

2023

CYBER SECURITY LAWS IN INDIA

Awantika Singh

Recommended Citation

Awantika Singh, 'Cyber Security Laws in India' (2023) 2 IJHRLR 286-290.
Available at www.humanrightlawreview.in/vol-2-issue-3/.

This Art. is brought to you for free and open access by the International Journal of Human Rights Law Review by an authorized Lex Assisto Media and Publications administrator. For more information, please contact info@humanrightlawreview.in.

CYBER SECURITY LAWS IN INDIA

Awantika Singh¹

“Technology trust is a good thing, but control is a better one”.

— Stephane Nappo

As with the growing network of internet the crime relating to the to cyber security is also taking place. The most important things related to the effect which is done by the internet is that created a high risk on the right to privacy. The people are mostly in social media and all the data relating to it can be used by the dark internet. The security relating to the data is the most important and highly considerable point which must be dealt in the proper manner.

The cyber security in India is also becoming the most important. The reason why it is important to know about the cyber security is the increasing use of the internet. The most important step taken by the legislative is that they introduce the Information Technology Act,2000. Which mostly cover different variety of the cybercrime. The step was taken to prevent cybercrime in India.

- 1. IDENTITY THEFT**- The criminal in the steal the personnel information of the individual to use it for the purpose of financial fraud.
- 2. CYBERTERRORISM** - In this the information of person is used for the crime against the person or government for the reason to extort anything which the hacker need.
- 3. CYBERBULLING** - The person is targeted by the hacker and is humiliated, harassed, or defamed in the different social media platform as it created the feeling self-low stem in the eye of the person and the other people who are connected to that person.

¹ Advocate, High Court of Lucknow, Uttar Pradesh.

- 4. HACKING-** The information of the individual is hacked by the Hacker to use it for the illegal benefit. The hacking is of two type –
- a. Ethical-** use for legal purpose to identify the reason of crime,
 - b. Unethical-** which is punishable by the law of the land in which it is committed. The law relating to hacking is also given in the Indian Penal Code under Section 4(3) specifically talk about the “*any person in any place without and beyond India committing offence targeting a computer resource located in India*” is subject to the extra-territorial offence.
- 5. HARASSMENT AND STALKING-** The hacker may use the social media to collect the information and to harass and stalk the person most of the crime of stalking is taking place in relation to the women the social media is use to temper their image in public. The offence relating to the Stalking is also punishable under Indian Penal Code under Section 54D (1)(2) “*monitors the use by a woman of the internet, email, or any form of electronic communication, commits the offence of Stalking*”.

The basic reason why the need of cyber security system was needed is for the reason the people who suffer wrong should get justice. The people are hacked by the hacker for the reason of financial purpose, or women are targeted because of the reason to outrage the modesty of women and for the harassment purpose.

In the recent meeting of India- US jointly stated that “*PM Modi and President Biden reaffirmed their countries’ commitment to open, secure, inclusive, safe, interoperable and reliable internet, and to continuing cooperation on a range of cyber-security issues, including preventing and to responding to cyber-threats, promoting cyber-security education and awareness and measure to build resilient Cyber infrastructure*”.

Further they said that on military front “*there plan to expand the strength of cyber command, which is staffed with a limited number of officers as compared to either the US or China. The cyber command will have three center – two in north and one in south-to not only defend India but also to counter the cyber challenge*”.

Now if we look into data which was given by parliament, India is facing 1.16 million cyber-attacks in the year 2020, in which 3,137 incidents take place every single day in a year. According to the IBM report “*Cost of Data Breach Report, 2020*” in India there are 2 Million attack which has been seen the rise of 9.4 percent from the last year of 2019. In the report of FBI’s Internet Crime report, India has been ranked on 3rd position among the first 20 countries which are mostly affected by the cybercrime.

If we look into the drawback which is face by the India is that it cannot fulfill the 30 percent of its job due the lack of proper qualification. People in India are slowly getting aware of the fact that cyber security is a good career option and this has created hustle in the manpower the supply of the person is very much less than the demand. The it sector is developing in its full level and to understand the need and requirement of the industry people should become aware of the cyber security.

JUDGEMENT BY THE COURT ON CYBER SECURITY

1. Shreya Singhal v. Union of India²

The apex court gave the judgement on the point where two women posted offensive comment on Facebook under Section 66A. In this case supreme court observed that the Section 66A is creating a hurdle in Freedom of Speech and Expression.

2. People's Union for Civil Liberties v. Union of India³

² *Shreya Singhal v. Union of India*, AIR 2015 SC 1523.

The case was filed by the NGO after the judgement of the case the supreme court said that it is shocking how the police is still using the Section 66A which was struck down and declared unconstitutional by the court.

CONCLUSION

As the Internet network grows, so does cybersecurity-related crime. The most important thing about the impact of the Internet is that it poses a high risk to your right to privacy. People mainly use social media and all data associated with it can be misused by the dark web. Data security is the most important and very important issue and should be properly addressed. Cyber security in India is also becoming more and more important. The reason why it's important to know about cyber security is because of the increasing use of the Internet. The most significant move by Congress is the introduction of the Information Technology Act of 2000. Most of them target different types of cybercrime. This step was taken to prevent cybercrime in India.

“Arguing that you don’t care about the right to privacy because you have nothing to hide is no different than saying you don’t care about free speech because you have nothing to say”-Edward Snowden

In conclusion, we can say that people should get much aware of the technology which is used by them. Using something for the comfort is not bad but not full getting known about it can create mess in the life.

³ *People's Union for Civil Liberties v. Union of India*, AIR 1997 SC 568.