



Cybercrimes & The Law

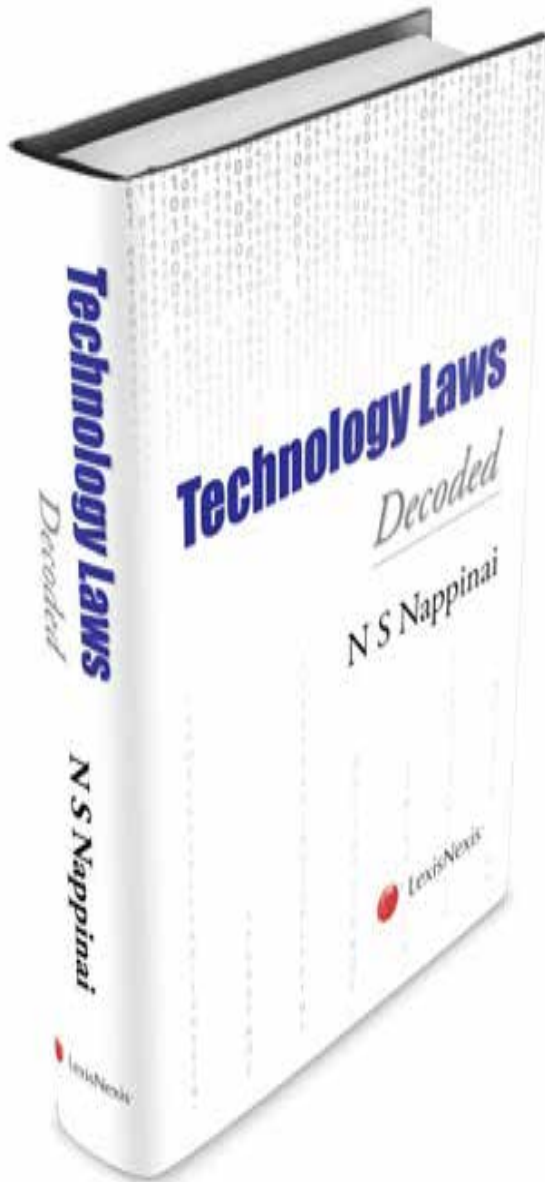
N. S. Nappinai

Senior Advocate &

Founder – Cyber Saathi

nappinai@nappinai.com

***Author – “Technology Laws Decoded” &
CSassy Tales – Cybercrime Stories & The Law***



- *“Law in the world of the Internet is a constantly changing and evolving beast.*
- *It neither has parental guidance nor memory genes to guide its path to the lighter horizon.*
- *It had to rely on existing logic and purposive interpretation in its formative years.” (Chapter 1, Technology Laws Decoded by N. S. Nappinai)*

Criminal Justice System

- **Guarantees of a Criminal justice System**
 - Governmental guarantee of Rule of law;
 - Social contract to uphold societal control;
 - Deterring and mitigating crime & imposing sanctions against those who violate laws;
 - Protecting against misuse of such laws against persons Accused;
 - Through the arms of the Legislative, Judiciary & Executive – Police & Prisons;

Objective of the Criminal Justice System

- Provide substantive & procedural mechanisms for:
 - Prevention of Crime – maintain law and order;
 - Deterrent against temptation of crime or its spoils;
 - Retribution – punishment or sanction for violation;
 - **Protect rights of victims & ensure compensation to them;**



Challenges - Cyber Pangaea



- “Where the world has not been broken up into fragments; By narrow domestic walls” - (Tagore, R. 1910);
- The Cyber Convergence – Shrinking World or Expanding Frontiers?;
- Death of Distance;
- Erasure of Shadow Lines;
- Territoriality Challenged;
- Sovereign concepts turned on their head;

W(h)ither the State?

- Governmental guarantee of Rule of law;
- Social contract to uphold societal control
- Absolutism of Bodin, Hobbes & Austin to Bentham's Moderation;
- Sovereign Rights & Obligations;
 - Deterring and mitigating crime & imposing sanctions against those who violate laws;
 - Through the arms of the Legislative, Judiciary & Executive – Police & Prisons

Crimes & Cybercrimes



Challenges in combatting Cybercrimes

According to United Nations Commission on Trade and Development (UNCTAD), four **challenges** faced by countries when dealing with cybercrime are:

1. Enacting laws to criminalize computer abuses
2. Committing adequate personnel and resources
3. Improving abilities to locate and identify criminals
4. Improving abilities to collect and share evidence internationally

Cyber Justice

- Effective use of technology in justice delivery systems to:
 - ensure access to justice,
 - speedy and effective justice delivery,
 - cost effective justice,
 - alleviating burden on the system and judges;

- **Laws in India to Combat Cybercrimes**

Law or Regulation Helping Innovation

- Nappinai N. S. (2017): *Technology Laws Decoded*:
- “Technology may be propelling us into a **“new century with no plan, no control, no brakes”** and it may now very well be the time for **“reprising control before we cross the “fail-safe point”**”
- (Draws on Thoreau from Joy, B. (2000). “Why the future doesn’t need us. Nanoethics.”.)

CYBERCRIMES – QUICK VIEW

- National:
 - Cyber Terrorism – primary focus (66F);
 - Power of Controller (68);
 - Offences against Protected Systems (70);
 - Encryption; blocking of access; monitor & collect data or information traffic (69, 69A & 69B and 84A);
 - Confidentiality of information to authority under Act (72);
- Economic:
 - Tampering with Source Code (S.65);
 - Transposing Civil penalties under S. 43 to S.66;
 - Intermediary liabilities(2(w), 67C,);
 - Data Protection & Confidentiality;(S.43 A (Civil) & 72A (criminal));
- Personal:
 - Privacy (66E; 67 + 67A & 67B & 72A);



S.66 of ITA-2000

66 r/w 43

- With Dishonest & Fraudulent Intent!

66 r/w 43(a)

- Hacking

66 r/w 43(b)

- Data Theft

66 r/w 43(c)

- Virus Attack

66 r/w 43(d)

- Damages or Causes to be Damaged a Computer, computer System etc.,

66 r/w 43(e)

- Disrupts or Causes Disruption to Computer, Computer systems etc.,

S.66 of ITA-2000

66 r/w 43(f)

- Denial of Service Attack

66 r/w 43(g)

- Provides assistance to any person to facilitate access to any computer

66 r/w 43(h)

- Illegal charging of services to victim's account thro tampering / manipulating systems

**66 r/w
43(i)**

- Deletes destroys or alters information in a computer **or** diminishes value or utility or affects it injuriously **by any means**

**66 r/w
43(j)**

- steal, conceal, destroys or alter computer source code to cause damage;

S.66 of ITA-2000

~~66A~~

• ~~Sending of Offensive Messages~~

66B

• Receiving stolen resources

66C

• Identity Theft

66D

• Cheating by personation

66E

• Violation of Privacy

66F

• Cyber Terrorism

ITA-2000

- Further Additions

67

- Publishing / Transmission of Obscene material in electronic form

67A

- Publishing / Transmission of sexually explicit Act or Conduct

67B

- Depicting Children in sexually explicit Act or Conduct in electronic form

67C

- Prevention / Retention of Information by Intermediaries (2 (w))

69

- Interception / Monitoring / decryption of data in computer resource

69A

- Blocking from public access

69B

- Monitor & Collect Data for Cyber Security

Other Important Provisions

| Offense | Act |
|---------|---|
| S.72A | Breach of Confidential Personal Information |
| S.75 | Extra Territorial Jurisdiction |
| S.76 | Confiscation |
| S.77A | Compounding of Offences |
| S.77B | Offences with 3 yrs imprisonment – Bailable; |
| S.78 | Power to Investigate – vested with Inspector; |

Some More to reckon with

| Offense | Act |
|---------|---|
| S.79 | Intermediary Liability |
| S.81 | Overriding effect of the IT Act |
| S.84A | Punishment for Abetment of Offences |
| S.84C | Punishment for Attempt to commit offences |
| S.85 | Offences by Companies |

IPC – Old & New

- IPC Provisions & Cybercrimes:
 - Sharat Babu Digumarti v. Govt. (NCT of Delhi), (2017) 2 SCC 18;
- Bharatiya Nyaya Sanhita, 2023;
- Crimes expanded to online domains;
- Enforcement through existing mechanisms;
- Need for further review?

Cybercrime Trends - Cybersecurity

- Loss due to cybercrimes - \$10.5 trillion by 2025.
<https://aag-it.com/the-latest-cyber-crime-statistics/>
- **422 million individuals were impacted**, according to the FBI's internet crime records
- Ransomware
- Deepfake Frauds
- IoT Vulnerabilities
- Phishing Attacks
- DDoS Attacks
- Supply Chain Attacks
- Financial frauds – recourse?

- Cases & Case laws on Cybercrimes

In the world of Cyber ...

- Nothing is what it seems...: [The New York Times](#). Retrieved October 1, 2007.



AI's Polyjuice Portion

CSassy
Tales



Obama-Peele deepfake sends message about fake news



Barack Obama



Jordan Peele

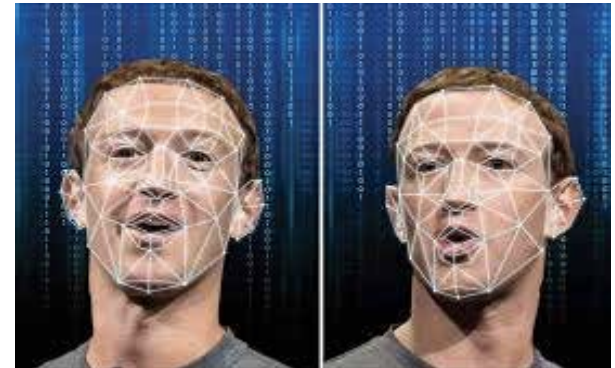
BREAKING

AMIT SHAH DEEPFAKE NOW

**TELANGANA CONGRESS
SOCIAL MEDIA TEAM ARRESTED**

**R.
DIGITAL**

CSassy
Tales



Digital Arrests

- 22.02.2025: Chennai engineering college asst professor held for Rs.3.8 crore digital arrest scam – poses as ED!



Deep Fakes & Information Warfare



- “Information Warfare” or “Info war” -technology enabled **manipulation of information** entrusted by individuals **to engineer their decisions or thoughts** to align with propagator of such act or to promote the interests that the perpetrator of such acts intends (Libicki. M. 1995). Libicki, Martin (1995), *What Is Information Warfare?* ACIS Paper 3, Washington, DC: National Defense University;
- Social Engineering & Elections;

Prajwala & Beyond



- In" *Re: Prajwala Letter Dated 18.2.2015. Violent Videos & Recommendations* - (2018) 15 SCC 551):
 - Starts with uploading of gangrape videos but expands to CSAM;
 - October 23, 2017: Precedent Law through consensus recommendations;
 - August 1, 2023: Directions to Government and conclusion of case;
- *Subru @ Subramani Vs. State* (2017 SCC OnLine Mad 5857):
 - S.341, 323/34, 560(ii)/149, 354, 392/379, 376(D) of IPC, §67(A) of IT Act and § 4 of Tami; Nadu Prohibition of Women Harassment Act.
 - Gang Rape videographed;
 - '*men may lie, but not the science*' – Appeal against conviction rejected;

Sextortion / Blackmail



- ***Inyat Abdul Majid Hurjuk Vs. State of Maharashtra*** (2017 SCC OnLine Bom 5237)
 - Offence under: S376(2)(n), 328, 313 and 506 of IPC and §67 of IT Act.
 - Bail granted – on grounds of consenting adults;
- ***Joji Jose V. State of Kerala*** (2015 SCC OnLine Ker 13949): blackmailed using naked pics into marrying accused.
- ***Jekibhai Sharadbhai Rami Vs. State Of Gujarat***, (2015 SCC Online Guj 413): consent to take pictures does not amount to consent for dissemination. Withdrawn as settled;

Revenge Porn



- ***Amandeep Kaur v. State of Haryana*** (2013 SCC OnLine P&H 23120): Husband files complaint for revenge porn dissemination by accused;
- ***Adarsh @ Adarsh Singh V. State of Punjab*** (2013 SCC OnLine P&H 25944):
 - *"The Court observed that the tendency and frequency of sending such vulgar messages and projecting the objectionable photographs on internet of innocent young girls by such accused was increasing day-by-day, ruining the social fabric of society and held that such crimes ought to be "curbed with heavy hands" and therefore rejected the Application for Anticipatory bail."* – Extracted from "Technology Laws Decoded" by N. S. Nappinai

Threatening Online Circulation



- *Vinupriya's case*
- *Puja Kumari & Virendra Shah Vs. The State of Bihar* (2017 SCC OnLine Pat 780):
 - Sections 306 r/w 120B, 354, 323 of IPC and S.67, 67A, 84B of IT Act.
 - Photos of deceased taken in compromising positions
 - Evidence insufficient to attribute the girl's suicide to the obscene images circulated by accused;
 - Acquitted.

Cyber Terrorism & Law



- ***Harjinder singh Vs. State of Punjab*** (2012):
 - Criminal Writ Petition before the High Court of Punjab and Haryana for quashing;
 - Accused arrested & case registered u/s 66 D and 66 F of the Information Technology Act, 2008;
 - Found in possession of a Pakistani Sim card;
 - WP Dismissed;
- ***Mohammedayub @ Sakir Shabirbhai Shaikh Vs. State Of Gujarat*** (2015):
 - Gujarat D.C.B. Crime Police Station, for the offences punishable under Sections 121, 121(A), 123 and 120(B) of the Indian Penal Code and Section 66(F) of Information Technology Act and Section 3 of Official Secret Act.
 - F.S.L., Gandhinagar Report disclosed cell phones and sim cards of the applicant and other persons, recovered from the Cyber Cafe, used to make calls to Pakistan;
 - Bail granted as report insufficient to prove charges;
- ***Pavan M. Vs. State by Ulsoor Gate Women's Police Station*** (2015): *Case withdrawn as settled but clear misuse of S. 66F IT Act in a matrimonial case;*

Cyber Terrorism & Online Grooming



- UN report titled “The Use Of The Internet For Terrorist Purposes” (2012):
 - Threats of propaganda, recruitment, and radicalization of children through social media, chat apps, and games;
- United Nations Office on Drugs and Crime, ‘Handbook on Children Recruited and Exploited by Terrorist and Violent Extremist Groups: The Role of the Justice System’, 2017: reiterates its warning;
- Fulton, Caitlin (2019) writes about how ISIS modified GTA into “*Grand Theft Auto: Clash of Swords*”; ‘Call of Duty: Black Ops’ renamed ‘*Call of Jihad*’;
- Ahmed Al- Rawi (2018): “Salil al-Sawareem” (The Clanging of the Swords in Arabic), an ISIS shooter game used to radicalise and recruit westerners. Statements such as “*Your games which are produced from you, we do the same actions in the battlefields!!*”

Financial & Online Frauds



- ***Ranjeet Kumar v. The State*** (2016 SCC OnLine Del 3638):
 - Accused posts on matrimonial site “*jeevansathi.com*” claiming to be single. Initiates relationship with victim & then cheats her to part with property;
 - Convicted under Sections 420, 467, 468, and 471 IPC;
- Marie Rohde, ‘When Words With Friends Turns Ugly’, *AARP*, October 2, 2020 <<https://www.aarp.org/money/scams-fraud/info-2020/words-with-friends-romance-scam.html>> (last accessed August 19, 2022);
- ‘Delhi Police Busts Racket That Duped 27,000 With Fake Govt Job Offers, Arrests Five People’, *india.com*, November 5, 2020; <<https://www.india.com/news/india/delhi-police-busts-racket-that-duped-27000-with-fake-govt-job-offers-arrests-five-people-4198637/>> (last accessed August 19, 2022).

Online Predators & Social Engineering



- *Ashok Kumar Vedprakash Sharma v. State of Maharashtra* (2018 SCC OnLine Bom 18089):
 - Accused Ashok Kumar created a fake online profile on Facebook pretending to be a girl named 'Riya Sharma'. He befriended the victim - 17 years and 9 months then.
 - Induced to share nude imagery; faces prosecution under Section 354D of the IPC and Section 12 of the POCSO Act read with Section 67B of the IT Act; Bail granted though;

Social Engineering Attacks

- Social engineering attacks manipulate people into sharing information that they shouldn't share, downloading software that they shouldn't download, visiting websites they shouldn't visit, sending money to criminals or making other mistakes that compromise their personal or organizational security.
- Types:
- Phishing
- Whaling or Spearphishing
- Baiting
- Diversion theft through spoofing
- Business Email Compromise
- Smishing / SMS Phishing
- Pretexting
- Honey Traps
- Tailgating / Piggybacking

Ransomware



- Nappinai N S (2022): CSassy Tales – Cybercrime Stories & The Law. Oakbridge Publishing.
 - It does not take much to indulge in the crime of ransomware:
 - '14-Year-Old Japanese Teen Arrested for Allegedly Creating Ransomware', *tripwire*, June 6, 2017; <https://www.tripwire.com/state-of-security/latest-security-news/14-year-old-japanese-teen-arrested-allegedly-creating-ransomware/> (last accessed August 19, 2022).

Crypto Scams

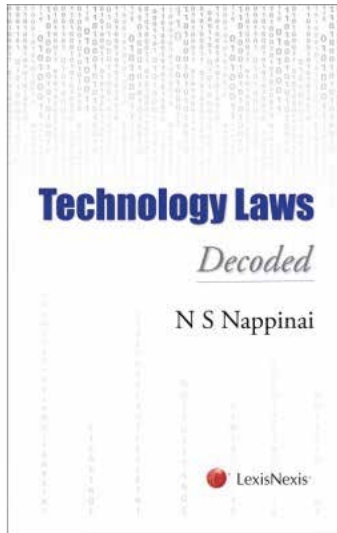


- Crypto Scams: Need for stringent enforcement & awareness:
- Abhijit Ahaskar, 'Gullible users, lack of regulation, spur crypto cybercrimes in India', *Mint*, January 10, 2022; <https://www.livemint.com/technology/tech-news/gullible-users-lack-of-regulation-spur-crypto-cybercrimes-in-india-11641737163936.html> (last accessed August 19, 2022).
- Shaju Philip, 'In 'ICO' for fake crypto coin, investors lose over Rs 1,200 crore', *The Indian Express*, January 6, 2022;
- <https://indianexpress.com/article/cities/thiruvananthapuram/in-ico-for-fake-crypto-coin-investors-lose-over-rs-1200-crore-7708813/> (last accessed August 19, 2022).

Law As the Safety Net & Brakes

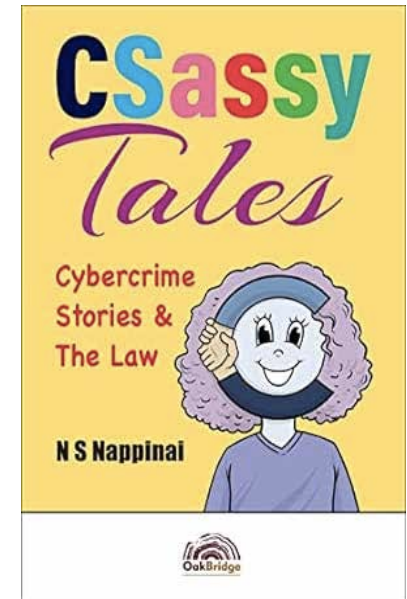
- “Technology may be propelling us into a *“new century with no plan, no control, no brakes”* and it may now very well be the time for *“reprising control before we cross the “fail-safe point”* (Nappinai N. S. (2017) drawing on Thoreau & Joy B.);





THANK YOU

N S NAPPINAI
SENIOR ADVOCATE
&
AUTHOR
“TECHNOLOGY LAWS DECODED”
& “CSASSY TALES – CYBERCRIME STORIES &
THE LAW”



nappinai@nappinai.com; nappinai@gmail.com;