the developing nations have ingress to the web and associated goods and services[ii]. Traditional letters have been dislodged by the E-mails. To several business, Virtual Web delineation have become more imperative.

The introduction of ICT is a cornerstone for the advancement concerning the formation, obtainability and utilization of network related service. The evolution of ICT has resulted in e-education, e-commerce, e-health, e-governance, and e-environment[iii]. These applications of ICT have had significantly yield basic amenities in rural as well as urban areas. The appropriation of ICT has substantially turned down the cost of transaction, refine the service of delivery, generated employment on a large scale and created latest revenue streams. E-governance is one of the vital facets of ICT. According to the council of Europe, e-governance suggest the application of electronic technologies in three aspects of Public action namely, relation between the public authorities and civil society, working of the public authorities at all stages of the democratic process (e-democracy) and the provision of public service (electronic

public service). Given the application of ICT, e-governance is a coherent step to guarantee more extensive support and more profound inclusion of citizens, private sector and civil society pertaining to the decision- making procedure of governance[iv]. It is worth mentioning that the fundamental purpose of e-governance is to give effect to SMART i.e. Simple, Moral, Accountable, Responsive, and Transparent governance via the application of ICT[v].

Had anyone pondered about the ramifications proposed by ICT in the guise of cybercrime? There is no any statutory definition of cybercrime. Cybercrime, in general, alludes to an unlawful activity namely, cyberbullying, cyber extortion, data theft, etc. carried out through digital means. Two pertinent definitions were expounded at the 10th United Nation Congress on the Prevention of crime and the Treatment of offenders i.e. cybercrime in a contracted sense deals with such unlawful act, escorted by electronic operation that preyed on the safety of computer system as well as a volume of data handled by them. On the other hand, cybercrime in a wider sense refers to an illegal act perpetrated by computer system or network like unlawful ownership dispersing personal information. Such crimes are also known as computer-based crime[vi]. The materialization of technology has adversely catalysed its abuse.

The initiative of e-governance has become susceptible to security gaps owing to lack of well-eloquent security stratagems. This has given rise to an intrinsic debate between right to Privacy and Protection of Data as well. The advancement of technology has made personal data smoothy available as well as communicable. Lack of stringent security mechanism may prohibit the accomplishment of e-governance. To corroborate the success of ICT, its reliability plays a major role. Certainly, security is a sine qua non to reliability.

MAJOR CYBER THREATS

The growth and development in the field of technology is now adversely escorted by new cyber threat. cyber-attack against information infrastructure as well as web administrations presently have the ability to hurt society in a critical manner. The financial harm caused by cybercrime is detailed to be gigantic. Hacking and online fraud are the major computer-related offense perpetrated extensively. Some of the major cyber threats are as follows:

1. ***Confidentiality Threat***

   Confidential information of customer or end user ought not to be available to any unwarranted or unauthorized person. At the time of transmission, such vital information should not be expropriated. Injection, unauthorized ingress, Packet sniffing, Password Attack, Port scanning, Dumpster Diving, etc. are the major confidential threat[vii].

2. ***Integrity Threat***

   Such threat seeks to corrupt and devastate the data or system. When it comes to Integrity, data should not be modified or revised during its dissemination over the network. Threats concerning integrity include data diddling, salami attack, MITM (Man in the Middle), Data Manipulations, etc[viii].

3. ***Accessibility Threat***

   Data ought to be accessible wherever and at whatever point it is demanded within a stipulated period of time. Denial-of-service-attack, SYN Flooding, server room threat, etc. are the major threat pertaining to Accessibility[ix].

4. ***Password Cracking***

   Certainly, very user is well versed with the fact that a great password security is pivotal for securing delicate framework and information. Every citizen, thus, ought to use vigorous passwords that cannot be speculated effortlessly. A strong password should be more than 12 characters in respect of length including upper case and lower-case letters and with extraordinary characters. However, Hackers have now developed several techniques to compromise the password of the user[x]. Some of them are as follows:

   a. **Rainbow Table Attack-** It is an act of hacking wherein the hacker attempts to use a rainbow hash table to decipher the password stashed in the database. It is basically a hash function which is utilized in the cryptography to store the critical data[xi]..
   b. **Brute Force Attack-** It is the cyberattack of attempting every conceivable combination of numbers, letters and symbols to track down the password of user or any other personal detail[xii].
   c. **Malware-** Malware is a defective or malicious software consciously designed by the cybercriminals to gain unauthorized access or vandalize completely a

computer framework or network for unlawful activity such as financial crime. In such situation, users are basically not acquainted with until they come across to damage. Malware, usually, comprises of Trojan Horses, viruses and worms[xiii].

5. ***Remote to Local Attack***

It is a cyberattack where a hacker over network dispatches packets to a machine, subsequently utilize the vulnerability of machine to procure unauthorized access to a machine. Such adverse attack may result in theft of services, data loss, etc[xiv].

6. ***XML Injection***

It influences or operate the rationale of an XML Application or service. The infusion of an inadvertent XML content into XML message can easily modify calculated logic of an application. A fruitful XML infusion can let the hacker to access the complete database or even log in as the controller of the website[xv].

7. ***Phishing***

Phishing is often perceived as a web threat. It is an attempt to imitate a web page to procure the confidential information viz username, passwords and other financial details. Hackers uses a bogus URL which is disguised as if it emerged from the legitimate source which regulate the personal details. And when customers capitulate their personal information via such URL, their credentials are transferred to the hackers[xvi].

8. ***Cross-site scripting XSS***

It is too a sort of infusion. However, they make use of defective or noxious scripts which are directly infused into trustworthy websites. Hackers uses XSS to consign a malevolent script to trick a user[xvii].

9. ***SQL Injection***

It is primarily an infusion assault in which an assailant accomplishes spiteful SQL statement accompanied by variable payload to ingress web application's database server. SQL Injection is one of the most seasoned as well as unsafe web application assault and can adversely affect database or webpage[xviii]

10. LOG Injection

It is used by a hacker to infuse pernicious content or cast log entries if there is a susceptibility which permits unsupported end user input to be composed within the logs. An attack of LOG injection can result in infusion of fraudulent log event[xix].

RELATION BETWEEN E-GOVERNANCE AND IT ACT, 2000

Section 4 to section 10A of IT Act 2000 dealt with e-governance which are as follows:

1. Legal Recognition of Electronic Record

Section 4 of the IT Act, deals with legal recognition of electronic record. It explicitly says if any Law requires that any information or matter shall be in writing or in typewritten form or printed form then such stipulations shall be considered to be satisfied if the same is available in an electronic form and accessible for further purpose. The aforesaid has significantly perceived the application and cogency of electronic record in lieu of paper based docket.

Section 65A of Evidence Act,1872(hereinafter referred to as Evidence Act), states that subject matter pertaining to the electronic record should be manifested in accordance with the provision of section 65B of the Evidence Act. Section 65B (1) of Evidence Act states that any information envisaged in an electronic record which is printed on a paper, or stored, recorded or copied in optical or magnetic media produced by a computer shall be considered equivalent to document and admissible as an evidence in proceedings without any further proof of the original provided the necessary conditions mentioned under sub- section (2), (3), (4) and (5) of section 65B are satisfied.

Section 65B (4) of Evidence Act provides for the certificate of Authenticity. The fundamental purpose concerning the certificate is to corroborate the rectitude of the source as well as veracity of the data since digital data is susceptible to moderation. The certificate of Authenticity ought to be signed by such person possessing an accountable position in connection to the gadget through which the information has been adduced.

Legal Elucidation Prior to enactment of Section 65A and 65B under Evidence Act

Earlier courts used to take int consideration section 61 to 65 of Evidence Act to ascertain the suitability of Electronic Record or Data. The subject matter of Electronic Record could be satisfied either by primary or secondary evidence. According to section 62 of the aforesaid Act, Primary Evidence are the original dockets adduced before the court of Law for the purpose of verification. However, if the original documents are not accessible then it becomes obligatory to adduce secondary Evidence in consonance with the conditions mentioned under section 65 of Evidence Act to manifest the content of the original record.

Legal Elucidation after the enactment of Section 65A and 65B under Evidence Act

Section 65A and 65B were incorporated in relation to Amendment in the year 2000. This amendment has made a computer output equivalent to primary evidence to manifest the content of the original record. As discussed above, as per section 65B (4) whenever any party wishes to adduce secondary evidence as a primary evidence, then in such situation, a certificate of authenticity should be delivered expressing any of the thing explicitly envisaged in the aforesaid action.

An important legal paradox that emerges in this respect is whether the certificate of Authenticity under section 65B (4) of Evidence Act is Mandatory? The Primary case in which the aforesaid issue emerged was Navjot Sandhu v. NCT Delhi[xx], and the hon'ble Supreme Court has said that if the certificate is not adduced in connection with conditions named under section 65B (4), electronic evidence would not be accepted. But it may be manifested or proved as a secondary evidence according to section 63 read with section 65 of the Evidence Act. However, the hon'ble Supreme Court overruled the aforesaid judgement in Anwar P.V v. P.K. Basheer and others[xxi], wherein it was said that documentary evidence via electronic record should be demonstrated only when it is escorted by a certificate of authenticity as mentioned under section 65B (4) of Evidence Act.

Furthermore, in Shafhi Mohammad v. The State of Himachal Pradesh[xxii], the hon'ble Supreme Court has said that the requirement to adduce a certificate as per section65B (4) is procedural and can be loosed within the intrigued of justice. The aforesaid requirement is not mandatory

if a party are not in a state to produce the same. Furthermore, a party can also adduce a computer output as a secondary evidence in respect of section 63 and section 65 of Evidence Act. Eventually, in Arjun Kushanrao and others v. Kailash Kushanrao[xxiii], the three-judge bench of hon'ble supreme court has established that the necessity to adduce certificate under section 65B (4) is a pre-requisite to the acceptability of evidence via electronic means under the aforesaid section while maintaining the law expounded in Anvar P.V v. P.K. Basheer and others.

2. Legal Recognition of Electronic Signature

Section 5 of IT Act accords Legal recognition to electronic signature. It explicitly states if any law requires that information or any matter shall be substantiated by attaching the signature or any document shall be signed or hold the signature of any individual person then the aforesaid stipulations shall be considered to be gratified if such matter or information is corroborated via means of electronic signature attached in consonance with the manner specified by the central government. Section 2(1) (ta) of IT Act, deals with the expression 'Electronic Signature'. It says verification of an electronic record by a subscriber by way of an electronic technique indicated in a second schedule and involves digital signature.

According to section 3A of IT Act, a subscriber, in whose name an electronic signature is furnished, may certify an electronic record either through an electronic signature or an electronic authentication technique which are basically reliable or authentic as well as in congruence with second schedule of IT Act. Sub-clause 2 of section 3A deals with the conditions necessary concerning an electronic signature or electronic authentication technique. These are as follows:

(a) The data pertaining to authentication shall be linked to signatory or authentication
(b) During the authentication or signing, the authentication data were in the possession of signatory or authentication only.
(c) Any modification to an electronic signature, shall be identified, made after attaching the same.

(d) Any modification to an information which is made after its authentication shall be identified.

Electronic signature suggests, signing the docket virtually. It is digital course of action through which an entity or any person venture into an electronic contract. Electronic signature, identical to Traditional Wet Signature, are legitimately authoritative. To corroborate the validity of an electronic document, a mathematical sequence is involved or utilized which is known as Digital signature. It is an algorithm which the recipient can utilized to scrutinize and validate if the digital document procured by them is not altered and is in its primal configuration[xxiv].

A Public key Infrastructure (hereinafter referred to as PKI) is used to confirm the highest level of reliability or security. PKI is certainly a universally established tack that facilitate inter-country undertakings electronically with less risk of false identity. Both Electronic signature as well as Digital Signature are frequently used interchangeably[xxv]. However, these two concepts are different in the sense that the former is the rendition of traditional wet signature whereas the latter is employed as a technology to certify the cogency of document[xxvi]. It is the cryptographic authentication technology that significantly buttress electronic signature. PKI demands two types of keys namely Public key as well as Private Key to encrypt and decrypt the information. Public Key is defined under section 2 (zd) of the IT Act as the key of a key pair used to substantiate a digital signature and mentioned in Digital Signature certificate whereas Private Key is defined under section 2(zc) which means the key of a Key pair used to give effect to Digital Signature[xxvii].

The Public key is basically used to encrypt the messages which can be decrypted via corresponding Private key only. Cryptographic authentication technology can be predominantly divided into two facets i.e., Symmetric Key cryptosystem as well as asymmetric key cryptosystem. In the former system, secret key is used to encrypt and decrypt the message. Herein, both the sender as well as recipient uses the same key whereas in the latter system, Public and Private key are used. Public key is

known to everyone and Private key is known to recipient only. When it comes to India, asymmetric key cryptosystem is used.

3. ***Use of electronic records and electronic signatures in Government and its agencies***

Section 6 of the IT Act promote the application of electronic record as well as electronic signature in government and its agencies. If any law permits, 1. the filing of an application or any document with office or authority or agency regulated by the appropriate government; 2. the grant of a licence or approval in a particular way; 3. the payment of money then in such situation the aforesaid stipulations shall be considered to be satisfied if the same is affected via means of electronic form which is specified by the appropriate government.

4. ***Retention of Electronic Record***

Section 7 of the IT Act explicitly provides for retention of electronic record. If any law suggests that documents, records or information, for a definite period, shall be retained then such stipulations shall be considered to have been satisfied if the same are retained in the electronic version.

5. ***Audit of documents, etc., maintained in electronic form***

Section 7A of the IT Act provides for the audit of documents, records or information. If any Law consist of provision pertaining to audit of documents, records or information then it shall be applied in the electronic form only.

6. ***Publication of Rule, Regulation, etc. in electronic gazette***

Section 8 of the IT Act explicitly provides for publication of rule, regulations, etc. in electronic gazette. It says that if any rule, regulation, order, bye-law or any matter shall be published in the official gazette then such stipulations shall be considered to be satisfied if it is published in the official or electronic gazette.

7. ***No Right to insist any Document ought to be accepted in the electronic version***

Section 9 of the IT Act states that nothing envisaged under section 6,7 and 8 of the aforesaid Act shall grant a right to any person to claim that Ministry or Department of central or State government or any such body managed or funded by the central or state government should accept any document in the guise of electronic record or constitute any kind of financial undertaking in electronic form.

8. ***Power to make rules by Central Government concerning Electronic Signature***

Section 10 of the IT Act empowers the central government to formulate certain rules concerning electronic signature. The Central government may specify the following:

(a) kind of electronic signature
(b) the method and configuration to affix the electronic signature
(c) the plan of action to expedite the recognition of person affixing the electronic signature
(d) regulate the procedure to corroborate the safety and covertness of certain electronic records or payments
(e) other important aspect obligatory to give effect to electronic signature

9. ***Validity of contracts formed through electronic means***

An E-contract is primarily governed by Indian Contract Act, 1872. The legitimacy of an e-contract depends on the fulfilment of all the basics of a valid contract namely, Offer and acceptance, Lawful consideration, Lawful object, Free Consent, Intention of Parties concerning legal relation, and Parties which are competent to contract. Section 10A of the IT Act legally recognized the validity of such contracts which are formed via electronic means. If in the formation of a contract, communication, revocation and acceptance of proposal are demonstrated in the electronic form, it shall not be considered invalid exclusively owing to the use of electronic form or means. To give effect to a valid contract, signatures of parties are necessary to corroborate the acceptance of terms and conditions pertaining to contract. In case of E-contract, electronic signature comes into picture. An electronic signature is considered correspondent to traditional wet signature and has been legally appreciated under

section 5 of IT Act. Furthermore, Section 4 of the IT Act, accords legal recognition to the electronic record. In the light of the aforesaid provision concerning IT Act, the courts have periodically affirmed the cogency of e-contract.

In Trimex International FZE Ltd. Dubai v. Vedanta Aluminium Ltd[xxviii], the Hon'ble Supreme court has said that the electronic communication in case fulfilling all the pre-requisites of Indian Contract Act, 1872, without being the implementation of a formal contract, amounts to a valid enforceable contract. Similarly, in Tamil Nadu Organic Private Ltd. and ors. v. State Bank of India[xxix], the Madras High Court had connected the provision pertaining to IT Act to an E-auction and explicitly held that legally binding liabilities may emerge via electronic means and such contract are enforceable under law.

Moreover, Under the Evidence Act, an e-contract is considered equivalent to paper-based agreement. The expression 'Evidence' under Evidence Act means all the documents including electronic records adduced before the court of law for inspection and such documents are known as documentary evidence. In Harpal Singh @chhota and Ors. v. State of Punjab[xxx], the hon'ble supreme court has ingeminated that any electronic record as a secondary evidence is not admissible per se unless the necessities envisaged under section 65B of Evidence Act are fulfilled. Thus, section 65-B provide for the evidentiary value of e-contract.

As mentioned by first schedule of the IT Act, the following dockets cannot be accomplished in the electronic form:

1. Negotiable Instruments other than a cheque under the ambit of Negotiable Instruments Act, 1881
2. Powers concerning Attorneys as explicitly expounded under the Powers of Attorneys Act, 1882
3. Trusts as defined under the Indian Trusts Act, 1882
4. Contract pertaining to Sale or transference of immovable property or any interest therein.

5. Wills/testamentary dispositions as given under the Indian Succession Act, 1925

NEED TO AMELIORATE THE CYBERSECURITY

With the development of Internet, computer-related umbrage and cybercrime have turned out to be a worldwide problem. Perversion of Internet has gained currency in several buckets namely government organizations, institutions, social media and so forth. Hackers are persistently seeking out different techniques of assaulting the information framework to alter or venture into the system. Delicate information pertaining to biotechnology, military resources, Business, etc. are undermined by the hackers. Certainty plays a critical part in building up a steady communication when volume of things transmitted in ICT environment. Two pertinent aspects ought to be taken into account concerning the framework of certainty i.e. certainty within the fundamental interaction between organizations or entities and certainty in the internet system. The integrity of ICT tools is significantly supported by components of ICT tools such as Hardware, software, etc[xxxi]. Thus, there should be a productive mechanism to delineate the certainty at length in a dynamic environment of ICT. Privacy has become one of the significant issues in ICT tools as well as services owing to pervasive nature of ICT space. Several entities are materially associated and covert information is widely transmitted as well as interchanged on the web which consequently affect the privacy of the user[xxxii]. Well-designed cybersecurity is the cornerstone to fabricate the virtual aspect of society along with others connected policies namely digital economy, digital society, networking, etc. Cyberspace has been positively recognized as a digital dimension of the society wherein information is created, amassed and transferred within the cyberspace itself. It represents the synchronization of all the societal sectors to safeguard the certain core values concerning Liberty, fairness and Rule of Law in the digital aspect of the society[xxxiii].

The expression cybersecurity includes several aspects namely accumulation of tools, stringent polices, security shields, risk management, and advanced technologies which can be used to secure the cyber environment and the resources of clients and organizations. Such resources embrace linked computing gadgets, telecommunication, and stashed data within a cyber atmosphere[xxxiv]. Upgrading the cybersecurity and securing cardinal information infrastructure

are necessary to ensure the security of nations as well as economic growth and development. Forging the web more secure has become intrinsic to the evolution of new services and government policies[xxxv].

CONCLUSION

It is conspicuous that information security is instrumental to ensure the success of e-governance. Policies covering information security considerably bolster the security of information assets. They constitute the bedrock of Information security in an organization. Procuring the adequate data at the proper time, in an organization, could make the enormous difference between consummation and non-consummation of goal. Certainly, security of data will succour the users to manage and safeguard the data from rancorous changes as well as unapproved divulgence. The security of information is fundamentally determined in the context of confidentiality, integrity and availability.

Effectiveness, Efficiency, Flexibility and Transparency ought to be discussed at length to dispense reliable service to citizens. If the citizen is to obtain the greatest advantage from the e-service via e-governance, the e-service needs to focus on the following aspects[xxxvi]:

1. The arrangements of e-service should be confidential and under any circumstances infringe the right to Privacy
2. Solely to calculated users, the arrangement of e-service sought to be available.
3. Information concerning e-service should be extensive, veritable, meticulous and easy to grasp
4. The structure of e-governance must adhere to the pertinent statutory Acts and subsisting data safety stipulations
5. The users should be well acquainted with the information in respect of available e-service.

ENDNOTES

[i] Professor Dr. Marco Gercke, understanding Cybercrime: Phenomena, Challenges and Legal Response, 1, (2012)
[ii] Ibid
[iii] Ibid
[iv] Second Administrative Reform commission, Promoting e-governance: The SMART Way Forward,1, (2008)
[v] Ibid
[vi] See Supra Note 2 at 11
[vii] Best Practice to Protect your E-commerce Business, available at https://so-cyber.com/cyber-security-for-e-commerce/#:~:text=Server%2Dside%20masquerading,to%20be%20the%20legit%20one.(Last Visited on March 7, 2021)
[viii] Ibid
[ix] Ibid
[x] Ibid
[xi] Rainbow Table Attack, available at https://www.techopedia.com/definition/30617/rainbow-table-attack-cryptography (Last visited on March 9, 2021,)

[xii] BRUTE FORCE ATTACK available at https://www.varonis.com/blog/brute-force-attack/ (Last Visited on March 9, 2021)
[xiii] Dr. (Mrs.) G. Padmavathi and S. Divya, A Survey on Various Security Threat and Classification of Malware Attack, Vulnerable and Detection Technique, 2 The International Journal of Computer Science and Applications 68,(2014)
[xiv] Shailendra Singh & Sanjay Silakari, A Survey of Cyber Attack Detection System,9 International Journal of Computer Science and Network Security 2, (2009)
[xv] White Hat Security available at https://www.whitehatsec.com/glossary/content/xml-injection (Last Visited on March 9, 2021)
[xvi] Phirashisha Syiemlieh, Golden Mary Khongsit, et. al., Phishing-An Analysis on the Types, Causes, Preventive Measures and Case Studies in the Current Situation,1 IOSR-Journal of Computer Engineering 1, (2015)
[xvii] See Supra Note 9
[xviii] Ibid
[xix] Ibid
[xx] (2005) 11 SCC 600
[xxi] (2014) 10 SCC 473
[xxii] (2018) 2 SCC 801
[xxiii] 2020 SCC OnLine SC 571
[xxiv] Electronic Signature or eSign, available at https://www.pichainlabs.com/esign-or-digital-signature (Last Visited on March 11,2021)
[xxv] Ibid
[xxvi] Ibid
[xxvii] Ibid
[xxviii] 2010 (2) AWC 1170(SC)
[xxix] AIR 2014 Mad 103
[xxx] (2017) 1 SCC 734
[xxxi] Mohamed Abomhara and Geir M.Koien, Cyber security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks, 4 Journal of Cyber security and Mobility 71, (2015)
[xxxii] Ibid
[xxxiii] Aleksander Klaic, A Method for the Development of Cyber security Strategies, 34 Information and Security Journal: An International Journal 41, (2016)
[xxxiv] The Role of ICT Regulation in addressing offenses in Cyberspace available at https://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR10/documents/GSR10-paper6.pdf (Last Visited on March 13, 2021)
[xxxv] See Supra Note 1 at 2

[xxxvi] Ministry of Communications and Information Technology, E Governance Security Standards Framework: An Approach Paper available at http://egovstandards.gov.in/sites/default/files/eSAFE%20Framework%20ApproachPaper%20Ver1.0.pdf (Last Visited on March 13, 2021)