Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2023 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

Regulation of Cybercrimes and Penalties: A Comparative Analysis

Tisha Bansal[a]

[a]Llyod Law College, Greater Noida, India

Received 20 August 2023; *Accepted* 11 September 2023; *Published* 15 September 2023

This Paper contends that cybercrime is a category of offence that implicates a computer and a network or system where the internet and computers enact a semantic role in the accreditation of crime. It elucidates the cybercrimes in India, Australia and Saudi Arabia. This research paper furnishes a meticulous analysis of types, statistical data and recent cybercrimes. Nowadays, particularly the young generation squandering computers or networks so, this paper is to make enlightenment regarding cybercrimes in distinct parts of the world. As everyone appreciates cybercrime may outrage someone's surveillance and pecuniary health so this paper examines escalating cyber security by awaking people. This research paper accentuated on connection between cybercrime and community. Criminals perpetrating crime are burgeoning constantly with the density of the population using e-banking. So, this paper will inspect the boost of cybercrimes in India along with other parts of the world. It also furnishes recent scams committed by wrongdoers related to computer networks. Ultimately this paper furnishes penalties for various countries perpetrating an offence of cybercrime.

Keywords: *cybercrime, cyber security, acts, crimes, penalties*.

INTRODUCTION

The Internet in the contemporary world is determined as a basic requisite, equivalent to food, water and shelter. It is similar to oxygen for surviving generations. Utilizing more access

networks led to habituation. The Internet is a cardinal part of mankind as it also directs positive and negative functions. Positive functions in the sense it administers rich or deep information and proficiency etc. whereas negative function in the sense of upsurges in offence of cybercrimes. Now the question arises what specifically are cybercrimes?

Cybercrimes are executed utilizing computers and information technology with the ulterior motive of indicating humankind, enterprise and collective or even administration or authority. Cybercriminals do all their illicit data processor exertion or scams in terms of the 'Dark Web'.[1] These crimes are substantially executed with the intent of generating money through persuasions or peculating statistics and merchandising them to obnoxious parties or contenders. These crimes are not only executed to procure pecuniary interest but can be rendered for special consideration and administrative reasons also and alike to terrify mainspring security. Mainspring, why cybercriminals are committing these offences, is a part which we will examine henceforth. The definition of cybercrimes is not categorized in any Act however any misconduct that is cybercrimes and their infliction is cited in the Information Technology Act 2000.[2] Many grounds led to cybercrimes such as counterattacks, capital gain, inattentiveness operator, instigation, gratification, blackmailing, civic and sectarian Revenge etc. Various infliction have been put in motion to prevent cybercrimes under the Information Technology Act 2000 which we will examine henceforth.

Cybercrime is done with the help of 'Computers' and 'Computer Networks'. What exactly are they? According to The Information Technology Act 2000 definition of a computer is 'Computer' means 'any electronic magnetic, optical or other high-speed data processing device or system that performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a

[1] 'What is Cybercrime? Types, Examples, and Prevention' (*Cyber Talents*) <https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention> accessed 08 August 2023

[2] Vishwa, 'All about classifications of cyber crimes' (*iPleaders*, 04 September 2022) <https://blog.ipleaders.in/all-about-classifications-of-cyber-crimes/> accessed 08 August 2023

computer system or computer network[3] and 'computer network' means the interconnection of one or more computers through —

1. The use of satellite, microwave, terrestrial line or other communication media;
2. Terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained.[4]

TYPES OF CYBERCRIMES

Cyber Terrorist: Computers accumulate peculiar, enterprise and the empathetic details of an individual. The hacker with the motive of personal avenge or for merriment, for fiscal gain, executes this offence of cyber terrorism to get recognition of information. Cyberterrorists by this can supervise every exertion done by individuals, enterprises etc. This not only troubles humanity, capitalistically but also miserably.

Breach of Account Security: This can be said to the offence in which a person's peculiar information like credit card numbers, secluded image, social assistance, debit card number and other perceptive insight. This offence is executed for fiscal gain and as a result, loss occurs to the person whose account gets breached.

Cyber Obscenity and Cyber inculcation: In this contemporary world, cyber obscenity or pornography is executed. Here in this offence, the perpetrator brings about an emotional attachment with a youth with the intent of child trafficking and child maltreatment for financial gain. As a repercussion of unlawful acts of cyber obscenity youth are obscenely exploited and offenders record the video and create fear in the mind of youth of webcasting it.

Cyber-Bullying: This is an offence engaged virtually in which intruders stalk sufferers and blackmail and demand ransom which causes nervous exhaustion. As an outcome of this wrongdoing and because of defamation sufferers commit suicide and are sometimes prone to depression at a young age.

[3] Information Technology Act 2000, s 2(I)
[4] Information Technology Act 2000, s 2(j)

Processor Annihilation: These are the telecommunication cybercrimes where malware-based applications are equipped in innocent people or corporation computers. They intend to accomplish deleterious ventures such as obliterating hard drive input or withdrawing identification and confidential passwords.

Defrauding Information: It is also known as Data Diddling. It is a sort of offence in which data is modified to induce trouble or obscure deceptive actions. Fluctuating data blundered, revamping data subject matter, or expunging data. The repercussions of defrauding information are pecuniary fall-off defamation, etc.[5]

Swindling of Calls/ E-mails: Fraud call is called Phishing. In this sort of offence, the wrongdoer reaches you via forged messages, calls or e-mails and professes some perks for its efficient delegation. They ask for exclusive particulars of accounts like details of Credit Card, Debit Card, OTP, Password, ATM card etc. With the motive of transaction and consequently the impact of all this is scam and depletion of fiscal or vacate account.

Distributed Denial of Service Attacks (DDoS): It is a sort of cyberattack that strives to generate an internet site or web database and intends to impede the usual flux of the intended server or web by immersing the target with a rush of internet flux.[6] The consequences of this DDoS attack are depletion of finances and faith of emptor, deterioration of external fame.

Salami Attacks: A salami attack is a classification of pecuniary deceit that prompts the embezzlement of a slight quantum of money from an enormous figure of accounts. The ambition of this category of attack is to abstract a limited sum of money from various bank financial records over a prolonged duration in sequence to evade revelation.[7]

---

[5] 'What is Data diddling?' (*Tutorialandexample*, 31 March 2023) <https://www.tutorialandexample.com/what-is-data-diddling> accessed 08 August 2023

[6] 'What Is a DDoS Attack?' (*Akamai*) <https://www.akamai.com/glossary/what-is-ddos> accessed 09 August 2023

[7] 'Salami Attack: What it is and how to avoid it?'(*Codedamn,* 02 January 2023) <https://codedamn.com/news/cyber-security/salami-attack-what-it-is-and-how-to-avoid-it> accessed 09 August 2023

PENALTIES OF OFFENCES

According to The Information Technology Act 2000 penalties for the offences include the following:

Section 65: Tampering with computer source documents: Whoever knowingly or intentionally conceals, destroys, alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer program, 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.[8]

Section 66: Hacking with a computer system: (1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack; Whoever commits hacking shall be punished with imprisonment of up to three years, or with a fine which may extend up to two lakh rupees, or with both.[9]

Section 67: Publishing of information that is obscene in electronic form. Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.[10]

[8] Information Technology Act 2000, s 65
[9] Information Technology Act 2000, s 66
[10] Information Technology Act 2000, s 67

THREATS TO CYBER SECURITY IN INDIA

1. Over-reliance on multimedia systems poses a great threat because empathetic particulars can be exposed and it blemishes the faith of customers.

2. Unavailability of cyber security experts which means it becomes strenuous to detain cyberterrorists so, there is a need to strengthen cyber security by commencing distinctive training and awareness programs.

3. Glitches in the Internet of Things (IoT) device security, such as default passwords and the inadequacy of frequent software updates, create vulnerabilities that can be subjugated by maleficent actors.[11]

4. India is not even a signatory to some of the vital international frameworks on cyber security like the convention of cybercrime of the Council of Europe (Budapest Convention) which not only European nations but Japan, the US and South Africa have become signatories to, except India.[12]

JUDICIAL INTERPRETATION

Shreya Singhal v Union of India[13]: Two women have perpetrated an offence of obnoxious commentary on Facebook considering the entire close of Mumbai and they got apprehended under Section 66A[14]. The women submitted a petition that section 66 is undemocratic or against the Law and opposed Article 19[15]. Judgment was delivered by Justice Jasti Chelameswar and R.F. Nariman and they purported that Section 66A was undemocratic and opposed to Article 19(1)(a)[16].

---

[11] Shubham Mishra, 'Challenges faced by cyber security in 2023' (*The Times of India*, 19 June 2023) <https://timesofindia.indiatimes.com/blogs/voices/challenges-faced-by-cyber-security-in-2023/> accessed 10 August 2023

[12] 'Challenges to Cyber Security' (*INSIGHTS IAS*) <https://www.insightsonindia.com/security-issues/cyber-security/challenges-to-cyber-security/> accessed 10 August 2023

[13] *Shreya Singhal v Union of India* AIR 2015 SC 1523

[14] Information Technology Act 2000, s 66A

[15] Constitution of India 1950, art 19

[16] Constitution of India 1950, art 19(1)(a)

Avnish Bajaj v State (NCT) of Delhi[17]: The case was reported against three individuals Ravi Raj, Avnish Bajaj (Director) and Sharat Digumarti (CEO) under the illegal act of presenting a lascivious MM'S video footage with the identification Alice-Elec with the narration, 'DPS girls having fun'. Ravi Raj disappeared or escaped and Avnish Bajaj submitted a petition exempting him from Section 67[18]. Supreme Court in its decision purported that Avnish Bajaj was not guilty and exonerated.

CBI v Arif Azim (Sony.Sambandh.com Case)[19]: Arif Azim was inculpated of wrongdoing under sections 418[20], 419[21] and 420[22] for utilizing a Credit Card of an American National for purchasing an electrical appliance of SONY because as an employee in the call Centre, he has an approach to it and held guilty and as a first time condemn, he was freed on probation for One Year.

Kalandi Charan Lenka v The State of Odisha[23]: In this case, a victim is competing against a dilemma of getting indecent text from anonymous numbers by using her transfigured pictures sham account on Facebook was created which led to the defamation of the victim. The High Court in its judgement held the accused legally responsible under diverse sections of the IT Act and Section 354[24].

NASSCOM v Ajay Sood & Ors[25]: In this case, at the defendant's domain two hard disks were occupied from which sham e-mails were forwarded by the defendant in the name of NASSCOM and Justice Pradeep Nandrajog held that 'phishing' on the web to be an unlawful act, incorporating a decree and reprisal.

---

[17] *Avnish Bajaj v State (NCT) of Delhi* 116 (2005) DLT 427
[18] Information Technology Act 2000, s 67
[19] *CBI v Arif Azim* (2013)
[20] Indian Penal Code 1860, s 418
[21] Indian Penal Code 1860, s 419
[22] Indian Penal Code 1860, s 420
[23] *Kalandi Charan Lenka v The State of Odisha* BLAPL No 7596/2016
[24] Indian Penal Code 1860, s 354
[25] *NASSCOM v Ajay Sood & Ors* (2005) (30) PTC 437 Del

State of Tamil Nadu v Suhas Katti[26]: In this case, a divorced lady was competing against mental harassment through the passage of Web that means defamatory and displeasing text, calls and e-mails. After inspection, the accused was held legally responsible for paying a fine and was incarcerated at Central Prison, Chennai.

RECENT CYBERCRIMES IN INDIA

- On August 4, 2023, the South Delhi police incarcerated 5 people including juveniles on the ground that a senior citizen reported a case of resisting them for doing fraud calls and taken 48 lakh Rupees on account of that.[27]
- On July 29, 2023, 2 people were incarcerated executing crimes for sending fraud APK files for the superintendence of the victim's smartphone and Rs. 1.7 lakh was charged to her Credit Card.[28]
- On 25 July 2023, Police incarcerated three individuals including a SIM agent and two POS agents, inculpated in the unauthorized sale of pre-activated SIM Cards to cyber criminals in Singrauli. They were incriminated in making terrifying calls to convert Religion.[29]

STATISTICAL DATA OF CYBER CRIMES IN 2021 IN INDIA

National Crime Record Bureau (NCRB) establishes its recent data for 2019-2021 that exhibits crimes committed by cybercriminals.[30]

Recent overall data of Crime committed by cybercriminals in India:

---

[26] *State of Tamil Nadu v Suhas Katti* CC No 4680/2004
[27] 'Cybercrooks posing as girls dupe senior citizens, 5 held' (*Times of India,* 04 August 2023) <https://timesofindia.indiatimes.com/city/delhi/cybercrooks-posing-as-girls-dupe-senior-citizens-5-held/articleshow/102407440.cms> accessed 10 August 2023
[28] Dwaipayan Ghosh, '2 fall prey to cyber fraud, 2 arrested' (T*imes of India,* 29 July 2023) <https://timesofindia.indiatimes.com/city/kolkata/2-fall-prey-to-cyber-fraud-2-arrested/articleshow/102219307.cms> accessed 10 August 2023
[29] Sudeept Mishra, 'Pre-activated SIM card racket busted, 3 arrested in Singrauli' (*Times of India*, 25 July 2023) <https://timesofindia.indiatimes.com/city/bhopal/pre-activated-sim-card-racket-busted-3-arrested-in-singrauli/articleshow/102093778.cms> accessed 10 August 2023
[30] Ministry of Home Affairs, *Crime in India – 2021 Statistics* NCRB (2021) vol 1

S. No.	Section under IT Act and IPC	Offences	Statistical Data
1.	66 C (IT)	Identity theft	4047
2.	66 D (IT)	Cheating by personation by using Computer Resource	11339
3.	66 E (IT)	Violation of Privacy	365
4.	67 (IT)	Publication/ transmission of obscene/ sexually explicit acts in electronic form.	11,491
5.	354 D (IPC)	Cyberstalking/bullying of women/ children	1154
6.	Sec. 420 r/w sec 465, 461-471 (IPC)	Fraud	27,960
7.	420 (IPC)	Cheating	6306
8.	506,503, 384 (IPC)	Cyber Blackmailing/ threatening	688
9.	505 (IPC)	Fake news on social media	179

IS THERE ANY DIFFERENCE BETWEEN CYBER CRIME AND CYBER SECURITY?

Yes, there is a complete difference between cybercrime and cybersecurity as cybercrime exerts influence on personnel and family whereas cybersecurity strikes the government and corporations. There is also a difference in crimes between the two that is cybercrime covers Cyberbullying, Cyberstalking etc. Whereas the latter engages in crimes like DDoS attacks, viruses etc. Former is the meticulous apprehension of how and why crimes are executed.

Whereas the latter accomplishes coding, networking for creating networks more strengthened. Cybercrimes have scholastic programs like Criminology, psychology and sociology whereas the latter have computer science and information technology.[31]

CYBERCRIMES IN AUSTRALIA

Cybercrimes enclose an enormous collection of offences that commence a substantial oppression on Australians, Crimes listing: - Identity crime, network hacking, cyber encroachment, cryptocurrency fraud, Phishing, Email fraud, detriment and malignant extirpation of data. In 2020-21 Australian Government Cyber Security Center catalogued 67,500 cyberattacks or cybercrimes.[32]

OFFENCES AND PENALTIES FOR CYBER CRIMES IN AUSTRALIA

The offences and Penalties are:[33]

S. No	Sections	Offences	Penalties
1.	477	Serious computer offences- Unauthorized access, Modification or impairment with intent to commit a serious offence.	Life Imprisonment or 5-year imprisonment or more.

[31] 'Cyber Security vs Cyber Crime: Do you Know the Difference?' (*Cyber Security King*) <https://cybersecuritykings.com/2020/04/03/10-differences-between-cyber-security-and-cyber-crime/#google_vignette> accessed 12 August 2023

[32] Niek Dekker, 'Critical Cyber Crime Statistics in Australia 2023' (*Eftsure*, 07 February 2023) <https://eftsure.com/statistics/cyber-crime-statistics/> accessed 12 August 2023

[33] Cybercrime Act 2001

2.	478	Other computer: • Offences like unauthorized access to, or modification of restricted data. • Possession or control of data with intent to commit a computer offence.	2 years of Imprisonment 3 years of imprisonment

COMMITTED CYBERCRIMES IN AUSTRALIA

In September 2022, an Australian Company named Optus underwent a cybercrime attack in which peculiar information of customers like Names, passport details, Government ID numbers etc. Got divulged. Cybercriminals acquired access to the username or password of the company and asked Ransom for A$ 1.5m.[34]

- In December 2022, Medibank, Australian health Insurance underwent a Cybercrime attack in which all the peculiar information got divulged that troubled about half the population of New York and due to which health insurance impulse customers to check credits frequently.[35]
- The Australian Personal Loan Supplier Latitude was troubled by the data breach that afflicted 14 million people in Australia and New Zealand.[36]

JUDICIAL PRECEDENT

Australian Securities and Investments Commission v RI Advice Group PTY. LTD[37]: A Case was filed resisting RI advice group which has insubstantial cyber security that ended in

[34] Edward Kost, '3 Biggest Data Breaches in Australia [Updated 2023]' (*UpGuard*, 4 August 2023) <https://www.upguard.com/blog/biggest-data-breaches-australia#:~:text=In%20December%202022%2C%20Medibank%2C%20the,Russia%2C%20the%20REvil%20ransomware%20gang> accessed 12 August 2023

[35] *Ibid*

[36] *Ibid*

[37] *Australian Securities and Investments Commission v RI Advice Group Pty Ltd* [2022] FCA 496

revealing empathetic client information, a ransomware attack and also a client bears deficit of $50,000 So, the Federal Court in its Judgement held RI advice group legally responsible and have to compensate with an amount of $750,000.

R v Vose[38]: In this case, a mature male stalked an adolescent accompanying him taking his pictures, webcasting and equipping all the latest information about him on his website hence wrongdoer was legally responsible for the offence of Cyberstalking.

Kennison v Daire[39]: The court dismissed an appeal disregarding the conviction for larceny of a man who, having closed his account at a bank, used a card to extract a sum of $200 of which he had no possession.

CYBERCRIMES IN SAUDI ARABIA

Saudi Arabia is at the apex of committing cybercrime. They also interpolated new Arab cybercrime covenant which embraces wrongdoing like Credit Cards, Scams, Cyber terrorism, hacking, unauthorized usage of Networks and so on.

Penalties for cybercrimes in Saudi Arabia[40]:

S. No.	Articles	Offences	Penalties
1.	Article 3	Offences like Spying, Unlawful access to computers, Unlawful access to computers, Blackmail	Imprisonment not exceeding one year and a fine not exceeding 5 lakhs Riyal or either punishment.

[38] *R v Vose* [1999] VSCA 200
[39] Kennison v Daire [1986] 160 CLR 129
[40] Anti-Cyber Crime Law 2007

2.	Article 4	Offences like illegally accessing bank or Credit Card, acquiring bonds through Fraud	Three years imprisonment and a fine not exceeding two million riyals or to either punishment.
3.	Article 5	Offences like Unlawful access to computers, distortion etc.	Not exceeding four years imprisonment and three million Riyals or either punishment.
4.	Article 6	Offences like the Construction of sites to facilitate human trafficking and gambling sites violate Public Morals.	Not exceeding Five years imprisonment and three million Riyals or either punishment.
5.	Article 7	Offences like the Construction of websites for terrorist Organizations, data jeopardizing the internal or external security of the state	Not exceeding 10 years imprisonment and five million Riyals or either punishment.

COMMITTED CYBERCRIMES IN SAUDI ARABIA

- In March 2019 Dalil-Caller ID is a widespread Saudi App for detecting and ascertaining telephone numbers and reporting distrustful ones. VPN Mentor team found malicious software that was strenuously encrypting data and exposing the data of 5 million people.[41]
- On 21 September 2020 cyberpunks got into the Virgin Mobile KSA system, filed details and produced it on the dark web for sale.[42]
- On 11 June 2021, Globe Med Saudi serves support to insurance companies in Saudi Arabia, including international health services and customer services. It was transgressed by Xing Team, a data revelation Internet site for healthcare information. Cyberpunks acquired 201 GB of data and circulated a portion of it on the internet domain.[43]

CONCLUSION AND SUGGESTIONS

Cybercrime is an enormous impediment in this burgeoning technological world. Rather than benefitting from and amplifying knowledge youngsters are becoming cyberpunks or cybercriminals at a young age is a prodigious matter of contention before our vulnerable population. Counterattack, Capital gain, personal or social revenge and lack of Moral education, are many other happenings of increasing cybercrime throughout the world.

According to my consideration, the remedies to encumber cybercrimes are First, Bank servers and security should provide a secure shield to their customers so that credits can be secured. Secondly, Unemployment is the main reason for these cybercrimes. Youngsters' acquaintance with computers leads them to perpetrate offences like Cyberbullying, Cyberstalking, Cyber terrorism and blackmailing to gain money. They do so because not getting employed after education makes their minds devil to execute cybercrimes for the sake of Money. Thirdly, the government should have surveillance over classified sites e.g., Pornography sites, drug dealing

[41] 'Top-9 Cybersecurity Breaches in Saudi Arabia' (*Cyberlands*, July 2019) <https://www.cyberlands.io/topsecuritybreachessaudiarabia> accessed 12 August 2023
[42] *Ibid*
[43] *Ibid*

sites and virtual offences against the state and national security sites. If the person is perverting and approaching the site persistently the government should take the initiative to intercept the person from executing crimes. Fourthly, do not use third-party applications because using these applications may lead to exposing your pecuniary information lastly, parents should monitor their children's activity using an internet site.

Yes, all countries have laws and Acts to intercept cybercrime and provide penalties for executing cybercrimes but as a responsible citizen, it is our incumbency to help the country in becoming a crimeless country. For the emerging world, technology plays a significant role so cybercrime should be averted in every feasible way.