IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

ECONOMIC CRIMES IN THE AGE OF TECHNOLOGY

Radhika Sharma, Dr Savita NayyarPh.D Scholar, Professor Department of Law
University of Jammu, Jammu, India

Abstract: The concept of economic crimes has come a long way since its conception, from being first introduced as "white collar crimes" a "phenomenon of law breaking by "respectable" persons in the upper reaches of society" coined by American Sociologist Edwin. H. Sutherland to acquiring several forms in the wake of globalisation and liberalisation.

These crimes in the 21st century however, have cruised behind past the perimeter of business and trade thereby obsoleting the term "white collar crimes" which is deficient and unsuitable to detail all the forms of economic deviances found.

The magnitude and enormity of such crimes has undergone immense change by reason of highly advanced and enhanced means of transport, communication and technology development. With the advancement in the technology and more use and reliability of computer machines in various businesses and government installations not only has the quantum of these crimes increased but the nature of such crimes has also become increasingly digitised.

While most of these crimes are majorly regulated by the Indian Penal Code and several special laws enacted over the years. There however, at present is no unified law to deal with such crimes. Given the increasing digitisation of such crimes the Indian criminal jurisprudence is found to be lacking. To address this void in literature the first part of this paper will trace the history of economic crimes from white collar crimes to becoming more digitised in this day and age. The second part will critically analyse multifarious laws and they're interrelationship. The third part will critically analyse whether the Information Technology Act, along with Indian penal code is sufficient to deal with the new phenomenon of "cyber economic crime" and lastly the paper will conclude with a few suggestions.

Indexterms: Economic crimes, cyber economic crimes,Indian Penal Code,1860, Information Technology Act,2000

INTRODUCTION:

A silent revolution has taken place in the criminal law as well as the law enforcement theory dating back to the nineties.1 English philosopher and political theorist John Stuart Mill in the nineteenth century propounded that the only time government should interfere with people's liberty is when it is necessary to obviate harm to others.2 As per Stuart's harm principle, the State can impede with the liberty of an individual only in two circumstances i.e. to intercept behaviour that causes or threatens harm to others or to prevent harm to others.3 In line with the harm principle, the state got in the way of individual liberty, only for those crimes which caused a direct harm to an identifiable victim. Since direct harm to an "identifiable victim" was at the core of the punishment under the old paradigm, the absence of an injured victim usually meant that the offenders were entitled to relish the yields of their crimes.4

However, post Second World-War era, Mills harm principle underwent a change. There was a rise in new types of crimes which were more economic in nature, which the existing criminal justice system was not accustomed to addressing. Such crimes were different from the traditional crimes in differing aspects for instance:

- they were avaricious crimes that produced huge profits,
- they did not appear to cause any direct harm to any identifiable victims though, offenders couldreap benefits from them,
- There was absence of an identifiable victim, proving traditional legal instruments, to be of limitedutility in judicial attempts to seize the proceeds of economic crimes and
- lastly, because of the extensive means obtainable for camouflaging the proceeds of economiccrimes, it was remarkably onerous to trace and directly link them to their original source.5

Today in the 21st century a new reality has set in for the society as white collar crimes and technology enabled crimes have become indistinguishable. As a result the experts battling white collar crimes face the inevitable challenge of aligning their operational capabilities and defenses.6

White-Collar Crime is a field distinguished by sharp changes. It is also a field with many unforeseeable, contrary and shifting norms. These circumstances make it even more significant to inquire into the changes and progression of economic crimes in a long historical standpoint.7 With the economy increasingly becoming more international, different national systems of legislations control and norms meet through their clash. However, attempts are being made to create common international regulations to combat such crimes.8

In the history of crimes economic crime has not attracted much attention. Conventionally economic crime is not treated as a distinct category in historical studies. Violation against tax, custom or trade regulations are often included in other categories as 'crimes against the authorities', 'violations against the state

regulations', or 'property crimes".9

Economic crime is simply identified as violations against economic regulations and the category is composed of several different types of violations. Most of them concern different trade regulations, which may include acts as different as cheating customers (by forgery, by using false measures and weights, by selling goods already bargained for and so on), nonpayments of customs and toll duties, violations of ban on export and different types of unlawful trading (such as trading in the rural areas against town privileges, unlawful retail trading and violations against market regulations)

While crime is defined as an unlawful act against the State and has punishable sanctions. The term "economic" is used generally to cover activities pertaining to the economy. Putting the words together the term "economic crime" is relatively unfamiliar.10

White collar crimes Vs. Economic crimes:

The term economic offences and white collar crimes are often used interchangeably. It was Edwin Sutherland who in 1939, for the first time introduced the concept of white-collar crime in his presidential address to the American Sociological Association, calling attention to crimes in various areas including the medical profession, the political arena, the securities industry, and the banking system, to name a few.11

As per Edwin Sutherlands theory white-collar crimes are primarily conducted using the special knowledge or the position that the offender holds in the society. The material benefits gained by immoral, un-ethnical and illegal acts using the professional or positional edge over and above the others constitutes white-collar crime. According to him they are "crimes committed by a person of respectability and high social status in the course of his occupation".12

As per his thesis the persons of the upper socio-economic class primarily engage in criminal behaviour and this criminal behaviour differs from the criminal behaviour of the lower socio- economic class. He came to regard white-collar criminals as the upper world equivalent of the professional thieves.13 White-collar crime insinuates elite crime by skilful delinquent who are often neglected of lawbreaking primarily due to the fact that:

First, that "persons of the higher socioeconomic class are politically and financially more powerfuland elude arrest and conviction to a greater extent as opposed to the person of lower class".14 Second, on arrest, white collar offenders are often treated in a fundamentally different way by thecriminal justice system:15

Herbert Edelhertz disapproved with Sutherland and argued that "the character of white-collar crime must be found in its modus operandi and its objectives rather than in the nature of the offenders." 16 From a criminal's standpoint, white-collar crime appears to be the quintessential crime: it reaps tangible rewards, there is an excellent chance of getting away with it, and seldom does an offender have to confront the victim or a ghastly crime scene. As a result, the offender normally does not experience any guilt or contrition.17

By defining white-collar crimes strictly concerning occupational and professional activities of upper strata, Sutherland narrowed the concept of white-collar crimes to the interest of Capitalistic society. Santhanam committee report found this notion too confined for the Indian context and opined that "the fabric of Indian society, whilst capitalistic has different strata with the apportioning of economy being inequitable. A "guilty" individual in such a society cannot be termed as a white- collar criminal.18

The law commission in its 29th report observed that the nature and scope of economic crimes is much extensive when juxtaposed to white collar crimes. These crimes have now cruised behind past the perimeter of business and trade thereby obsoleting the term "white collar crimes" which is deficient and unsuitable to detail all the forms of economic deviance found in India.19

Economic crimes on the other hand, unlike the white-collar crime aren't necessarily committed in connection with one's occupation. Economic crime is an umbrella term and consists of profit- motivated, illegal activities conducted within or arising out of an economic activity that is in itselflegal or is purported to be so.

Economic crimes is an offshoot of a novel form of society, a society earmarked by scientific and technological developments, a society inspired by values antithetical to the traditional values of morality. With the society growingly becoming a welfare state, there was a shift from the protection of the interest of the individual to that of the public at large i.e."collective interest". The shift in the interest of the society gave rise to an increasing need to regulate these anti-social activities.20

Although there is no universally accepted definition of economic crimes the term can be defined as follows, "Economic crimes are a manifestation of criminal acts done either solely or in an organised manner with or without associates or groups with an intent to earn wealth through illegal means, and carry out illicit activities violating the laws of the land, other regulatory statutory provisions governing the economic activities of the Government and its administration". 21

Law and White-Collar Crimes:

Today White-Collar crimes are convoluted which have garnered immense significance in this global age. Such crimes are not impulsive in nature but rather are carefully planned and performed in secrecy so as to leave no shadow of their performance.22

There has not only been an increase in such crimes but today each of such crime is more complex than the

other making the detection and prevention of such crimes a difficult task for the criminal justice system. The nature of these newer forms of crimes is such that it warrants unceasing legislative vigil.23 The Indian criminal justice system is largely modelled on the British criminal justice system which is versed in the trial and punishment of the traditional crimes. Economic crime however, is constantly evolving with its nature and dimensions undergoing an astronomical change along with the revamping of the character of socio-economic context of property and development in the information and communication technology therefore presenting challenges to the criminal justice system. 24

Economic crimes such as cheating, forgery, criminal breach of trust etc. as laid down by the Indian Penal code have acquired new forms, character as well as dimensions becoming more and more complex and difficult to detect. On the other hand the pace of criminal law jurisprudence has been slow to match the considerable rise of such crimes thereby making it hard for the criminal justice system to bring order in the society. Barring the India Penal Code, there are an inordinate number of laws that exist to ward off and take care of economic offences being imposed by varied agencies with their distinct enforcement apparatus, procedures and sanctions. Yet there has been a steep rise in the number of such crimes owing much to the public apathy towards such crimes. Neither the offender nor the society

adequately realises the harm, because of the absence of an immediate victim or an immediate tangible object of harm.25 Economic crimes being different in their nature and execution from the ordinary crimes present a peculiar problem in respect of detection, investigation, prosecution and trial.

The need of the hour is a multi-disciplinary, inter-state and transnational investigation with requisite evidentiary alterations to bring the guilty to book.26

Law regime for the economic crimes has two major sources one is Indian Penal Code, 1860 and second is Special laws enacted for specific purposes to curb the economic crimes. Indian Penal Code, 1860 is the main act which deals with the major economic crimes like Cheating, forgery, Criminal Breach of Trust or fraud and Counterfeiting. On the other hand there are several special laws, for instance Prevention of Corruption act 1988, Money Laundering Act 2002, Information technology Act,2000 etc.

Besides the Indian Penal Code, there are large number of central laws that currently exist to prevent and take care of economic offences and they are being enforced by diverse agencies with their own enforcement apparatus, procedures and sanctions. Long ago, the Santhanam Committee on Corruption (1964) had recommended that these disparate laws should be made part of a separate section of the Penal Code in order to effectively deal with them by the criminal justice agencies.27

Draft National policy on Criminal Justice as published in 2007 argued that inspite of several laws enacted to deal with economic offences it was not within the capability of the standard civil police to detect and

inquire into such crimes which calls for advanced expertise in multiple disciplines and capacity to probe trans-national transactions on a continuing basis.28

Several countries like the U.K have set up high profile Serious Frauds Offices under a criminal justice legislation to deal with major economic offences. As the investigation, prosecution and trial of serious frauds demand special expertise and modified rules of evidence, it is better to have a Serious Frauds Bureau, created under an independent Central legislation for specified offences. The Bureau should be manned by trained professionals from all the required disciplines as also investigation experts, and should have a well-designed mechanism to co-ordinate enforcement.29 Given the rate of complexity that the white-collar crimes have acquired it is natural that such crimes in time to come will entail complex transactions, legitimate and illegitimate, difficult to interpret by the ordinary police. It would require advanced technology, superior training, adequate resources and legal authority to intercede quickly, across jurisdictions. Hence the importance of a central enforcement agency and a federal (joint) criminal code.30

CYBER ECONOMIC CRIMES:

It was not until at least two decades after Sutherland published his *White-Collar Crime* tome when it was recognized how technology was beginning to shape new types of crime and since the technological revolution had not yet occurred, the term cyber economic crime had not yet been legally or socially constructed.31

Modern economies all over the world whether developed or developing are absolutely dependent upon Information and Communication Technology (IT) based information systems and Internet for their survival as well as their augmentation. An increasing trust is placed on information systems, which in turn is subjecting one to increased vulnerabilities and risks.32

The spread of the cyberspace has materialised at a dramatic pace over the last two decades, Internet invariably covers almost every location on the globe. Mobile technology and Internet has brought change in the way economic transactions are being done. Technology is moving from cash to plastic to virtual money. As a consequence, criminals have captured the lacunas of it, as an opportunity to commit the new type of crime. New crimes like cybercrimes and economic crimes are on the rise, which can be called as Cyber Economic crimes.33

Cyber economic crimes thus are those crimes, which are perpetrated using cyber technology but basically for financial gains. Virtual financial crime, Cyber economic crimes, online frauds, online cheating is nothing but cyber economic crimes with different names.34

Although economic crime is just one aspect of the crimes that can be committed in cyberspace, the damage caused thereby is however enormous. The nature of the Internet allows criminals to commit almost any

illegal activity anywhere in the world. The traditional jurisdictional boundaries are not applicable to this crime as it is borderless and can be carried out state-sponsored anywhere in the world. Crimes like cheating, forgery, criminal misappropriation, fraud etc. have become increasingly digitised whereas the criminal justice systems responding to such crimes are legacy systems. The Cyber economic crime uses various methods like socio- psychological engineering and technical tools like malware or spyware to commit the crime. It is destabilizing the trust of the users in the digital technology.35

The role and status of the offender has very little significance when it comes to Cyber Economic criminals, to put it simply there is nothing inherently "Sutherlandian" about it. Key to the white- collar crime was opportunity. With the availability of digital technology in the modern workplace and the masses a range of new criminal opportunities is created. These opportunities are not just reserved for those of high social status but equally with the ordinary workers.36

India in consonance with the Model law of E-commerce adopted by United Nations Commission on International Trade and Law (UNCITRAL) in 1996, enacted Information Technology Act, 2000, which came into force on 17 October 2000.38 As laid down in the preamble of the Act the objective of the Act was to facilitate the electronic commerce, provide legal recognition to electronic and online transactions and facilitate the electronic filling of the documents with government agencies. The Act, also provided legal recognition to the electronic signature or digital signature and made electronic contracts and agreements valid, legal and enforceable. Although there is no mention of cyber economic crime in the Act it did define some cyber crimes and provide punishments for it.38

The enactment of the IT Act brought with it amendments in several Acts like the Indian Penal Code, Indian Evidence Act, Reserve Bank of India Act, Civil Procedure Code, Bankers' Book Evidence Act and Code of Criminal Procedure to make them consonant with the technology-enabled transactions.

Major Sections of IT Act related to Cyber Economic Crimes

Chapter XI of the Act gives details of the cybercrime. The chapter contains section from 65 to 74. Each section has sub sections, which explains the offence. Following are the sections, which are mainly relevant from the point of view of cyber economic crime.

Tampering Computer Source Code: Section 65 of the act defines the tampering as "knowingly or intentionally concealing, destroying or altering any computer source code (series of computer command) used for a computer, computer programme, computer system or computer network". This provision is mainly breached in case of software piracy and illegal stealing of the source code. This section attracts

punishment up to three years or with fine of two lakh or both. 39

Offences related to Computers: Section 66 explains that contravention of provisions in section 43. It carries punishment up three years or fine up to two lakh or both. Section 66 is cognizable and bailable.40 Dishonest and fraudulent intention is the main ingredient to attract the provisions of this section as compared with section 43.

Damage to Device and Computer System: Section 43 and 43 (A) details many minute procedures and practices to be followed by individual and body corporate.41 This section mainly deals with accessing the computer, its network or system without permission of the owner. Copying, downloading of content, damaging the computer or data or contaminating the data or system using the virus or any other kind or malware also attracts this section. Alerting or manipulating the data or denying the access to the legitimate owner also attracts provisions of this act. Breach of this section attracts only penalty for the damages. Section 43 is basically for civil adjudication, but if the intention of the accused is fraudulent or dishonest, then the criminal section 66 is attracted. The dishonest or fraudulent intentions are basically to gain the wrongful gain or wrongful loss to others. Thus, these two sections are more important from the cyber economic crime point of view.

Identity Theft: Section 66 C is most important section from the point of view of economic crime and makes identity theft a punishable offence.42 Brought about in the Act via 2008 amendment mandates a fraudulent and dishonest intention. This section makes stealing of electronic signature or password, or electronically identity a criminal offence punishable with three years or fine up to one lakh. Identity theft, Phishing attacks and vishing attacks are more prominent in the Cyber economic crimes. Delhi High Court in ***National Association of Software and Service Companies (NASSCOM) vs. Ajay Sood and others (2005)*** case delivered `a landmark judgment regarding phishing case. It also defined that it is one kind of Internet fraud and person pretends to be a legitimate association like a bank and extracts personal data. The high court mentioned that there is no specific legislation for phishing, but is defined as an illegal act.

Cheating by Personation: Section 66 D mentions about cheating by personation using communication device or computer resource.43 Thus, this section prohibits the illegal use of the computer resources by others for cheating to gain wrongfully or cause loss to someone wrongfully. Impersonation on the Internet is the most common type of cheating on the internet, mostly carried out by the criminals for defrauding the gullible people. Section 66 D is most important form of cyber economic crime. This type of crime form was not covered in IT Act 2000, but was added by an amendment. It carries punishment of three years and or fine of one lakh rupees. Offense as per Section 66 D is cognizable and bailable.

Cyber Terrorism: Section 66 F provides definition and punishment for cyber terrorism. Money laundering and use of online platforms for collection, transmission and use of money for terrorism attracts this section.44

Breach of Confidentiality / Privacy: Section 72 deals with confidentiality of the service providers or intermediaries.45 This particular section provides for the protection of personal data. Illegal use of data without the consent of the customer has been defined as an offense.

Procedural Aspects of Cyber Economic Crime under IT Act:

An offensive act committed outside India: Section 75 of the act specifies that any act committed outside India which is an offense as per this act by any person irrespective of the nationality, provisions of this act are applicable.46 The nature of the cybercrimes is global; as the world is virtually interconnected and anyone connected anywhere can commit the crime. Thus, this provision especially strengthens the hands of Criminal Justice mechanism to investigate and put to trial the criminals who are carrying out cross-border crimes. This is yet another important section from the point of view of cyber economic crimes.

Confiscation: Section 76 empowers the Criminal Justice system for the confiscation of the computer resources used in the crime. 47 Main system or accessories can be confiscated under the provisions of the act. This section is especially important from the point of view of response of the Law enforcement agency for collection and analysis of the evidence and its presentation in the courtof law.

Power of Investigation by the Police Officers: Section 78 does not empower an officer not below the rank of Police Inspector to investigate the offenses as per the IT act.48 This section has large- scale impact both negative and positive on the registration and investigation process by the police machinery, as the number of the officers at this rank are very less in police department. Thus, this section is very important for understanding the police response towards cyber economic crimes. **Offenses by the companies:** Section 85 deals with the offenses by the companies. It has been mentioned that those in charge of the company may be punished for the offenses committed by the companies.49

There are no sections in the IT Act which directly covers the criminal acts like Cheating, Fraud, and Breach of Trust as enumerated under the IPC. Thus, Crimes having undertone of financial aspect draws the IPC sections of cheating, fraud, and forgery and counterfeiting in addition to the IT Act sections if the act is carried out using a computer or facilitated by the computer or internet. In case of Special Local Laws (SLL), these laws are formulated for the specific criminal act, and when such specific criminal acts are carried out using cyber technology, then they attract the IT Act and SLL sections. Thus, Cyber crimes with IPC sections and special local laws are Cyber Economic crime.

CONCLUSION:

Technology and crime are closely related to each other. The distinct ideas of cybercrime and economic crimes have combined and overlapped over the past 20 years to the point that a new trend has emerged. I.e.

"cyber economic crimes". This fusion has forced law enforcement and the legal process as a whole to struggle to stay on the technological cutting edge. The laws and regulations governing economic crimes /cyber economic crimes are extensive, far reaching, everchanging and increasingly difficult to comprehend. Economic crimes today involve complex transactions, legitimate and illegitimate, which are difficult to decipher by the ordinary police. The need of the hour is high technology, superior training, adequate resources and legal authority to intervene quickly, across jurisdictions.

Further, the accused of such crimes are well read and in the know who employ sophisticated weapons and state of the art techniques to commit the crime, not leaving any trace of the evidence behind thereby posing several challenges at the investigation stage itself. The role and status of the offender have very little gravity for crimes that have perpetrated into the cyberspace.

REFERENCES:

1. Guy Stessens, Money Laundering: A New International Law Enforcement Model (Cambridge University Press; 1stedition (2008)
2. John Stuart Mill, *On Liberty*, 21–22 (Batoche Books Limited 52, Canada,4th edition. 2011)
3. D. Lyons, Liberty and Harm to Others in *Mill's On Liberty*, 115–136 (G. Dworkin, ed. 1997).
4. Ibid
5. Ndiva Kofele-Kale , *Combating Economic Crimes: Balancing Competing Rights and Interests in Prosecuting the Crime of Illicit Enrichment ,* 33 (Routledge London and New York ed.2012)
6. KPMG International "Batteling Economic Crime and Winning Together; How to integrate fraud, financial crime and cyber security to combat threats". 4 (2020)
7. Lindström, Dag; "Historical perspectives: Swedish and international examples (2004) 89 Sjögren, Hans; Skogh, Göran, "New Perspectives on Economic Crime" Edward Elgar Publishing (2004). 8. Dharma Raj Bhusal , Economic Crime: Law and Legal Practice in the context of Nepal (2009) (University of Technology, Germany)
9. Ibid
10. Yijsoff Bin Nookl; Economic Crime in Malaysia : An Analysis Into The Changing Role of The Police (1993) (University of Stirling)
11. Brian K. Payne, White-Collar Cybercrime: White-Collar Crime, Cybercrime, or Both? 19, Criminology, Criminal Justice, Law & Society 16–32 (2018) 12.Jatin Sharma and Dr. Manu Singh, "White Collar Crime In India: An Analytical Study" 13 Journal of Pharmaceutical Negative Results 3508
13. Supra note 10, pg 23
14. Arjan Reurink; "From Elite Lawbreaking to Financial Crime The Evolution of the Concept of White-Collar Crime" 3; 2016
15. Ibid
16. Ibid
17. James Gobert and Maurice Punch; *Because They Can :Motivations and Intent of White-Collar Criminals* 98 (Springer International Publishing, 2018) 18. Government of India, Report: Committee on Prevention of Corruption, (1964).
19. Law Commission of India, 29th Report on Proposal to Include Certain Social and Economic Offences in the Indian Penal Code 1968 (February 1966)20. Mahesh Chandra, *Socio-Economic Crimes* 32 (Tripathi,1979) 21. Crime in India 1996, Chapter 17, NCRB (M.H.A), Govt. of India.

22. Supra note 1

23. Supra note7

24. Balsing Rajput , "Understanding Modus Operandi of The Cyber Economic Crime From People - Process- Technology Framework's Perspective" 5 *JETIR* (2018).

25. The Law Commission of India, 47th Report on Trial and Punishment for Socio-Economic Offences 1972. 26. Draft policy of criminal justice; Report of the Committee appointed by Ministry of Home Affairs Government of India, July 2007; Prof (Dr.) N. R. Madhava Menon, pg 16

27. Government of India, Report: *Draft National Policy on Criminal Justice* (Ministry of Home Affairs 2007) 28. Ibid

29. Ibid

30. Ibid

31. Ibid pg no 32

32. Balsing Rajput , "Understanding Modus Operandi of The Cyber Economic Crime From People - Process-Technology Framework's Perspective" 5 *JETIR 2* (2018)

33. Ibid

34. Ibid

35. Ibid

36. Hn Pontell and G Geis., International Handbook of White-Collar and Corporate Crime. 359-365 (Springer ScienceMedia publication USA, 2007)

37. The Information Technology Act,2000 (21 of 2000)

38. ibid

39. Section 65; *Information Technology Act,2000*; Tampering with computer source documents.–Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both. Explanation.–For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form. 40. Section 66; *Information Technology Act,2000*; Computer related offences.–If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine whichmay extend to five lakh rupees or with both.

Explanation.–For the purposes of this section,– (a) the word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code (45 of 1860); (b) the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code (45 of 1860). 41. Section 43; Information Technology Act,2000; [Penalty and compensation] for damage to computer, computer system, etc.–If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network,– (a) accesses or secures access to such computer, computer system or computer network 7 [or computer resource];(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium; (c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network; (d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network; (e) disrupts or causes disruption of any computer, computer system or computer network; (f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means; (g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder; (h) charges the services availed of by a person

to the account of another person by tampering with or manipulating any computer, computer system, or computer network; 1 [(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means; (j) steal, conceal, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;] 2 [he shall be liable to pay damages by way of compensation to the person so affected.] Explanation.–For the purposes of this section,– (i) "computer contaminant" means any set of computer instructions that are designed– (a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(b) by any means to usurp the normal operation of the computer, computer system, or computer network; (ii) "computer data-base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network; (iii) "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource; (iv) "damage" means to destroy, alter, delete, add, modify or rearrange any c(iv) "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means. 1 [(v) "computer source code" means the listing of programme, computer commands, design and layout and programme analysis of computer resource in any form.]

Section 43A; Information Technology Act,2000; Compensation for failure to protect data.–Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.Explanation.–For the purposes of this section,– (i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities; (ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;

(iii) "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.] 42. Section66C; Information Technology Act, 2000; Punishment for identity theft.–Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh. 43. Section 66 D; Information Technology Act,2000; Punishment for cheating by personation by using computer resource.–Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees. 44. Section 665; Information Technology Act,2000; Punishment for cyber terrorism.–(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 data base that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or

computer data base, with reasons to believe that such information, data or computer data base 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.

45. Section 72; Information Technology Act,2000; Penalty for Breach of confidentiality and privacy.–Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

46. Section 75; Information Technology Act,2000; Act to apply for offence or contravention committed outside India.–

(1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality. (2) For the purposes of sub- section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network locatedin India.

47. Section 76; Information Technology Act,2000 Confiscation.–Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made thereunder has been or is being contravened, shall be liable to confiscation: Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made thereunder, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorised by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made thereunder as it may think fit.

48. Section 78; Information Technology Act;, 2000; Power to investigate offences.–Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), a police officer not below the rank of 1 [Inspector] shall investigate any offence under this Act.

49. Section 85, Information Technology Act,2000; Offences by companies.–(1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly: Provided that nothing contained in this sub-section

shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that

he exercised all due diligence to prevent such contravention. (2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly. Explanation.–For the purposes of this section,– (i) "company" means any body corporate and includes a firm or other association of individuals; and (ii) "director", in relation to a firm, means a partner in the firm.