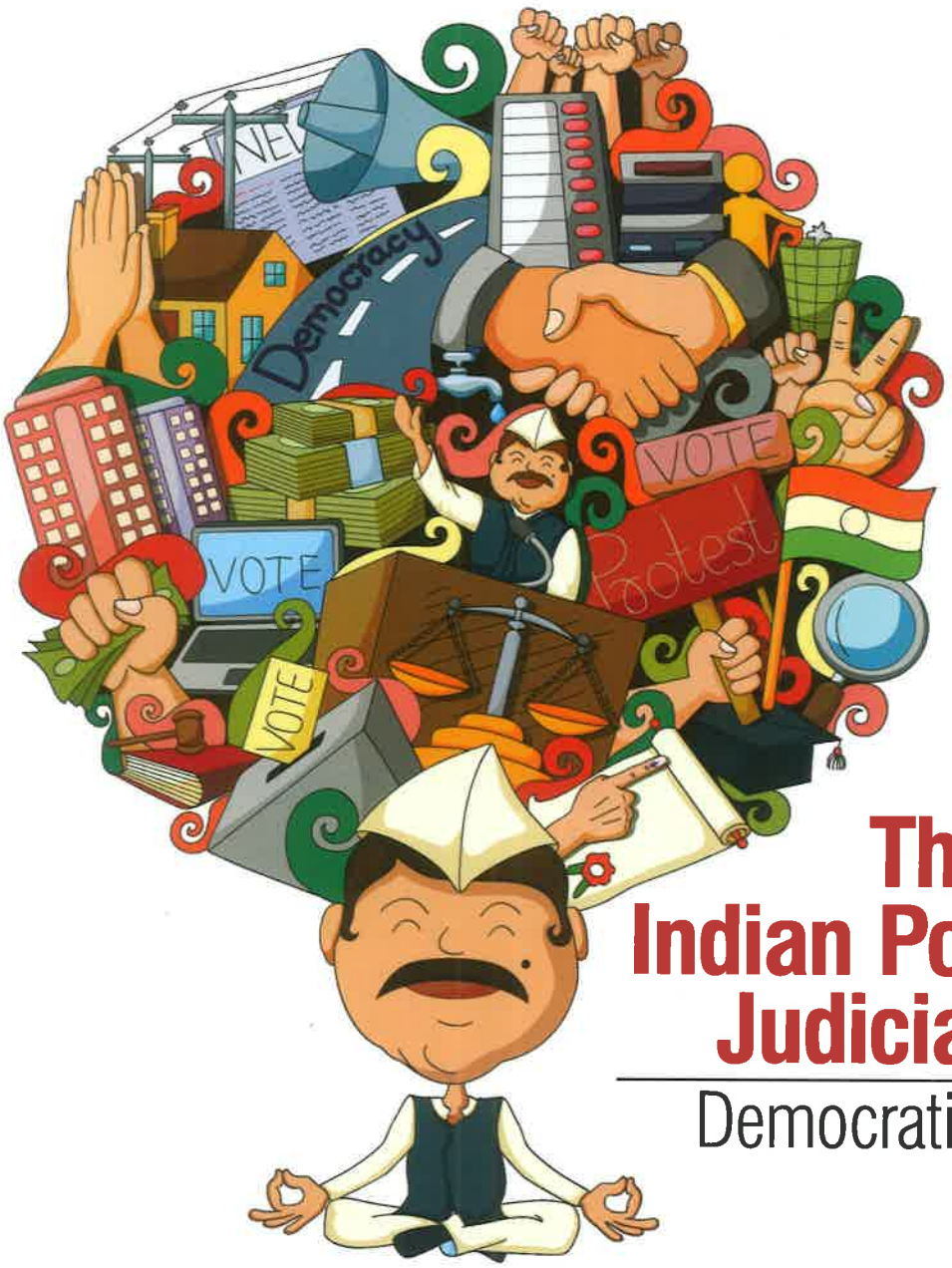
INDIA'S FIRST MAGAZINE ON LEGAL AND CORPORATE AFFAIRS

LEX WITNESS

Volume 10 Issue 7 | February 2019

₹65 US $6 UK £4



The Great Indian Politics & Judicial Rides

Democratic Enough?

P08

■expert speak

Ashu Kansal
Partner, Adhita Advisors

P47

■expert speak

Sharad Tyagi
Partner, Fair & Just Legal

P38

■expert speak

Rohan Swarup
Senior Associate,
Singh & Singh

P32

■let's arbitrate

S. Ravi Shankar
Sr. Partner, Law Senate

P28

expert speak

Jayashree Shukla Dasgupta
Partner, Dhir & Dhir Associates
Umang Thakar
Associate, Dhir & Dhir Associates

P16

expert speak

Rajesh Sivaswamy
Senior Partner,
King Stubb & Kasiva

P22

expert speak

Hardeep Sachdeva
Senior Partner, AZB & Partners
Nitin Saluja
Associate, AZB & Partners

P20

Players Involved in Cybercrime & Role of Intermediaries

Rohan Swarup

Technological advancement and easy accessibility of Internet has made the burgeoning cyberspace vulnerable and the repercussions associated with it can be witnessed in the recent times. Cybercrime has become rampant across the globe, which impacts the lives of people and the rate of cybercrime has increased in the recent years. What is to be blamed? The advancement of technology or the easy access to Internet? Perhaps both are equally to be blamed. Both are equally responsible for making it easier for carrying out a diverse range of criminal activities that has no boundaries and is capable of causing serious harm to people worldwide.

WHAT IS CYBERCRIME?

Before discussing the various aspects of cybercrime. It is important to understand the nuances of cybercrime. Cybercrime refers to any criminal activity that in carried out using a computer, network device or a network.

CAUSES OF CYBERCRIME

Increase in the rate of cybercrime has become a concern for every country and India is not an exception to it. In order to find a solution to curb it, it is important to understand the causes of cybercrime. Just like any other crime, the causes of cybercrime are at times difficult to establish. However, by seeing the emerging trends, here are two major causes or factors that are responsible for it.

- **Economical Motivation:** One of the primary causes of such crime is money. When you hide behind a network, the risk of being caught is lower and the monetary gain is much higher, making money one of the major motivators for most of the criminals. Owing to this, a huge group of cyber criminals target online banking accounts.

- **Personal Grudges:** Since cybercrimes involve lower risk, a lot of individuals, who are well-versed with hacking, vent out their personal grudges by hacking someone's social media accounts or even websites. For example, an unhappy employee may install viruses in the computer networks of an organization just to take out his grudge against his/her employer.

TYPES OF CYBERCRIME

The Indian IT Act 2000 (amended via 2008) Act has listed some common cybercrime scenarios, which attracts penalties. These include:

- **Harassment via fake public profile on social networking site**

A fake profile of a person is created on a social networking site with the correct address, residential information or contact details but he/she is labelled as 'prostitute' or a person of 'loose character'. This leads to harassment of the victim. Provisions applicable are Sections 67 of IT Act and Section 509 of the Indian Penal Code.

- **Online Hate Community**

Online hate community is created inciting a religious group to act or pass objectionable remarks against a country, national figures etc. Provisions applicable are Section 153A & 153B of the Indian Penal Code.

SINGH & SINGH
C-139, Defence Colony
New Delhi - 110024, India
T: +91 11 - 4987 6099
T: +91 11 - 4982 6000 to 6099
E: email@singhandsingh.com

• Email Account Hacking

If victim's email account is hacked and obscene emails are sent to people in victim's address book. Provisions applicable are Sections 43, 66, 66C, 67, 67A and 67B of IT Act.

• Credit Card Fraud

Unsuspecting victims would use infected computers to make online transactions. Provisions applicable are Sections 43, 66, 66C, 66D of IT Act and section 420 of the IPC.

• Web Defacement

• The homepage of a website is replaced with a pornographic or defamatory page. Government sites generally face the wrath of hackers on symbolic days. Provisions applicable are Sections 43 and 66 of IT Act and Sections 66F, 67 and 70 of IT Act also apply in some cases.

• Introducing Viruses, Worms, Backdoors, Rootkits, Trojans, Bugs

All of the above are some sort of malicious programs which are used to destroy or gain access to some electronic information. Provisions applicable are Sections 43, 66, 66A of IT Act and Section 426 of Indian Penal Code.

• Cyber Terrorism

Many terrorists are use virtual (GDrive, FTP sites) and physical storage media (USB's, hard drives) for hiding information and records of their illicit business. Provisions applicable are Conventional terrorism laws may apply along with Section 69 of IT Act.

• Online sale of illegal Articles

Where sale of narcotics, drugs weapons and wildlife are facilitated by the Internet. Provisions applicable are Generally conventional laws apply in these cases.

• Cyber Pornography

Among the largest businesses on Internet. Pornography may not be illegal in many countries, but child pornography is. Provisions applicable are Sections 67, 67A and 67B of the IT Act.

• Phishing and Email Scams

Phishing involves fraudulently acquiring sensitive information through

masquerading a site as a trusted entity (e.g. Passwords, credit card information). Provisions applicable are Section 66 and 66D of IT Act, and Section 420 of IPC

- **Theft of Confidential Information**

Many business organizations store their confidential information in computer systems. This information is targeted by rivals, criminals and disgruntled employees. Provisions applicable are Sections 43, 66, 66B of IT Act and Section 426 of Indian Penal Code.

- **Source Code Theft**

- A Source code generally is the most coveted and important "crown jewel" asset of a company. Provisions applicable are Sections 43, 66, 66B of IT Act and Section 63 of Copyright Act.

- **Tax Evasion and Money Laundering**

Money launderers and people doing illegal business activities hide their information in virtual as well as physical activities. Provisions applicable are Income Tax Act and Prevention of Money Laundering Act. IT Act may apply case-wise.

- **Online Share Trading Fraud**

It has become mandatory for investors to have their demat accounts linked with their online banking accounts which are generally accessed unauthorized, thereby leading to share trading frauds. Provisions applicable are Sections 43, 66, 66C, 66D of IT Act and Section 420 of IPC.

PLAYERS INVOLVED IN CYBERCRIME

Cyber criminals are not anonymous to us as we may think. It can be one amongst us. As per Professor Federico Varese, "Understanding cybercrime isn't just about the victims. You have to look at the supply of the activity. For too long the emphasis has been put on cybercrime as a global activity, but it is a very localised issue. Cybercrime thrives in those places where they can operate with less fear of arrest or punishment. The people involved are not necessarily sophisticated or even high tech, criminal masterminds. They are everyday people with a motivation and an opportunity. Almost anyone can do it. If we really focus on where this activity is taking place, we should see a reduction in crimes committed."[1]

He has rightly said that people involved are not necessarily sophisticated or high-tech or must have criminal mastermind. Even online stalking is a form of cybercrime and it is done by anyone, not necessarily by someone with a criminal mindset. Here is a list of the players involved in cybercrime –

- **Insiders** - Disgruntled employees and ex-employees, spouses, lovers

- **Hackers** - Crack into networks with malicious intent

- **Virus Writers** - Pose serious threats to networks and systems worldwide

- **Foreign Intelligence** - Use cyber tools as part of their Services for espionage activities and can pose the biggest threat to the security of another country

- **Terrorists** - Use to formulate plans, to raise funds, propaganda

SECTION 43 OF INFORMATION TECHNOLOGY ACT, 2000

Before we further discuss about cybercrimes in India, it is important to understand Section 43 and Section 66 of the IT Act, 2000.

Section 43 of the Act deals with Penalty for damage to computer, computer system, etc. This section states-

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.

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 there under.

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.

he shall be liable to pay damages by way of compensation not exceeding one

crore rupees to the person so affected.

Section 66 of the Act deals with Hacking of Computer System. This section states that -

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:

2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

CASES OF CYBERCRIME IN INDIA

The advancement of technology has without any doubt revolutionized the entire world and the banking system is not an exception. Today, most individuals prefer transferring funds online rather that standing in long ques to deposit cheques or even cash. Electronic fund transfer has made it easier for people to make online payments or transfer money as it is less time consuming as well as one can do it from the comfort of their home or office or while they are on the move. Aside these, there are several other benefits of EFT. One of the biggest benefits of EFT is that it eliminates the need to carry a huge amount of cash. However, even EFT comes with some risks and one of the most common risks is bank frauds. The number of incidences of bank frauds has increased substantially as it has become easier for cyber criminals to hack into your mobile phone or your computer and get your bank account details. The main cause behind such crime is easy money. The number of incidences of bank frauds are reported under deposit, loan and inter-branch accounting transactions, including remittances.

In a recent case R.S. Chauhan Vs. Bharati Airtel and Ors. before the Ld. Adjudicating Officer and Chief Secretary, M.P. Administration, Science and Commerce Department, Bhopal, Mr. R.S. Chauhan, Managing Director, Narmada Forest Industries Pvt. Ltd. Bhopal had filed an application under Section 43, 43A read with Section 85 of the Information Technology Act, 2000 against Bharati Airtel, Bank of Baroda, IndusInd Bank and Punjab National Bank. In the application, he stated that an amount of Rs.49,99,000 was transferred through RTGS from their account in Habib Ganj Branch of Bank of Baroda out of which Rs. 29,99,000 was transferred to IndusInd bank and Rs. 20,00,000 to Punjab

national bank. He further stated that his mobile phone was switched off when the transfer took place and the OTP was received on a duplicate sim, issued by a fraudster on his name by furnishing forged documents. So, who is responsible for such scam? The bank or the Service Provider? In this case, the court stated that both Bharati Airtel and the bank are equally responsible for the fraud that happened with R.S. Chauhan.

In the application, it was stated that in the police investigation no proof with regard to involvement of any person in the incident has been found. And, it was found that the password, login ID and personal sensitive information of the applicant has been leaked out due to negligence on the part of Bank of Baroda. Further investigation by the police found that information system has been illegally accessed by someone and after obtaining the sensitive information of the applicant, the amount is illegally transferred. Also, it was negligence in part of Bharati Airtel, who issued a duplicate SIM card without following proper verification. In this case, the Ld. Adjudicating Officer and Chief Secretary, found both the respondents guilty under Section 43, 43A of the Information Technology Act, 2000 and they are accordingly directed to indemnify the loss occurred to the applicant.

Bharati Airtel has filed an appeal before the Hon'ble TDSAT against the judgement passed by the Ld. Adjudicating Officer and Chief Secretary, which is pending.

In another case, State Bank of India Vs. Shri Chander Kalani & Anr., the bank has filed an appeal under section 57 of the IT Act, 2000 before the Hon'ble TDSAT, aggrieved by an order passed by the Adjudicating Officer, Government of Maharashtra (Principal Secretary, IT, Government of Maharashtra); whereby, the said officer had imposed a penalty of Rs. 40 lakhs. The said penalty was imposed on account of violation of section 43 of the IT Act by the bank. Further, the said officer was of the view that this is a case of contributory negligence; and hence, both the parties i.e. the complainants and the State Bank of India are to be equally blamed.

The State Bank of India preferred an appeal against the said order of the Ld. Adjudicating officer, stating that the Bank was not involved in any negligence whatsoever, as observed in the aforesaid impugned order. The Ld. Senior Counsel appearing for the Bank further submitted that on the contrary, the Bank took necessary steps to inform the police authorities with regard to the hacking of Email IDs of the Complainants. The Appellate Authority, after hearing both the sides and length, was of the clear view that the Adjudicating Officer, Government of Maharashtra (Principal Secretary, IT, Government of Maharashtra) cannot be held liable to have acted in contravention of the IT Act, 2000. The Appellate Authority while dismissing the appeal of the State Bank of India and upholding the order passed by the Adjudicating Office, was pleased to observe that the Bank has indeed been negligent towards the illegality suffered by Shri Chander Kalani and his wife.

ROLE OF INTERMEDIARIES IN CYBERCRIME

Looking at the above case, it is important to discuss and understand the role and liabilities of Intermediaries. In the above case, both Bharati Airtel and Bank of Baroda were intermediaries. "Intermediary" is defined in Section 2(1)(w) of the Information and Technology Act 2000. "Intermediary" with respect to any particular electronic message means any person who on behalf of another person receives stores or transmits that message or provides any service with respect to that message. The liability of the intermediaries is coherently explained in section 79 of the Act.

Section 79 of the Information Technology Act, 2000 exempts intermediaries from liability in certain instances. It states that intermediaries will not be liable for any third-party information, data or communication link made available by them. The Act extends "safe harbour protection" only to those instances where the intermediary merely acts a facilitator and does not play any part in creation or modification of the data or information. The provision also makes the safe-harbour protection contingent on the intermediary removing any unlawful content on its computer resource on being notified by the appropriate Government or its agency or upon receiving actual knowledge.

The Intermediary shall lose the immunity if the Intermediary is found to have conspired or abetted or aided or induced in the commission of the unlawful act or fails to expeditiously remove or disable the access to that material or link residing in or connected to a computer resource controlled by the Intermediary which is being used to commit the unlawful act.

The Central Government has also notified The Information Technology (Intermediaries guidelines) Rules, 2011. These rules provide the guidelines and procedure to be dealt by Intermediaries as part of the due diligence and administration. Recently, the Ministry of Electronics and Information Technology has proposed draft on Information Technology [Intermediary Guidelines (Amendment)] Rules, 2018 to deal with the phenomenon of misuse of social media platforms and spreading of fake news. The Ministry has sought comments from stakeholders and the Rules are expected to be notified shortly.

WHAT HAS THE GOVERNMENT DONE TO CURB SUCH MENACES IN INDIA?

The Information Technology Act, 2000 deals with the various types of cybercrimes in India. And, the various provisions that are applicable for different types of cybercrimes has been stated above. However, just by enacting laws, the Government cannot curb such crimes. Spreading awareness among people regarding the various crimes that take place in the cyberspace is equally important.

Also, recently, the Ministry of Home Affairs of India gave 10 government agencies power to monitor, seize and look into computers and phones via an order signed by Rajiv Gauba, Union Home Secretary, which states - "In exercise of the powers conferred by sub-section (1) of section 69 of the Information Technology Act, 2000 (21 of 2000) read with rule 4 of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, the Competent Authority hereby authorises the following Security and Intelligence Agencies for the purposes of interception, monitoring and decryption of any information generated, transmitted, received or stored in any computer resource under the said Act".

This can be a good step to prevent any illegal activity going on using computers, Internet and Mobile phones. This will to a certain extend help in curbing cybercrimes to a certain extent but without proper awareness, it is not possible to put an end to it completely.

While the Act and Rules enacted by the State are to some extent combating the ever growing menace of cybercrime, the golden rule of "prevention is better than cure" applies to this space as well. It is always advisable to stick to best practices such as - avoiding dubious and shady web sites, avoiding using unsecured public Wi-Fi networks and strictly not giving out sensitive information over unencrypted networks.

[1] http://www.ox.ac.uk/news/2017-08-08-cybercriminals-are-not-anonymous-we-think

Rohan is currently working with Singh & Singh Law Firm as a Senior Associate and his practice areas include Telecommunication & Broadcasting Litigation and Consumer Protection litigation before the Hon'ble Supreme Court, Hon'ble Delhi High Court, Telecom Disputes Settlement and Appellate Tribunal, and National Consumer Disputes Redressal Commission. He also has a keen interest in media and sports law.