

## CYBERCRIME WITH RESPECT TO RIGHT TO PRIVACY

Priya Garg

Student , School of Law, Lovely Professional University, Phagwara Punjab, India

Priyagarg2102@gmail.com

Received 30 April 2022 Received in revised form 15 May 2022 Accepted 17 May 2022

Available online 22 May 2022

### ABSTRACT

In today era the pace of technology development is expanding day by day. the people have turned completely dependent on the internet. It has become a necessity in people's life. The netizens have threatened their privacy in cyberspace. With the increasing use of internet, citizens privacy is being exploited. This concern is felt more in the case of youth and teenagers who constitute maturity of the internet addicts and are susceptible in understanding the threat of exposing themselves to the cyber world. crime is rapidly increasing against women is in all field of cybercrime The issue of 'internet privacy' has been increased by social networking sites, which are increasingly used for social interactions between individuals through uploading personal content. When a person's privacy is violated through internet, there are a number of questions arises, as what constitutes a violation. Who is responsible for this? And what is the remedy for this crime? One of the most important fundamental human rights is the right to privacy. In addition, courts in India have recognized it as a fundamental right, despite the fact that it is not stated in the Indian Constitution. There are laws that ensure the right to privacy is protected. As IT act 2000 has been existence for 21 years the cybercrimes are rising day by day and enforcement of law faces many challenges as a result of existing lacunae in this act. Many provisions regarding the cyberlaw are absent in this act. The present research paper includes various Indian laws which are for the protection of cybercrime, and how right to privacy can be protected and various remedies to counter the increasing cybercrime against women, children and suggestion can be given to improve present situation.

**Keywords:** Right to privacy, Cyber crime

### I.INTRODUCTION

It is very important to discuss about the constitutional and legal status of right to privacy. The right to privacy is supreme right which is given to all the human beings at the time of birth. From these right human beings are free from any interference but it is with some exception. Right to privacy is considered supreme from the time of ancient time. it has received recognition and protection all over the world. Human beings, by their very nature, demand a space free of all forms of disturbance. This is essential for the growth of their unique personalities. The fact that the right to privacy is mentioned specifically in ancient texts and sources demonstrates its relevance to all communities. This right has always been recognised and protected in all communities. Human rights movements have had a significant impact on the notion and jurisprudence of legal rights in the 21st century. The right to privacy is mentioned specifically in all international human rights documents. This right has the status of a fundamental human right, which States Parties to the Human Rights Instruments are required to preserve[1]. As a result, nations all over the world have established and implemented provisions in their legal systems to ensure that the Right to Privacy is protected. Under the Indian Constitution, the right to privacy is given the highest level of protection as a basic right. Although the Indian Constitution does not expressly specify this right, other essential rights such as the right to life and personal liberty provided in the Constitution

clearly suggest that it exists implicitly[2]. The Indian judiciary has often stated that the right to privacy is an integral aspect of the right to life and personal liberty. The Supreme Court has consistently upheld this right, with few exceptions, in the interests of national security, law, and order.

In India, the introduction of information technology has opened up new options for infringing on one's right to privacy. Prior to this, there were only a few ways to violate one's right to privacy, and it was difficult to do so. It was simple to track out the source of any such infringement and assign responsibility for it. Cyberspace, on the other hand, has provided new difficulties in this area. Individuals are exposed to privacy infringement not only because of the rise of cyberspace, but also because of major problems with the steps to take to prevent such infringement and the remedies to give if it occurs.

The internet's threat to privacy is not a new phenomenon. The developed countries of the globe, where information technology is deeply embedded among the public, have already introduced security measures that can successfully address this problem to a large extent. While operating in cyberspace, the 'citizens' of these countries usually observe all of these security procedures.

Information technology, on the other hand, has not yet reached the grassroots levels in countries like India. The general public is still unaccustomed to the dangers it poses to their privacy. As a result, security precautions are frequently disregarded, making people more vulnerable to attacks on their privacy. In India,

the bulk of internet users are teens who are unaware of the dangers of exposing themselves to the wholly unknown cyber-world. They frequently fail to assess the potential harm they face when utilising the internet for social networking or other purposes. Internet users in India are so unconcerned about privacy issues, and a lack of security and regulatory measures in this area is exacerbating an already major problem.

Various Indian laws which are for the protection of cybercrime, and how right to privacy can be protected and various remedies to counter the increasing cybercrime against women, children are discussed in this paper.

## II. THREATS TO PRIVACY IN CYBER SPACE

William Gibson used the term "cyberspace" in his novel *Necromancer*, published in 1984. Cyberspace is a virtual world of computers that uses the internet to allow people to interact, do commerce, conduct transactions, and create graphics. The Internet was created in the 1960s to improve communication and research. With the advancement of 'e'-technology, everything becomes easier to obtain, as well as a means of committing crimes without exerting any effort. Social networking sites, which allow users to interact, discuss, and share with others, capture the pictures better than anything else. However, in recent years, there have been increased in "moral panics" about the information available on the Internet and its potential for illegal exploitation.

- **Cyber Snooping** – we see many ads on the internet and mobile phones offering software that will let us keep an eye on a computer system. these types of software keep an eye on your computer. this type of software is not used for good this but it is used by criminals. cyber snoop traces the activity what is done on computer and its data. cyber snoop is used widely to keep an eye on the internet activity. The configuration programme for Cyber Snoop allows us to configure how we track and restrict access to the Internet Web, E-mail. Individual users' Internet access is supervised with the help of profiles. The system's available Windows User names are used to create user names. It infringes the privacy of the other people.
- **Cyber stalking** – internet became the important pathway for ab cyber stalker. it means to stalk someone on social media and collecting their data. Downloading pictures and using it as blackmailing. There are 2 famous case of cyber stalking Ritu kholi case and Pandurang prabhu. cyber stalking is clearly infringement of right to privacy under article 21 of Indian constitution.

- **Identity Theft**- The crime of electronically impersonating someone else for financial gain is frequently referred to as phishing. This is typically done by gaining access to secured systems using someone else's login ids and by using someone else's digital/ electronic signature in the process of electronic contracts. A new sort of crime has evolved in which mobile phone sim cards are 'cloned ' allowing criminals to make calls on other people's accounts. Today locked cell phones are not safe by using this people can use your data for there benefits. It is punished under information technology act 2008
- **Copyright infringement**- Copyright is a legal privilege granted to writers or creators of works by the government. The copyright owner has a range of exclusive rights under copyright law, including the right to publish the work, regulate copying, and make the material available online. Copyright protection is activated when the manuscript is completed. The Indian Copyright Act, 1957 supervises and controls India's copyright system; nonetheless, the majority of copyright infringement occur online, such as clicking, downloading photographs without permission, and uploading to the Internet.
- **Website defacement** -Website defacement is a first-time offence committed against a website with the goal of defrauding the website's visitors. It is an assault on a website that alters the site's or a webpage's aesthetic look. Typically, this is the work. Defacers are hackers who get access to a web server and replace the hosted website with one of their own. Defacement is sometimes referred to as an electronic kind of graffiti, although it can also refer to other types of graffiti. Politically motivated "cyber protestors" employ vandalism to propagate their messages. or hacktivists, for example. It is a newer version of the Pharming concept.

## III. WHAT AMOUNTS TO PRIVACY INFRINGEMENT IN CYBERSPACE?

By its very nature, cyberspace is not user-friendly in terms of privacy. Any information published and shared on the internet is permanently kept in the form of a link and is available for reference by anyone who can track it down. Information of any kind, whether it's an email, credit card information, personal content like photographs and documents, chats and messages in all formats, and so on, is stored someplace on the remote computer and can be read at any time and by anyone unless a few security

precautions are taken. As a result, speaking about perfect privacy protection via the internet is a paradox, as it is not realistic.

Similarly, while transacting on the internet, internet users disclose a variety of information in the form of text and images about their personal and professional lives, such as bank accounts, credit card numbers, passwords, emails, chats, and messages. The information thus provided is intended for a specific recipient, and most users expect it to be utilised only by the person to whom it is addressed and for the purpose for which it was shared. The information shared on social networking sites is more general in nature and can be accessed by a large number of people, whereas the information shared during individual chat sessions, via email, or on any commercial website for specific transactions is less general in nature and intended only for those with whom it is shared. Furthermore, the information supplied on social networking sites or any other website has a specific purpose, and the user expects that this information will be utilised only for that purpose. Any unlawful access or use of this information compromises an individual's privacy significantly.

#### **Cybercrime against women**

Cybercrime against women is a common occurrence nowadays. Every second, one woman in India falls victim to cybercrime, and online podiums have become the new venue where a woman's privacy, dignity, and security are increasingly being threatened. Some criminals use technology to defame women by sending obscene e-mails, WhatsApp messages, stalking women on websites, chat rooms, and, worst of all, developing pornographic videos, most of which are created without their consent, spoofing e-mails, and morphing images for pornographic content using various online software.

Indian women are unable to report cybercrimes immediately because they are either unaware of where to report such crimes or are unwilling to risk social disgrace if they do so. The impact of cybercrime on women is more mental than physical, despite the fact that the focus of laws safeguarding women's protection is more on physical than mental harm. In this case, it may be said that women's mindsets in particular need to broaden, and they must be the whipping boys, taking derring-do against such offenders and filing an urgent complaint. The majority of issues may be resolved if women report crimes and abusers as soon as possible. [3]

Cybercriminals use computer technology to gain access to personal information and to use the internet

for harassment and exploitation, such as stalking, blackmailing, threatening via email, photo morphing, and cyber pornography, among other things. In India, criminals are increasingly utilising cyber platforms to harass and assault women for entertainment. Cyber stalking, harassment, extortion, blackmail, and other forms of harassment primarily target women. Women frequently place their faith in criminals or abusers and disclose sensitive information, leading to a rise in cybercrime.

Cybercrimes against women begin with the creation of fake Ids on Facebook, Twitter, and other social media platforms, which cause serious harm to women by allowing criminals to blackmail, threaten, intimidate, or cheat women via messenger conversations and email.[4]

#### **Reasons for the growth of cyber crime against women in india**

The reasons for the rising rate of cybercrime against women can be divided into two categories: legal and sociological. The statute dealing with cybercrime does not expressly mention those crimes under the related sections, whereas various laws such as the Indian penal code, Constitution, and others provide special protection to women, but the same protection does not appear to be provided in general. Cybercrimes, on the other hand, went unreported for a variety of reasons, including the victim's uncertainty and shyness, as well as her fear of defamation of her family's name. Many times, such victims believe that they are to blame for the crime that has been committed against them.

#### **IV. JUDICIAL APPROACH OF CYBER CRIME**

- **Ritu Kohli case [5]-** Mrs. Ritu Kohli filed a police complaint against a person who was using her name to communicate over the Internet at the website <http://www.micro.com/>, particularly in Delhi channel, for four days in a row. Mrs. Kohli further claimed that the individual was communicating on the Internet, using her name and address, and using vulgar language. The same person was also distributing her phone number to other chatters with the intention of encouraging them to call Ritu Kohli at odd hours. As a result, Mrs. Kohli received about 40 calls in three days, the majority of which were during after-hours. The alleged call caused turmoil in the complainant's personal life; therefore, IP addresses were tracked and police investigated. The problem

was investigated thoroughly, and the culprit was eventually apprehended. He was arrested and charged under section 509 of the Indian Penal Code, following which he was released on bail. This is the first time a case of internet stalking has been documented. Cyber stalking is not protected by India's existing cyber legislation, similar to the issue of email harassment. The culprit can only be booked remotely for breach of security and privacy under the provisions of Section 72 of the IT Act. The culprit could possibly be charged with criminal trespass under Section 441 of the IPC, as well as outraging the modesty of ladies under Section 509 of the IPC.

- **State of Tamil Nadu vs. Suhas Katti [6]**, emails were forwarded to the victim, a divorced woman, requesting information by the accused through a phoney email account he made in her name. The victim was subjected to mental harassment as a result of the publishing of messages, as she received unwanted phone calls in the brief that was soliciting. In February 2004, she filed a complaint in the Egmore court, and the accused was apprehended by the Chennai police cyber cell. He was charged under Sections 469/509 of the Indian Penal Code and Section 67 of the Information Technology Act of 2000. He was charged with the above-mentioned sections once the charges against him were proven.
- **Unacademy Experiences a Data Breach** Unacademy, a Bengaluru-based edtech business, is one of India's largest online learning platforms, offering online courses to millions of students around the country. In exchange, it saves a vast quantity of information from users, including their name, age, email address, phone number, and financial information like credit and debit card numbers. According to reports, the data compromised included usernames, email addresses, hashed passwords, the date the user first joined and last signed in, first and last names, account profiles, and account status. Hemesh Singh, Unacademy's co-founder and CTO, confirmed the data breach and assured that no sensitive information such as bank records or passwords had been compromised due to Unacademy's strong encryption techniques and two-factor authentication. He further stated that only the most basic information of approximately 1 crore customers was compromised. However, according to Bleeping Computer, a website that answers computer security problems,

hackers have access to more than just the user database. Almost all businesses keep data in online database servers, making them vulnerable to cyber-attacks. Even a minor security breach can result in the loss of data belonging to millions of people who use their services. Unauthorized access to a protected system is covered under Section 70 of the ITA, as does breach of confidentiality and privacy under Section 72 of the ITA.

#### **V.PRIVACY INFRINGEMENT IN CYBERSPACE: TOOLS AND MEASURES**

The complete privacy on the internet is difficult to achieve. It is impossible to stay away from the internet in today's world. After the covid from teenagers to youth are working on internet for their livelihood from attending online classes to working in the office is all depend on internet. Cyber specialists and authorities at the national and international levels are already hard at work figuring out how to reduce the threat to an individual's online privacy. The essential approach that may generate positive effects in this area is the users' self-restraint on his 'web-habits.' The user must be aware of the dangers of using the internet in an unmindful and insecure manner. It is vital to use caution when providing personal information of various kinds that could be published on the internet. While using the rapidly developing social networking phenomena, it is also vital for internet users, particularly young internet users, to build in themselves a sense of responsibility toward their own person. These social networking sites contain built-in security features that allow users to limit the sharing of information to certain recipients, which must be used and relied upon by users.

The computers used for the online transaction should be properly secured by installing the high security. it is very important for the internet users not to use the public café for the important online transaction without knowing the security measures used by the café. It is essential to logout all the important websites and never saved the password which is usually asked the system. Online purchasing should be done through web portals that guarantee the highest level of security for the information that is provided with them. To improve security, software updates must be correctly updated, unused accounts must be terminated, and strong passwords must be used.

Web service providers and internet service providers are also obligated not to infringe on internet users' privacy and to take all reasonable steps to guarantee that their privacy is protected to the fullest extent possible.

### Privacy invasion in the cyber world

The most prevalent of all sorts of privacy breaches in the modern world is cyber-crime, in the virtual world of the Internet where "the computer is either a tool or a target." Most of the people utilise the Internet for a number of purposes, such as social networking sites like Facebook, Twitter, and LinkedIn, Instagram as a result of widespread Internet use and technological advancement in the e-world. These sites have over 400 million members, and their applications, such as talking, video calling, and photographing, can store a lot of personal information in their databases.

Internet users can reduce the danger of privacy invasions by disclosing personal information in a regulated manner, such as revealing their I.P. address or using non-personally identifiable profiling. Companies are hired in today's society to monitor which websites individuals visit and collect data in order to establish a database for marketing purposes. Spreading viruses and exploiting various types of flaws are two more harmful behaviours that involve violation of privacy. Privacy attackers can easily trace any information given by children and teenagers on social networking sites, making them easy target for them. E-mail scams and attachments may be used to manipulate them into installing malware and disclosing personal information. The Children Online Privacy Protection Act was formed in 1998 by the US Federal Trade Commission in response to the lack of privacy for children on the Internet. The Children's Internet Protection Act was enacted in 2000 with the goal of implementing safe Internet measures such as guidelines and filter software. These regulations, awareness efforts, parental and adult monitoring measures, and Internet filters can all contribute to making the Internet a safer place for children all across the world.

Privacy protection is one of the most critical topics on the Internet today, and it is a source of concern for Internet users. Users' personal information is collected by websites through online registrations, surveys, and forms. 'Cookies' are also used to collect information from users.

### Internet privacy legislative measures

Right of privacy is most important right for human being have to maintain his or her privacy .it became very necessary to make the rules and regulations to improve the internet privacy which is violated in large. various big countries have raised the issue of privacy infringement by cyberspace. many big companies whose right are violated have raised the issue in big events of

google and asked them to increase the security of internet. many big internet gains have also requested to united nation organization to make regulations for this infringement. but till now no common regulation came up for the breach of privacy through internet

In India, the right to privacy is recognised as a fundamental right, and it is the obligation of the government to preserve this right through appropriate legislation and policy measures. There is currently no comprehensive law protecting privacy or providing legal remedies for its infringement. The Information Technology Act of 2000, which incorporates several rules relating to privacy protection in India, is the primary law governing internet use in India. Various sections of the Information Technology Act and its Rules ensure that information shared on the internet by users is protected[7]. The following is a summary of the protection:

- These rules require corporate organisations to develop and maintain acceptable security practises in regards to the information they receive, keep, deal with, and transfer, among other things.
- It is required of business organisations to inform users of their privacy policies and gain their consent to do so [8].
- Before collecting any sensitive information, it is important to get the users' consent and to indicate the authorised purposes for which the information will be used by the corporate body [9].
- The regulations restrict the preservation of obtained information for longer than is necessary for the purposes for which it was collected [10].
- The regulations oblige corporate organisations to give users access to information that has been shared and to allow them to amend it if they so desire.[11].
- Any failure on the part of a corporate body in this respect is subject to a penalty in the form of compensation to the person affected by the failure, as well as the possibility of criminal culpability if the effect of the failure is wrongful loss or gain [12].
- The law also establishes a grievance system via which a person who has been harmed by a privacy infringement can seek redress[13].
- The Act stipulates harsh penalties for offences like as hacking, sending insulting texts, voyeurism, and child pornography, among others. The copyrighted data is further protected by prohibiting any use of the

material without prior authority.[14]

- The cybercafés are regulated by requiring them to implement various security measures as well as timely inspection in this regard by the authorities established within.[15]

Internet Service Providers are eligible for licences in India if they meet the criterion of implementing the relevant privacy and information security safeguards. The Telecom Regulatory Authority of India, which is in charge of maintaining and regulating telecom service standards in India, has also developed guidelines for unsolicited telemarketing calls and other intrusions into an individual's privacy in India. The Indian courts have also developed significant jurisprudence on the topic of online privacy by supporting the sanctity of this right and enforcing it through appropriate orders and, in some cases, by issuing guidance.

The Indian government has just agreed to adopt a complete privacy law, which would be introduced in parliament soon. For illegally recording phone calls and making their content public, this law imposes severe penalties, including the cancellation of telecom service provider licences. This would result in a five-year prison sentence and a fine of Rs 1 lakh.

#### **VI. CYBER CRIME CHALLENGES FOR INDIA**

The internet has both advantages and disadvantages, in addition to its convenience. It also brings with it some difficulties. that India is dealing with. Some of them are listed below. The threats posed by cybercrime to India.

- Security staff are not well -prepared to deal with high-tech crimes.
- The majority of cybercrime laws under the IT Act are bailable with only a minor fine.
- There is a significant difference between cyber criminals' technological skills and those of techno-legal specialist lawyers and judges. The current court system is incapable of appreciating digital evidence and the unique aspects of cybercrime.
- Lack of public awareness of cybercrime and its prevention measures.
- There are insufficient protocols for cybercrime that extends beyond India's borders.
- When compared to other crimes, government funds for information and communication technology are lower.

#### **Steps taken by the Government to spread awareness about cybercrimes:**

- Complainants can now register complaints about child pornography/child sexual abuse material, rape/gang rape imageries, or sexually explicit materials using an online cybercrime reporting system.
- The Indian Cyber Crime Coordination Centre (I4C) has been developed as part of a programme to deal with cybercrime issues in India in a comprehensive and coordinated manner.
- The National Critical Information Infrastructure Protection Centre (NCIIPC) was established to secure the country's critical information infrastructure.
- CERT has demanded that all enterprises that provide digital services disclose cyber security incidents.
- The Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) was established to detect dangerous programmes and provide free tools to eradicate them.
- Formulation of a Crisis Management Plan to Combat Cyber-Attacks and Cyber- Security Threats [16].

#### **VII. CONCLUSION AND SUGGESTIONS**

As the digital economy has evolved over the last decade, cybersecurity has taken on a new importance around the world. Furthermore, the relevance of cybersecurity is growing every day, thanks to the introduction of a new wave of cyber-physical systems known as the 'Internet of Things,' which includes wearables, "smart" home devices, autonomous vehicles, and unmanned aerial aircraft (also known as drones). Despite this digital transformation, it is becoming increasingly obvious that both the public and private sectors are falling behind when it comes to cybersecurity threats. There are some suggestions :

- In dealing with cybercrime, a more comprehensive approach is required.
- Stricter sanctions and punishments for such offences must be included in the ITA, IPC, and other cybercrime statutes.
- There must be a plan in place to teach internet lawyers and judges.
- Providing for the management of electronic evidence; allocating greater funds for security personnel training to deal with high-tech crimes.
- Raising public awareness about the many types of cybercrime that might occur and releasing guidance on the security steps that must be taken to avoid becoming a victim of cybercrime.

The value of a person's right to privacy in maintaining his or her dignity is immeasurable. In view of the growing number of attacks on internet privacy, it is critical to address this issue quickly and implement strict safeguards. The solution to this problem resides on global initiatives, and any action taken on a national level is unlikely to provide significant effects. However, some system for providing effective remedy to those who are victims of privacy violations must be developed. The regulatory measures implemented in India in this area appear to be sufficient on paper, but when it comes to implementation, there is a lack of understanding among users and their online habits in India.

### References

[1] Art.12 of the Universal Declaration of Human Rights and Art.14 and 17 of the International Covenant on Civil and Political Rights.

[2] Right to privacy is not enumerated as a fundamental right in our Constitution but has been culled out of the provisions of Article 21 of the Constitution and other provisions of the Constitution relating to Fundamental rights read with the Directive Principles of State Policy. Referred in Justice Palok Basu's 'Law relating to Protection of Human Rights' p.n.505.

[3] Dhruvi M Kapadia ,Cyber Crimes Against Women And Laws In India , <https://www.livelaw.in/cyber-crimes-against-women-and-laws-in-india/>.

[4] Nishant Singh, Crime Against Women, 52 (Ancient Publication House, Delhi, 2014).

[5] [https://en.wikisource.org/wiki/.ITact\\_2000\\_Act\\_](https://en.wikisource.org/wiki/.ITact_2000_Act_).

[6] Suhas Katti v. State of Tamil Nadu C No. 4680 of 2004.

[7] Based on the information sourced from India Telecommunications Privacy Report referred on <https://www.privacyinternational.org/reports>.

[8] Section 43A of the Act and Rule 4 of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

[9] Section 43A of the Act and Rule 5(1) of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

[10] Section 43 of the Act and Rules 5(5).

[11] Section 43A of the Act and Rule 5(6) of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

[12] Under Section 43A, any body corporate who fails to observe data protection norms may be liable to pay compensation if : it is negligent in implementing and maintaining reasonable security practices, and thereby causes wrongful loss or wrongful gain to any person. "Wrongful loss" and "wrongful gain" have been defined by Section 23 of the Indian Penal Code.

[13] Section 43A of the Act and Rule 5(9) of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

[14] Sec.66 and all its subsections of IT Act. 2000.

[15] Information Technology (Guidelines for Cyber Cafe) Rules, 2011.

[16] Press Information Bureau Government of India Ministry of Home Affairs, available at: <https://pib.gov.in/Pressreleaseshare.aspx?PRID=1579226>.