

4 CMET (2017) 69

Cyber Terrorism: An Analysis with an Indian Perspective


by

Aditya Goyal*

INTRODUCTION

Terrorism, as a part of the 21st Century, grew as a cult with an end in itself. Terrorism instils a fear in the minds of the people against their state's inability to protect them from damage in person and property; it also creates a psychological and social havoc in the lives of people. Conventional terrorism was aimed at eroding the tranquillity and tolerance among a group of people, or more precisely to disrupt the harmonious well-being of a nation. With emerging trends in generations, terrorism has changed its shape and form, keeping pace with modern era. With the advent of the culture of the world being online, cyber-terrorism developed its roots to tackle the ever advanced techno-geek reality, forcing into the personal space of people without any visible damage. But is there any remarkable difference between conventional and contemporary forms of terrorism? What makes it different from cyber-attacks and renders it a form of terrorism? How does it affect the government and its policies? How does the law deal with it? While most of these are lethal, the question regarding their legality with respect to ethical hacking and security also arises.

Cyber-terrorism has been defined by various organisations, adding various dimensions to its scope, but retaining the crux of the problem. NATO defines cyber-terrorism as *"a cyber-attack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal."* The National Infrastructure Protection Centre defines cyber-terrorism as, *"a criminal act perpetrated by the use of computers and telecommunications capabilities resulting in violence, destruction, and/or disruption of services to create fear by causing confusion and certainty within a given population conform to a political, social, or ideological agent."*¹ The most accepted notion of cyber-terrorism is defined by FBI which defines it as, *"a premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against*

 Page: 70

*non-combatant targets by sub-national groups or clandestine agents."*² A close analysis of these definitions reveals some common aspects of cyber-terrorism which are inherently present in it - fear, political association and/or ideological influence. What can be gathered is a simple line-up for this term, i.e., *Cyber-terrorism is a technologically transmitted crime with intent to destroy or affect a set of information which is politically, morally or ideologically undesired by a group or race of people and to create a sense of fear so as to stop its future perpetuation.* While cyber-terrorism is more or less assumed to be a form of hacking, the latter is subsumed by the former and thus encompasses a much wider centre-stage.

Conventional v. Cyber Age Terrorism

While most of the scholars believe that terrorism is a term which brings with it destruction, deaths, and devastation, the cyber-world of terror attacks is incapable of

such level of desolation. The conventional mode uses more of physical warfare and weapons, including both men and matter, in order to gather more fear and pressure, and sometimes to give effect to their own macabre ideology. Scuttling of peace attains topmost ground in a terror instance. On the other hand, the 'cyber enabled terrorism' uses virtual mode to delve into the lives of people and disturb them psychologically and financially. It uses a more formal approach of maliciously transmitted viruses and ransom wares. The motive behind cyber-terrorism is usually not personal, and this is what differentiates it from cyber-crime. The end result of cyber-terrorism may include shut down of networks, money extortion for terrorism purposes, stealing of information, and hacking of government systems. Just like the recent instance of 'Wannacry' ransom ware that hit more than 150 countries and demanded payment of 'Bitcoins', another cyber-related terrorism. The 'Flame' malware that hit the Middle-Eastern countries in 2012 is also an example of cyber-terrorism. Although, this form of terrorism is not as much devastating as its other counterpart, it is gaining more ground due to its other attributes, that is to say that it is comparatively easier to spread with no costs and no limits. Also, the identity of the perpetrator can be concealed along with his/her location. Cyber-terrorism has thus created a niche for itself with it being the 'new' normal.

FORMS OF CYBER-TERRORISM

With the advancement in the technological world, the cyber related crimes are on an increase with every coming day and it is humanly impossible to attempt a categorisation of the same. Cyber-terrorism can acquire new dimensions, with an edge in almost every sphere and thus, the types



of crimes are endless. While we await newer forms to dig up, the following forms are not hard to compile:

Privacy Violation

Every individual has a right to live in privacy and the right to be let alone. The Right to privacy gained recognition under Articles 21 and 19(1) (d) of the Indian Constitution in post-Maneka era. Also, privacy is an independent and distinguished concept recognised by the tort law, although it is not exercised much in India in that context. As 'Privacy' has now gained status of fundamental right³, it is well protected by both civil and criminal consequences. With the dawn of solidarity-oriented culture, people have become more and more sensitive to the invasion of their personal space, not only physical but also mental. To cope up with this intrusion done by information technology, the legal society has evolved a fresh new outlook, although not so advanced. Privacy violation may include information access without the consent of the person or the organisation involved, or passing off of information by an agent to a person not authorised to do so. Cyber-terrorism invades the right to privacy of an individual. The acts of cyber-crime are a threat to personal information and activities of a person and can be treated as a form of cyber-terrorism. It may include phishing, hacking of accounts, transmission of viruses etc.

Data Theft and Misappropriation

Cyber-terrorism also aims at leaking out confidential information not only of private individuals but also of the government and other agencies. Such information may be of national importance and of vital nature with respect to the security and defence of a country. It can be used by terrorist outfits to facilitate their objectives and to further facilitate their infiltrations by finding the probable lacunae in the system. The same

may be used to destroy property which is public or private, movable or immovable, and tangible or intangible. Data misappropriation is another tool of cyber-terrorism to tackle the odds. Data on a source can be manipulated to gain access to a particular object, while denying the same to the owner. This renders the security systems useless and puts information under seize.

Demolition of e-Governance Base

The e-governance is the main source of interaction between state and its citizens. The right to information is also an outcome of the e-governance. While it facilitates transfer of information on one hand, it also helps in raising voices and opinions on particular policies and actions. The government



Page: 72

acts as a custodian of public information, ranging from personal information of its citizens to data related to their public activities. The public has a right to information; however, it is not an absolute privilege to them. The Hon'ble Supreme Court of India in *People's Union for Civil Liberties v. Union of India*⁴ held that the government can withhold information related to various matters on certain grounds. While most of this information is in hard-copy form, the digital version is susceptible to a probable cyber-attack. Such an attack could cause a complete demolition of this established e-governance base.

Distributed Denial of Service Attack

Distributed Denial of Service (*hereinafter* DDoS) is a kind of attack where-in multiple 'infected' computer systems or servers attack another system or server, which causes the affected computer to 'deny' service to the user. The affected computer is actually flooded with endless data and information which causes the server to slow down or crash, which further causes it to stop working and denies the service requested or required by the legitimate user of the server. This works as an interlinked web of infections spreading from one system to another vulnerable system and finally attacking a single targeted system. The purpose of using multiple systems to attack a single system is manifold; first, it becomes impossible to block all the infecting systems, and second that multiple systems transmit large amount of traffic, so the collapse of infected system is ensured. Such an attack causes a communication break between various heads and also leads to monetary losses. On a national level, a DDoS can cause system slowdown and hinder efficient administration by the government, while at the same time hovering as a constant threat to national security and integrity.

CONVENTIONS ON CYBERTERRORISM

The international community realised the challenges posed by cyber-terrorism; and to address them coherently, various conventions and treaties were signed in the past decade or so, while various other international bodies also recognised and identified the threats situated by the cyber related crimes. Some of the major instances are enumerated below:

Convention on Cybercrime

Also known as The Budapest Convention, this convention in the year 2001 is considered as the first international convention aiming to combat cyber related crimes in a sync with international and national laws. It was drafted by Canada, South Africa, Japan and USA and since India was



Page: 73

not included in the drafting of the convention, it declined to adopt it. This convention has 56 signatories and the primary objective of this convention was to harmonise various national laws to effectively combat cyber-terrorism. Substantive law relating to cybercrime along with the procedural and jurisdictional aspects thereof is contained in Section 1, Chapter II of the Convention Treaty.⁵

It is still debatable whether India should adopt the Budapest Convention, but given the mounting instances of cyber-terrorism in India and providing thrust to the Digital India campaign of Indian Government, it has become more of a necessity rather than an option for India. According to the National Crime Record Bureau, a total of 9,622 cases of cyber related offences were recorded in India in the year 2014 under the Information Technology Act, Indian Penal Code and various local laws, with an increase of 69% from 2013. Further, with the Supreme Court going paperless with the Integrated Case Management Information System (ICMIS), all the litigation related data could be retrieved online, and this positive step also stresses upon the importance of a more secure cyber world and thus India should sign the Budapest Convention. It is an undisputed fact that the benefits of joining the convention outweigh its concern of not being an original signatory.

Twenty-second G-7 Summit on Cybercrime (1996)

The G-7 Summit held in Leon, France in July 1996 witnessed the commitment by the member nations to accelerate mutual consultations and co-operation through appropriate bi-lateral and multilateral meetings on encryption that allows lawful government access to data and communications in order to prevent the instances of cyber-terrorism while at the same time protecting the privacy of legitimate communications.⁶ The focus of the deliberation was on protection of security of IT related information, privacy violation and protection of intellectual protection rights. In the recent G-7 Summit on 26-27th of May, 2017, held at Sicily, Italy, the issue of terrorism was also put forth with a special focus on admonishing internet service providers and social media companies to substantially increase their efforts to rein in extremist content.

World Summit on Information Society

The world summit on information society held in 2006 created Internet Governance Forum (IGF) to bring various stakeholders within the ambit of on-going discussions related to the internet. It is convened under the Secretary-General of United Nations.



Seventh International Conference on Cybercrime (2007)

The Seventh International Conference on Cybercrime was held on September 12, 2007 in Vigyan Bhawan, Delhi (India). The conference focused on the need for spreading cyber security awareness and evolving effective preventive measures to combat cyber criminality, with a special emphasis on cyber-terrorism activities and organised crimes through internet. It also stressed upon the need for new investigation techniques to tackle this online menace.

CYBER-TERRORISM INSTANCES

There have been many cyber-terrorism instances around the world, while there has been an upsurge in the recent past. Some of the notable instances of cyber-terrorism are enumerated below:

- In 1998, the ethnic Tamil guerrillas swamped the Sri Lankan embassy with more than 800 mails a day for a period of two weeks. Intelligence authorities characterised it as the first ever cyber-terrorist attack against the country.
- Crackers in Romania once gained illegal access to computers, taking control of the life supporting system at an Antarctic Research Centre, endangering the lives of the scientists working there.
- In May 2007, Estonia was subjected to a mass cyber-attack in the Russian Federation which was alleged to be instigated by the Russian government, but denied by it.
- On July 26, 2008, a series of 21 bomb blasts hit Ahmedabad within a time span of 70 minutes with a total of 56 reported deaths and about 200 injured. Several news agencies reported receiving an e-mail from an Indian Mujahideen stating revenge for Gujarat. The terrorists hacked routers to send emails and this was a terror attack which used the internet as a medium. Although it is not a cyber-terrorism act in itself, but it certainly explains the complexity and gravity of the situation. Similar was the situation in the 26/11 Mumbai terror attacks where 'callphonex' was used for communications between the terrorists.
- Recently, a ransomware cyber-attack, that may have originated from the theft of 'cyber weapons' linked to the US Government, hobbled the hospitals in England. Its effect was recorded in more than 100 countries.
- 'Pakistani cyber army' is a group of hackers in Pakistan who are known for their defacement of websites. Some noticeable



instances are hacking of BSNL, CBI India and Kerala State's websites.

- Groups such as G-Force and Doctor Nuker, have attempted to deface and hack the websites of some of the most prominent institutions in India, namely The Indian Institute of Science, Bhabha Atomic Research Center. These groups are based in Pakistan. Many other instances of online terrorist recruitments have risen in the recent past.
- The recent instances of ISIS terrorism are perfect examples of cyber-terrorism. The videos released by them are potential cyber threats and the way they have intruded into the systems of major countries poses a serious question to the vulnerability of the security systems. Furthermore, the beheading videos of various journalists and social activists created a sense of psychological fear in the minds of people.

LEGAL ASPECTS

With the internet becoming a hub for illegal activities, the dimension of cyber-terrorism is touched by legal impressions in numerous ways. Apart from the fundamental problems of defining "terrorism", there are several other legal issues like protection of human rights, the legality of investigation tools and instruments, applicability of criminal and international law and other related provisions, appropriate legal response mechanism, and so on and so forth. Another challenge is related to the identification of suspects. Some countries have adopted the means of legal restrictions to address this challenge.² For instance, in Italy, public internet access providers are required to identify and verify users before granting them access to internet.⁸ While the most floated legal response to cyber-terrorism is criminalising all the relevant acts, there can be two approaches in this aspect. One, that the cyber-terrorism provisions be inserted in the cyber-crime related laws, or second, that a different specific

legislation be passed for it.

Presently, the provisions related to cyber-terrorism are contained in section 66F of the Information Technology Act, 2000 and this is the only legislation governing cyber-terrorism in India. Section 66F of the said act reads that whoever intends to threaten the unity, integrity, security or sovereignty of the country or intends to strike a sense of terror in the people using



Page: 76

electronic media and by such means causes death or instils a fear of its causation and/or accesses restricted information which is against the interest of India, is said to commit the offence of cyber-terrorism. The entire cyber-terrorism law in India can be summarised in this reproduced section from the Information Technology Act, 2000.⁹

Section 66F- "(1) *Whoever, —*

(A) *With intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by—*

- (i) *denying or cause the denial of access to any person authorised to access computer resource; or*
- (ii) *attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or*
- (iii) *introducing or causing to introduce any computer contaminant, and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under Section 70; or*

(B) *knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to 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, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber-terrorism.*

(2) *Whoever commits or conspires to commit cyber-terrorism shall be punishable with imprisonment which may extend to imprisonment for life."*

The IT Act makes a departure while defining cyber-terrorism as compared to the conventional cyber-terrorism definitions. It contemplates two broad categories as to how cyber-terrorism can be caused. The first, being an act which threatens the unity, integrity, security or sovereignty of India.



Page: 77

However, this act alone does not constitute cyber-terrorism and it must be accompanied by either (i), (ii), or (iii) clause mentioned above. That is to say, there should be a fear of death or disruption of supplies or services essential to life. The

second arm of this provision is contained in clause (B), consists of a person, (i) knowingly or intentionally; (ii) penetrating or accessing a computer resource; (iii) without authorisation or exceeding authorised access; and (iv) by means of such conduct obtaining access to information, data or computer database; (v) which is restricted for reasons of the security of the state or foreign relations. It may also be committed when a person is (i) knowingly or intentionally; (ii) penetrating or accessing a computer resource; (iii) without authorisation or exceeding authorised access; and (iv) accesses any restricted information, data or computer database; (v) with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury; (vi) to 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, or to the advantage of any foreign nation or a group of individuals.

The section has a very broad ambit when it comes to the scope of cyber-terrorism. The inclusion of the terms such as 'defamation' and 'contempt of court' seems vaguer than being broader. It fails to provide any nexus between them and the offence discussed. However, it misses out on most of the other aspects of cyber-terrorism, like privacy violation, human rights violation, personal information thefts etc. Again, it uses ambiguous terms like decency and morality which are hard to relate. The only provision on cyber-terrorism in the Indian legislative gamut seems to be more of a skeleton section, missing out on the nuances which are the essence of the offence sought to be controlled. It ignores the psychological effect that cyber-terrorism has on the minds of people, which is one of the most inevitable outcomes of terror attacks. As noted earlier, cyber-terrorism is also a kind of terrorism, with more sophisticated means and resources at its disposal, and therefore must be dealt with more advanced and dedicated provisions, if not similar to that of conventional terrorism. One more important aspect of cyber-terrorism, which is often neglected, is the problem related to electronic evidence which again goes unaddressed by the present provisions even in India. Securing e-evidence is an increasingly complex undertaking.

Article 21 of the Indian Constitution states that no person shall be deprived of his life or personal liberty except according to procedure established by law. Right to privacy is a fundamental right under Article 21. While terrorism causes a fear of destruction in the mind of an individual, it also infringes the right to privacy of an individual which is a fundamental right. Article 12 of the Universal Declaration of Human Rights states that no one shall be subjected to arbitrary interference with his privacy, nor to



attacks upon his honour or reputation.¹⁰ "Privacy" is defined as "*the quality or state of being apart from company or observation*" and protection from unwarranted intrusion. Cyber-terrorism intrudes into the minds and psychological well-being of the people, while being a constant threat to their personal data and computer space. It violates the very fundamental right of an individual to have personal space. Thus, while it can be stated that cyber-terrorism may infringe the fundamental right to privacy, it becomes all the more necessary to make provisions for the same.

JUDICIAL RESPONSE

The Judiciary has a very important role to play when it comes to controlling the menace of cyber-terrorism. With the advent of judicial activism, or rather judicial

adventurism, the Indian Judiciary has got a new dimension to venture into. The first issue which the Judiciary may face is of jurisdiction as before going into the merits, it should be satisfied that it has the requisite jurisdiction to do so. Since internet is not a 'single-entity owned or government operated', it cannot be regularised as an ordinary crime by invoking the jurisdiction. Again, the cross-border terrorism may also give rise to the problem of jurisdiction. The Indian Judiciary may have the jurisdiction to deal with these cases if the victim is in India, and/or the perpetrator is present in India, or the cause of action lies in India, or if the primary effect of the attack is on India. Another situation may arise when none of the given situations are present, but extraordinary circumstances are present and the country's sovereignty or security is at stake. In that case too, the Judiciary may have the jurisdiction to take up the matter. Otherwise also, section 1(2) read with section 75 of the Information Technology Act, 2000¹¹ gives courts the jurisdiction to deal with matters outside India.¹²

Apart from the jurisdictional matters, the Judiciary should also be well equipped with appropriate and adequate laws to decide the matters with utmost strictness and provide harsh and deterring punishments to the originators of these attacks. An active Judiciary must be backed with laws that are generic and living in nature, further watered by way of precedents. Lack of precedents causes hindrances in development of the law as without judicial interpretation, the law remains confined to its literal meaning and there is little scope to fill up the lacunae therein. The role of Judiciary must be supported by the whole lot of citizens and netizens who reap the benefits of internet but are targeted as victims. But at the same time, it is the duty of the court to ensure anonymity and security to them.



THE WAY AHEAD

Prevention is always better than cure. Now that cyber-terrorism has become an indispensable aspect of the cyber world with new facets and dimensions, it has rightly earned a space in cyber related laws and deserves provisions, separate from those of minor cyber-attacks. The intensity of cyber-terrorism has actually thickened with every advancing moment. What actually necessitates the need for a separate, fully-regulated law of cyber-terrorism is that the instances of the same are now well-versed, with well-defined nuances to it, and thus having only a single provision in the entire legal system would be like encouraging threats to hamper the national security and integrity. Cyberspace is a channel through which people react, interact, and transact, and this phenomenon has become a culture in modern times. It may be noted that certain amendments have been made to various statutes to make them compatible with modern times and to give effect to the provisions of Information Technology Act, 2000. Some of these amendments are made in the Indian Penal Code, 1860, the Indian Evidence Act 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934. Again, the executive can also roll out rules as notifications to tighten up the grip on cyber usage. This doesn't mean restricting the internet usage for general public, but simply making rules for verification, application or access of the internet. These rules are not only to be made by the Central Government but also by the state governments. A perfect example for this can be seen in Karnataka where the government has rolled out the Information Technology (Karnataka) rules 2004 which make it mandatory for the user to provide his identity before being allowed to access internet at a cyber café. It also provides for the liability of the cyber café's owner to make sure that the internet is not used for illegal activities. However, none of the legal

systems is short of any lacunae, but the one with a modern and collaborative approach can make a mark in the legislative reforms. There is a need to address this issue not only by the legislative bodies, but it may go well with technical experts, foreign collaborations, advanced security providers and of course there is a strong scope of developing legal acumen and nurturing intellectual scholarship in this field by way of extensive research.

A more vigilant citizenry can actually contribute to the development of law relating to cyber-terrorism. It is their active participation which can help in coping with this crime. The general public should undertake effective protective measures and report the instances of such crimes to the concerned authorities. More number of cited instances gives thrust to the ongoing debates on the issue at hand and contributes to the development of allied areas of study. Also, in case of India, it can make use of the SAARC forum to evolve consensus among the member nations about the need for curbing this cyber-criminality, especially cyber-terrorism, and build out a research



and development undertaking to put a stop to all possible terror related activities conducted online. A plethora of Research and development can actually provide many other useful insights into the problem and the benefits reaped from this will outweigh the initial costs involved. Simply looking into the minds of other countries is the sign of an incapability. What is actually required is that along with the legal dimensions, other important aspects of cyber-terrorism must be looked into, paving way for innovation and invention. Just as Facebook launched a program in the United Kingdom to train and fund local organisations to combat extremist material online, Indian companies can also take similar steps in this direction.

CONCLUSION

Efforts should be made to make a comprehensive law with both national and international approach to stop cross-border cyber-attacks with a smooth mechanism for redressal. Adopting a mutual code of cyber legislation can go a long way as cyber-terrorism knows no borders and thus, a well incorporated mechanism must be evolved. If internet can be used to spread terrorism, the same can be used to tackle it also. The Ministry of Electronics and Information Technology, Government of India's 'e-security' scheme is a well applauded step in this direction. While there can be various approaches to deal with this issue, the one provided in the United Nations' Counter Terrorism Implementation Task Force seems to be the most rational and practical one. According to Counter-Terrorism Implementation Task Force (CTITF), working group of UN, this proposition should be approached by a multi-disciplinary approach, involving experts in counter-terrorism, technology, law, public policy, law enforcement and human rights. As a single agency cannot deal with this issue, in the same way, a single legislation may not serve the purpose. Cyber-terrorism control can be put onto other Acts as well. For instance, online frauds because of online transactions and contracts can also come under the ambit of the Indian Contract Act, 1872 and the Sale of Goods Act, 1930. Protection of intellectual property is also one of the major problems in this era, be it inventions, formulae, movies, books, ideas or recipes and so on and so forth. The Indian Copyright Act and the Indian Trademarks Act may be altered to invoke special attention to this issue with respect to cyber-terrorism. As far as other illegal activities on the internet are concerned, while the Information Technology Act penalises them, other legislations may govern them. A specific legislation for this purpose may solve the problem to an extent, but as the gamut of cyber-terrorism is expanding, a holistic legal development is required to tackle this

issue effectively. This may demand amendments in the existing statutes, a lot more oriented research and development, combined with the ability of secure technology, an active government agency and an open-eyed Judiciary.

* Student, 2nd Year, BA LLB (Hons), National Law Institute University, Bhopal.

¹ NIPC, 'Cyberterrorism: An Evolving Concept. National Infrastructure Protection Centre' (*National Infrastructure Protection Centre*, June 2015) <www.nipc.gov/%20NIPC> accessed 20 June 2017.

² Title 22 of US Code, s 2656 f(d).

³ *KS Puttaswamy v. Union of India*, (2017) 10 SCC 1: 2017 SCC OnLine SC 996.

⁴ *People's Union for Civil Liberties v. Union of India*, (2004) 2 SCC 476 : AIR 2004 SC 1442.

⁵ ETS 185 Convention on Cybercrime 2001, chap 2 ss 1(2)-(13).

⁶ RK Suri and TN Chhabra, *Cybercrime* (1st edn, 2001) 279.

⁷ M Gercke, 'Understanding Cybercrime: A Guide for Developing Countries' (*International Telecommunication Union*, March 2011) <www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU_Guide_A5_12072011.pdf> accessed 26 September 2017.

⁸ 'Urgent measures for combating international terrorism' (*Decree-Law*, 27 July 2005) <www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026> accessed 26 September 2017.

⁹ Information Technology Act 2000, s 66F.

¹⁰ Universal Declaration of Human Rights, art 12.

¹¹ Information Technology Act 2000, s 1(2).

¹² Information Technology Act 2000, s 75.

Disclaimer: While every effort is made to avoid any mistake or omission, this casenote/ headnote/ judgment/ act/ rule/ regulation/ circular/ notification is being circulated on the condition and understanding that the publisher would not be liable in any manner by reason of any mistake or omission or for any action taken or omitted to be taken or advice rendered or accepted on the basis of this casenote/ headnote/ judgment/ act/ rule/ regulation/ circular/ notification. All disputes will be subject exclusively to jurisdiction of courts, tribunals and forums at Lucknow only. The authenticity of this text must be verified from the original source.