Cybercrime: A threat to Data Privacy
written by King Stubb & Kasiva | April 5, 2023

Cybercrime as the name suggests, refers to any crime committed in the virtual space involving the use of information technology or the internet. Since the advent of a globalised and technologically connected world, the ease of communication and networking has reached its zenith with the evolution of methods for transferring data and information from one place to another virtually. This has also given a huge scope for criminal activities in the virtual arena which include a number of white-collar cyber-crimes and cyber law along with data privacy breaches including identity theft, cyber espionage, pilferage of corporate information and data, banking frauds, and many other crimes.

Even though the right to privacy in India is a fundamental right under article 21 of the Constitution, data privacy and protection in the country does not have any specific statute or watchdog mechanism for the protection of data and prosecution of offenders.

Interlinking Cyber Crime And Data Privacy

The term cybercrime, not only refers to a crime committed on the internet but also a violation of privacy of individuals, identity theft, corrupt activities, sale of illegal narcotics and psychotropic substances through web-based portals and installation of spyware and malware through different programs. These illegal activities pose a huge threat not only to individuals but also to the security and well-being of the nation at large. Various scams including online shopping scams, credit card scams, theft from bank accounts

and other scams take place which lead to undermining the belief of people in online shopping apps and platforms. Therefore, in the present date, there is a proper need for cyber-crime and cyber law regulations.

Many times, theft of data in the forms of credit card, debit card and bank account balance takes place which undermines the faith of consumers while sharing payment details over the internet and also defeats the aim of the government in establishing a digital economy. Senior citizens and the less-technologically advanced groups also suffer due to breaches of data privacy by various vendors and e-payment platforms which may be identical to genuine payment portals and become victims of thefts and scams.

The challenges pertaining to cyber security and data privacy are not only faced by individuals but also huge companies and corporates who often become subject to spyware and ransomware. Various organizations maintain a database of important information including client information, market research, payment details and social media credentials, which if subjected to any electronic pilferage, can cause irreparable damage to the organization and related stakeholders.

The medical and pharma companies are also in the high-risk category due to the database of personal information including health and private vital statistics of users which are not subject to disclosure in open public. Therefore, any instance of cybercrime in this area would lead to a huge threat to data privacy. Moreover, the threat of cyberbullying and cyber defamation is also huge.

Growth Of Cybercrime In India

According to the National Cybercrime Reporting Portal, more than three lakh cases pertaining to cybercrimes and offences in the virtual space have been reported in the past two years. The Ministry of Home Affairs has also issued clarifications in the year 2019 stating the details of such offences and revealed that majority of the victims of cyber frauds and offences have been from the areas of Maharashtra, Karnataka and other areas which have a well-developed framework of internet facilities.

According to other reports, the number of cybercrimes in the past years has crossed more than one lakh in the year 2018 to nearly three lakhs in 2020. The COVID-19 lockdown and huge unemployment due to market fluctuations along with high rates of layoffs have also led to an increase in criminal activities in the virtual cyberspace.

Laws Pertaining To Cybercrime In India

Indian legislation does not have any specific law to tackle, prevent or punish cybercrimes. However, according to judicial decisions and precedents and relevant sections of the IT Act, 2000 cybercrime has been accounted and acknowledged in India.

Various landmark judgments have also shaped the jurisprudence pertaining to cybercrimes in India and have evolved the mindset of the courts to try cases of such nature along with laying down the procedure for trial. In the landmark case of Yahoo Inc. V. Akash Arora & Anr., the court for the first time took cognizance of a cybercrime and granted a permanent injunction refraining Mr. Akash Arora to use the name “Yahoo”.

The court has also taken cognizance of identity theft in digital space under various cases and in the landmark judgment of Vinod Kaushik &Anr. V. Madhvika Joshi and Ors., held that accessing email IDs of other individuals unauthorizedly is a criminal offence under Section 43 of the Information

Technology Act and calls for stringent action.
Section 43A in the Information Technology Act was also added in the year 2008 in order to add a mandatory provision for corporate bodies for protecting the leak of sensitive and confidential data. The amendment also brought in an angle of compensation and held that any breach of sensitive data by the company would render it liable for compensation to the aggrieved party. Section 72A of the Act has also laid down breach of personal data of any party as a penal offence which has called for strict action including imprisonment and/or fine.

Conclusion

The threat posed by cybercrimes to mankind is serious and adequate care must be taken in order to avoid any such incident. With the advent of Right to privacy becoming a fundamental right, strict measures should be taken by every stakeholder to minimise any scope for cybercrimes in the country. Adequate actions should not only be taken by companies or multi – national organizations by observing due care and caution but also by individuals as consumers and stakeholders by not letting their sensitive information get transferred into the wrong hands.

There is a need for proper digital training forevery user of virtual space and electronic modes. Moreover, social media and banking applications should be judiciously used in order to avoid any fraud or the likelihood of scams. There is a need to develop cybercrime and cyber law in Indiaalong with cyber defamation law in India.

It is high time that the legislature should also take adequate steps to ensure that there are proper laws and guidelines for ensuring compliance and guidelines for data protection. Secondly, adequate legislation to form separate offences along with payments and penalties should also be formulated to ensure confidence of people in the internet and virtual world.

King Stubb & Kasiva,
Advocates & Attorneys
Click Here to Get in Touch
New Delhi | Mumbai | Bangalore | Chennai | Hyderabad | Mangalore | Pune | Kochi | Kolkata
Tel: +91 11 41032969 | Email: info@ksandk.com