KP ASSOCIATES

ADVOCATES & CONSULTANTS

JUNE 2020
ISSUE NO. - II

K.P. Associates is a multi-service law Firm delivering legal, regulatory and advisory services to its clientele.

We deal in all the major disciplines and work with clients ranging from global organizations, government and non-profit businesses, to micro, small and medium organizations, private individuals and entrepreneurs.

At **K.P. Associates** we are followers of the belief that our success will come from our client's success. Therefore, we ensure a great degree of partner involvement and availability, attention to detail, and responsiveness towards client sensitivities.

CYBER CRIMES IN INDIA

A SUDDEN RISE IN THE NUMBERS WITH THE NATIONAL LOCKDOWN

Cybercrime in India has surged amidst the country's unprecedented coronavirus lockdown. The extreme measures of imposing the lockdown in order to contain the novel corona virus have been accompanied by a dramatic rise in cybercrimes across the country. Due to the restricted movement owing to the lockdown the people have been left with no other choice but to rely on online services for all their needs- be it work related, shopping of essential commodities of daily needs, social interaction or even entertainment. The present scenario of heightened online activity has provided cyber criminals enough opportunities to launch cyber attacks.

A closer examination of the sudden rise in the number of cases of cyber crime reveals that both private and state-sponsored cyber criminals have effectively exploited the ongoing crisis. With the increase in the percentage of India's workforce working from home during the pandemic situation, the cyber criminals have not only targeted the individuals' wallets but also their personal data. In times like these, we need to educate our work force to have "digital empathy" since the employees are working remotely and potentially outside of the company's firewall. It was reported that when the "PM CARES" coronavirus fund, was established by the Prime Minister's Office. At least half dozen fake versions of the site had emerged which lured thousands of Indians eager to contribute to the fight against coronavirus into making donations. Many of these fake websites are quite sophisticated and virtually indistinguishable from their genuine counterparts. They have successfully solicited thousands of dollars from unsuspecting individuals. India's Home Ministry said that more than 8,000 complaints had been received from Indians both home and abroad who had duped into giving money to fake versions of the government's flagship fund.

Personal data also continues to be a target during the pandemic. Indian officials have reported that malware and phishing schemes operating under the pretext of COVID prevention efforts have seen a steep rise since the outbreak. The so-called "coronavirus malware" is aimed at stealing bank account details, password and other sensitive information from users. With the rapid proliferation of Internet users, India has risen to the top five most targeted countries in the world by cyber criminals in recent years, reflecting the significant amount of work that still needs to be done in strengthening the country's cyber defenses. Cybercrime constitutes a serious problem for India even outside of crisis periods.

Until then, Indian officials continue find themselves battling not just the coronavirus outbreak, but those who see opportunities for illicit gains within it.

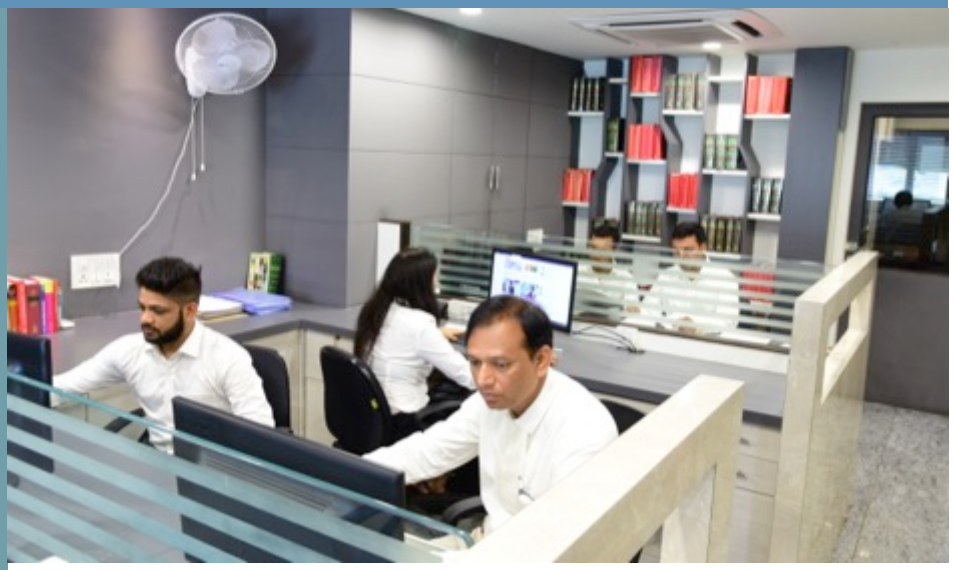
FIRM'S PRACTICE AREAS

Corporate & Commercial, Estate Planning, Trusts and Private Client, Dispute Resolution, Employment & Labour, Environment, Real Estate and Construction, White Collar Crimes, Start Ups, Non Governmental Sector, Insurance & Pension, Trademarks, Brands & Designs, Renewable Energy Practice, Insolvency And Bankruptcy Practice, Antitrust/Competition, Taxation Advisory, Media & Entertainment, Aviation, Education, Immigration, Cyber Laws, Medico-legal etc.

TYPES OF CYBER CRIMES

UNDER THE INFORMATION TECHNOLOGY ACT, 2000 [IT Act]

1. **HACKING (i.e. unauthorized access):** Section 43 of the IT Act provides that if any person accesses a computer, computer system or a computer network without permission of the owner, or downloads, copies and extracts any data, or causes disruption of any system, they will be liable to pay damages by way of compensation to the person so affected. The punishment for the offence of hacking is imprisonment for a term of up to 3 years or a fine up to Rupees 5 lakh or both.
2. **DENIAL OF SERVICE ATTACKS:** Section 43(f) of the IT Act punishes the Causing denial of access to any person authorized to access a computer network or resource with imprisonment for a term of up to 3 years or a fine up to Rupees 5 lakh or both.
3. **CYBER TERRORISM:** Section 66F of the IT Act specifies that whoever has the intent to threaten the unity, integrity, security or sovereignty of India, or to strike terror among people, denies or causes denial of access to any person authorized to access a computer network or resource will be punished with imprisonment for life.
4. **PHISHING:** Section 66C of the IT Act provides that whoever, fraudulently or dishonestly, makes use of the electronic signature, password or any other unique identification feature of any other person will be punished with imprisonment for a term of up to 3 years and a fine up to Rupees 1 lakh. Section 66D of the IT Act provides that whoever uses a computer resource for Cheating by Personation will be punished with imprisonment for a term of up to 3 years and a fine up to Rupees 1 lakh. Section 74 of the IT provides for knowingly creating or publishing an Electronic Signature Certificate for any fraudulent or unlawful purpose. The person will be punished with imprisonment for a term of up to 2 years or with a fine up to Rupees 1 lakh or with both.
5. **INFECTION OF IT SYSTEMS WITH MALWARE:** Section 43 of the IT Act provides that if any person introduces any computer contaminant or computer virus to a computer resource without the owner's permission will be liable to pay damages by way of compensation to the person so affected, and may also be punished with punished with imprisonment for a term of up to 3 years or with a fine up to Rupees 5 lakhs or with both.



INFORMATION TECHNOLOGY ACT, 2000

IT Act deals with cybercrime and electronic commerce in India. The Act extends to the entire country, which also includes Jammu and Kashmir. Further, it does not take citizenship into account and provides extra-territorial jurisdiction. The Act is applicable to any offence committed outside India as well. If the conduct of person constituting the offence involves a computer or a computerized system or network located in India, then irrespective of his/her nationality, the person is punishable under the Act.

The objectives of the Act are as follows:

i. Grant legal recognition to all transactions done via electronic exchange of data or other electronic means of communication or e-commerce, in place of the earlier paper-based method of communication.

ii. Give legal recognition to digital signatures for the authentication of any information or matters requiring legal authentication.

iii. Facilitate the electronic filing of documents with Government agencies and also departments.

iv. Facilitate the electronic storage of data.

v. Give legal sanction and also facilitate the electronic transfer of funds between banks and financial institutions.

vi. Grant legal recognition to bankers under the Evidence Act, 1891 and the Reserve Bank of India Act, 1934, for keeping the books of accounts in electronic form.

The features of the Act are as follows:

a. All electronic contracts made through secure electronic channels are legally valid.

b. Legal recognition for digital signatures.

c. Security measures for electronic records and also digital signatures are in place.

d. A procedure for the appointment of adjudicating officers for holding inquiries under the Act is finalized.

e. Provision for establishing a Cyber Regulatory Appellant Tribunal under the Act. Further, this tribunal will handle all appeals made against the order of the Controller or Adjudicating Officer.

f. An appeal against the order of the Cyber Appellant Tribunal is possible only in the High Court.

g. Digital Signatures will use an asymmetric cryptosystem and also a hash function.

h. Provision for the appointment of the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities. The Controller to act as a repository of all digital signatures.

i. The Act applies to offences or contraventions committed outside India.

j. Senior police officers and other officers can enter any public place and search and arrest without warrant.

k. Provisions for the constitution of a Cyber Regulations Advisory Committee to advise the Central Government and Controller.

SOCIAL MEDIA AND CYBER DEFAMATION

The increased usage of Internet services and smartphones has made social networking one of the most popular online activities. Social media enables users to connect, communicate and share information, photographs or videos with anyone across the globe. The tremendous growth in use of social media platforms/ social networking platforms has provided a fertile ground to cyber criminals to engage in illegal activities. For far too long, the Internet biggies have been making billions by ignoring the unscrupulous elements using their platforms.

The liability regarding cyber defamation in India can be on the author of the defamatory material online and on the service provider or an intermediary. However, Section 79 of the IT Act exempts intermediaries like Google, Facebook, YouTube and Twitter from liability in most circumstances, including if the intermediary did not put out the content and had observed due diligence while discharging duties under the Act. But these companies can be held liable for any unwarranted content if, despite adequate notice, it is not removed within 36 hours from their servers. At a time when everyone with a smartphone, from bureaucrats and politicians to a common person, is a self-styled 'news broadcaster' happily spreading (mis)information, 36 hours is like a decade. The duration would ensure the damage is already done. Most of these tech companies claim to have put in place in-house systems to check the misuse of their platforms, but the so-called checks and balances are often found lacking in their speed of response.

NON - APPLICABILITY OF THE INFORMATION TECHNOLOGY ACT, 2000

According to Section 1 (4) of the Information Technology Act, 2000, the Act is not applicable to the following documents:

- Execution of Negotiable Instrument under Negotiable Instruments Act, 1881, except cheques.
- Execution of a Power of Attorney under the Powers of Attorney Act, 1882.
- Creation of Trust under the Indian Trust Act, 1882.
- Execution of a Will under the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called.
- Entering into a contract for the sale of conveyance of immovable property or any interest in such property.
- Any such class of documents or transactions as may be notified by the Central Government in the Gazette.

6. **POSSESSION OR USE OF HARDWARE, SOFTWARE OR OTHER TOOLS USED TO COMMIT CYBERCRIME:** Section 66B of IT Act provides punishment for dishonestly receiving stolen computer resources or communication devices which may lead to imprisonment up to 3 years and a fine up to Rupees 1 lakh. Furthermore, any such tools used to commit a cybercrime may be confiscated under Section 76.

7. **IDENTITY THEFT:** Section 66C of the IT Act provides penalties for fraudulently or dishonestly making use of the electronic signature, password or any other unique identification feature of any other person. Such a person will be punished with imprisonment up to 3 years and a fine up to Rupees 1 lakh. Section 66D of the IT Act provides for the offence of cheating by personation using a computer resource. This attracts imprisonment of up to 3 years and a fine up to Rupees 1 Lakh.

8. **ELECTRONIC THEFT:** Section 72 of the IT Act provides for breach of confidentiality and privacy. It provides that if any person who has access to any electronic record, document or other material, without the consent of the person concerned , discloses such document or other material to any other person, they will be punished with imprisonment up to 2 years or with a fine up to Rupees 1 lakh or with both. Section 72A of the IT Act provides that any person who, while providing services under the terms of a lawful contract, has secured access to any material containing personal information about another person, discloses the same without consent, or in breach of the lawful contract, knowing it is likely to cause harm, will be punished with imprisonment up to 3 years or with a fine up to Rupees 5 lakh or with both.

9. **SECURING ACCESS OR ATTEMPTING TO SECURE ACCESS TO A PROTECTED SYSTEM:** Section 70 of the IT Act authorizes the appropriate government to declare a computer resource as a protected system and prohibit its access by the general public. The offence is punishable with 10 years of imprisonment.

CONCLUDING REMARKS

- Key to lowering cybercrime risk for private companies is by "gaining domain knowledge and putting in place a user-friendly cyber policy along with implementing a secure network." This includes "training users, monitoring the system and real-time response where a user requires assistance in operating the secure network."
- On the government side, bolstering information sharing mechanisms, building attribution capability and strengthening the coordination of vulnerability disclosure processes
- Although, there are laws in place which prohibit people from posting defamatory content online, most people are not aware of the same or are too negligent to realize whether such content is defamatory or not. There is a dire need of a system, which educates and makes people aware of what to do and what not to do, what is wrong and what is right and what is defamatory and what is not defamatory in the cyber space.
- Users can take variety of measures to keep themselves secure such as creating strong passwords, which are changed regularly, checking emails or links for authenticity etc.
- We need to educate our work force to have "digital empathy" since the employees are working remotely and potentially outside of the company's firewall. The organisations should ensure that employees are given necessary tools and training, and that there are lines of communication available in case they face any issue.

OFFICES

K.P. ASSOCIATES, JAIPUR

206, Axis Mall, Bhagwan Das Road, C-Scheme, Jaipur – 302001

K.P. ASSOCIATES, JAIPUR (BRANCH OFFICE)

107, LGF, Devi Nagar, New Sanganer Road, Jaipur-302019

K.P. ASSOCIATES, NEW DELHI

I-51, LGF, Jungpura Extension, New Delhi-110014

PARTNERS

PURVI MATHUR

9784339173 | purvi@kpandassociates.in

KUSHAGRA SHARMA

9829012069 | kushagra@kpandassociates.in

SAHIR HUSSAIN

9828825786 | sahir@kpandassociates.in