



## **The Socio-Legal Impact of Cybercrime on Children in India: Challenges and Safeguards**

***KHYATI SINGH<sup>1</sup>, RAJAT PANDEY<sup>2</sup>, DRONE KRISHNA<sup>3</sup>***

<sup>1</sup> EMAIL ID: [singhkhvati65@gmail.com](mailto:singhkhvati65@gmail.com)

Contact no.: 8210627634

Educational qualification: LL.B. (UNIVERSITY OF DELHI), LL.M. (NATIONAL UNIVERSITY FOR STUDY AND RESEARCH IN LAW, RANCHI)

<sup>2</sup> EMAIL ID: [rajat.asunrise@gmail.com](mailto:rajat.asunrise@gmail.com)

Contact no.: 9670820960

Educational qualification: LL.B. (UNIVERSITY OF DELHI), LL.M. (NATIONAL UNIVERSITY FOR STUDY AND RESEARCH IN LAW, RANCHI)

<sup>3</sup> EMAIL ID: [dronekrishna@gmail.com](mailto:dronekrishna@gmail.com)

Contact no – 8294343666

Educational qualification : 4<sup>th</sup> year , BA. LLB (Amity university, Jharkhand)

---

### **ABSTRACT :**

Cybercrime is becoming a major threat in the contemporary environment. Consider its disadvantages in addition to its advantages. Cyberspace is a more common place for computer-related crimes, such as hacking, data theft, privacy invasion, phishing attacks, intellectual property infringement, identity theft, and others which is proof of this.

Because of the anonymity and speed at which these crimes can be committed, cyberspace is an appealing medium for cybercriminals. For example, it might speed up cybercrime or breach someone's privacy. Although cybercrime is a worldwide problem, children are the obvious targets of this new kind of crime. Despite the fact that all criminal and penal laws place a high priority on protecting children and their vulnerability, they are unfortunately powerless online. It is alarming how common cybercrime against children is, as it may pose a threat to a person's general security. Through the World Wide Web, users can exchange text, images, audio, and video content. The extensive dissemination of this kind of material is especially detrimental to children.

---

### **INTRODUCTION**

The issue of cybercrime has not always existed. Any unlawful activity that takes place on or through a computer, the internet, or any other piece of technology is referred to by this phrase under the Information Technology Act. At the moment, cybercrime is the most pervasive and dangerous kind of crime in India. Criminals harm not just the government and society, a great deal of money, but they are also adept at concealing their identities. Technologically savvy criminals commit numerous crimes on the internet. A more expansive definition would be any illegal activity that makes use of a computer, the Internet, or both as a tool, a target, or both. Every day, millions of people utilize the Internet for anything from checking their emails to making purchases. Faster and more user-friendly connections that are available through additional channels, such mobile devices and portable gadgets that allow individuals to communicate with one another, have created new e-commerce prospects. The Internet may become as ubiquitous as gas or electricity over the next decade. Online shopping and banking are growing in popularity. People can now cheat in numerous ways because to the advancement of technology. Since the turn of the century, social networking services have grown in popularity. These websites have been used by many people to meet new people, discuss their feelings, and keep in touch with old acquaintances. Unfortunately, cybercriminal organizations have exploited these websites for their own illicit ends. People have been spending more money in recent years. They spend more time on these networks since they are growing in significance to them. The development of information technology (IT) in the modern world has an impact on people everywhere. People discover new things and create new creations every day. As a result, the scientific community has grown, and the legal community now faces additional challenges. As these technologies proliferate, new kinds of cybercrimes are being perpetrated, raising concerns about the future on a worldwide scale. Indian courts may be able to interpret the word "cybercrime," even though no law or act has defined it. Cybercrime is a bad thing that can't be stopped. It comes from people taking advantage of society's growing reliance on technology. The number of people who use computers and other related technologies in their daily lives is growing quickly. These technologies are now a necessity that makes life easier for their users. It has no limits and can't be measured. The internet has both good and bad things about it. Some of the most recent cybercrimes are cyberstalking, cyberterrorism, email spoofing, email bombing, cyberpornography, and cyberdefamation. Several traditional crimes could be called cybercrimes if they are done online.

---

## Cyberspace

The first person to use the word "cyber space" was William Gibson. He later said it was "an evocative and basically meaningless"<sup>1</sup> buzzword that could be used to mask what he really meant by all of his thoughts about cybernetics. People today use this to talk about everything that has to do with computers, IT, the Internet, and the numerous cultures that live on the web. "Cyber space" is a word that is often used to talk about the online world where all IT-based communication and actions happen. It will be hard for you to settle down online. Your internet presence, blog, social networks, email accounts, private data, and reputation are all examples of intangible assets. Cyberspace is more like a worldwide electronic community because there are no physical obstacles to contact. Cyberspace is the virtual world made by computer networks, where people can interact with each other in many ways, such as sharing information, working on projects together, promoting business, making art and entertainment, talking about politics, and more. Cyberspace is a new frontier that everyone may use. Unfortunately, cyberspace is a new place for many types of crime because some people use this shared past. It is now used for all things relating to IT, the web, and the many online groups.

People who utilize the Internet are called "netizens." The word comes from the words "network" and "citizen." People who use computers, IT, and the World Wide Web (WWW) are called "Netizens." According to Webster's Dictionary, cyberspace is an electronic system made up of different computer networks, message boards, and other things. People think of it as an endless supply of information where they can study anything, talk about everything, and even enjoy a kind of virtual reality.

---

## Concept of Crime

As someone once stated, crime has always hinged on the strength, energy, and movement of public opinion from decade to decade, country to country, and even within the same country. Crime has always been a part of society and will always be. As long as society keeps improving safety measures. Criminals will change the way they do things. People have sought to explain the idea of crime from the beginning of time to now in order to understand it. This is how you make sense of these two times.

### The Early Idea of Crime

Crime is always hard to find, and when things become better, it always tries to hide. Countries have diverse ways of dealing with crime, depending on how much and what kind of crime it is. There are a few ways to deal with it. People in England didn't recognize the difference between crimes and torts until the 10th century. This was because family ties were stronger than community ties, the hurt person and their family could achieve revenge on their own, and going to court was seen as a way to help oneself instead of getting even.

In those days, people who did bad things had to pay their victims. It depended on how serious the wrong was and how significant the person who got wounded was to the community how much money they got. We can only claim that the rules in the past didn't make people act a specific way like they do now. In the 12th and 13th centuries, In Early English civilization, the only things that were crimes were those that injured people or religion. In ancient societies, there was no difference between the law of crimes and the law of wrongs. In these cultures, the only rule was the law of wrongs. The legislation is put into effect right away when a crime is committed, no matter what the victim wants. In ancient cultures, the law didn't work unless everyone agreed to it. People thought that only the person who did something wrong could see that he had done something wrong and that no one else, not even outside agencies, could help him. This was true during the 18th century, which criminologists call the "Age of Miraculous Reorientation." At the time, it was clear that crime was connected to how society was run. Crime was also rare in the past, when farming, government, healthcare, medical research, and even the most basic needs of life were yet new. When it happened, it was frequently simple and based on our most basic needs, such as desire, greed, revenge, jealousy, and sexual drive.

This could be because the West and India have quite different economic conditions. Urbanization, industrialization, the rise of science and technology (S&T), and the spread of civilization are all things that have led to an increase in crime. Scientists have come up with ways to find criminals and stop them from doing bad things.

### *The modern definition of crime*

The new method to deal with crime is to be practical. Because to scientific development, the industrial revolution, and better civic institutions, crime has altered in modern civilization, especially in the information society. The law is continuously changing since it is not the same for everyone. The list of offenses is always changing. Some crimes are added, some are amended, and others are removed off. It's hard to realize how much crime has changed. People are changing, and because of that, the way people think about crime is changing all around the world. People in different nations and at different eras have different ideas about crime. For example, something that is unlawful in one country might not be illegal in another, and something that is prohibited now might not be illegal tomorrow. Because of the growth of the economy and the concentration of wealth, crime is more common now than it has ever been. Changes in the media have also changed how people think about crimes like rape, prostitution, burglary, murder, and other traditional crimes. They have also created new types of crime. Crime waves are now measured in hours and minutes instead of months and years. Social and economic issues can help explain its expansion, but there are also other reasons why it keeps growing, like the fact that criminals can stay mostly anonymous and that borders don't matter. This makes it almost impossible to figure out who has jurisdiction and offers criminals an equal opportunity to get away, which motivates them want to do more. So, you can understand cybercrime by looking at all the other kinds of crime and the fact that it is common, anonymous, and not monitored by the government.

---

<sup>1</sup> Introduction to Cyberspace, Computer and Internet - Adv Rajesh Kumar, (2012)

### ***Basic Parts of a Crime***

The state should always have to show proof of actus reus and mens rea in order to prove guilt, save in cases when the offense carries a lot of culpability. In the past, when strict responsibility was in place throughout Europe, anyone who did wrong got harsh punishments to make an angry god happy. Later, the connection between what God did and the bad things that happened because of it was replaced by the connection between what people did and the pain it caused. This duty also encompassed things that weren't alive, such carts, cauldrons, wooden beams, wheels, boats, and other things like that. Before any sanctions can be given out, it must be proven beyond a reasonable doubt what the criminal did and why they did it. Back then, criminal law was easy to understand, and crimes were similarly easy to understand and not very bad. By the 13th century, though, major offenses were labeled felonies, and bot and wit were no longer enough to punish anyone who did wrong. This was the first item that set a tort apart from a crime. There was a connection between moral guilt and being legally responsible. This was a shift in how the law viewed the mind's role in liability. For a crime to happen, these two things must happen:

#### ***Cybercrime : Actus Reus***

"Actus" denotes "a mental or spiritual act." "The result of human behaviour that the law tries to stop" is what "actus reus" means. There are many distinct kinds of cybercrime. In simple words, it says that what a person does make a difference in the world. It has everything but the mental part. Not only does it mean an action, but it also denotes the way things are. B. Hogan and J.C. Smith thought of actus reus in cybercrime as the kind of suggestion of what people do that the law attempts to stop. It's not enough for someone to be guilty of a crime just because they want to do something wrong; they also have to do or not do something to finish the crime. It is challenging to prove actus reus in cybercrimes since the crimes happen in places that don't exist. There may be some evidence left behind on the machine itself, but it will be impossible to establish it in court because it has to be in a physical form or at least in a form that can be used as evidence. It's not hard to figure out what happened with cyber crimes, but it's quite hard to prove it. When someone uses a computer function, gets information from a computer's storage, or an electronic device that can access storage information from outside the computer, tries to get in digitally, or sends signals to multiple devices, they may have done something that is against the law. In situations of rape, the fact that the victim did not provide permission is a fundamental aspect of the "actus reus." If the prosecutor can't show that the defendant declined to agree, they won't be able to prove that the defendant did what they were accused of doing. In this instance, the unsuccessful trial will happen. This makes it apparent that we can state that Actus reus and mens rea are sometimes the same thing.

#### ***Cyber Crimes: Mens Rea***

The law today realizes that you can't conduct a crime without a mens rea. "Mens rea" is another key aspect of a crime, and it's sometimes called a "guilty mind." Over time, this way of thinking evolved steadily. Now, people who break the law consider that a guilty mind or something like it is always necessary.

Mens rea means "guilty mind." It signifies that the individual who perpetrated the offense did it on purpose. The act itself doesn't alter, but the state of mind that makes it illegal is what makes it reus. Almost all crimes need proof of some form of mental part. Some judges have said that most criminality is in the mind.

There are many distinct ways of thinking that make it up, like intention, recklessness, and not caring. The word "intention" describes a person's state of mind, which encompasses not only their capacity to guess what will happen in the future but also their desire to know what might happen as a result of their actions. As the phrase goes, you can't have an without being able to see the future. A man should know what will happen if he does something before he does it. If someone causes damage or harm without meaning to or by doing something that is not unexpected, they are not guilty of a crime under Common Law.

---

### **Child and Adolescents between 6-18 yrs**

Teenagers who breach the law online sometimes don't know that what they're doing is against the law. Most of the time, kids and teens act this way because they want to know everything and are interested. They also really want to learn things that are different. For these people, hacking into someone's computer or website is fun, an adventure, or both. Another possible defense could be to show their coworkers and peers that they are even brighter than they actually are. Children could also be tricked into looking for new websites through illegal disclosure, even if they don't know they're doing anything wrong. Young people are breaking the rules right now mostly because they want to learn new things and utilize the Internet to find things. Another reason would be to show that they are better than the other young people in their town.

---

### **CLASSIFICATION OF CYBERCRIME AGAINST CHILDREN**

The below mentioned are the crimes, that can be attached against the below mentioned group.

Cybercrime against Children and Teenagers:

- I. Cyber-stalking.
- II. Defamation
- III. Harassment via e-mails.
- IV. Email spoofing
- V. Indecent exposure
- VI. Cyber Pornography
- VII. Hacking
- VIII. Cyber Bullying

1. Cyber-stalking-The Oxford Dictionary says that stalking is "covertly pursuing." In simple terms, electronic stalking is when someone uses computers, email, the World Wide Web, or other electronic devices to harass or stalk someone in person. Talk to someone in a way that isn't good. Stalking, showing up at someone's house or place of business, making harassing phone calls, leaving things or messages that are written, or damaging someone's property are all examples of harassing or threatening behavior that a person does on a regular basis. Most of these crimes are against women because the main goal is to dominate the victim. People who have been abused at home are one of the most at-risk populations for traditional stalking.<sup>69</sup> It's not unexpected that they also get harassed online. It's not true that women will be fine if they "just leave." Cyberstalking is a way to keep tight control over a partner and make them afraid, even after they break up with you. The person who is being cyber-stalked is usually new to the internet and doesn't know much about netiquette or how to stay safe online. Their main targets are women, children, and other people who are emotionally weak or delicate. It is thought that more than 75% of the victims are women. There are four things that lead to internet stalking: sexual harassment, love fixation, revenge and hate, and ego.
2. Defamation- Cyber Defamation is when you accuse someone of something in order to hurt their reputation in the eyes of others who are right-minded, to make them avoid that person, or to make them feel disgusted. In the Indian judicial system, derision or mockery. Cyber defamation is just putting someone down online or on a computer. Online defamation is more dangerous than offline defamation, both in terms of numbers and quality. One click can send a defamatory message or comment to a lot of people, and it's easy to do so in a news group like the attorneys' group. Corporate cyber smear is the worst kind of internet defamation since it spreads false information about a company, its management, or its stock. In most situations, the criminal's thirst—whether it's for money, to satisfy his illegal or immoral desire, or to get back at someone for a conflict—is what drives him to send the victim defamatory emails. This needs to be made public. Section 4 of the Information Technology (IT) Act of 2000 and Section 499 of the India Penal Code (IPC), 1860 hide cyber defamation. Section 499 says that it is against the law to publish any false information about a person with the intent to harm that person's reputation or if the person knows or has cause to believe that the false information would do so.
3. Harassment via e-mails: Most of the time, email harassment is when one or more persons send a target a lot of unwanted, threatening, and frequently repeating electronic messages. How a communication should look or sound to be considered. There isn't always a clear standard for harassment. A lot depends on the situation because what one person thinks is rude or hurtful could not be seen that way by someone else. This form of harassment is often made worse by social media networks and connections. It usually comes from broken relationships, workplace gossip, or bullying at school. There are restrictions against email harassment, but sometimes they aren't very strict. People often send inappropriate emails to scare, intimidate, or otherwise offend the person who gets them. But what counts as "harassment" usually depends on how other people see it and respond to it. The things that are sent are sometimes quite personal to the person getting them, but they can also include harsh jokes or other biased or sexual information. Even if this kind of harassment happens a lot, it can happen because of just one message if it is sent with bad intent or has information that could hurt the victim.
4. Email spoofing- It is when someone sends an email from a false address. The word means email that comes from an address that isn't really the sender's. If you reply to that address, your mail may bounce back or go to someone else whose identification has been forged and has nothing to do with the person who sent it. Masked email is a distinct subject. It provides users a "masked" email address that isn't their real address and isn't shared (for example, so that it can't be mined), but it sends messages to the user's real address. Email protocols can't figure out where an email originates from by themselves. This makes it easy for spammers and other bad actors to modify the metadata of an email. So, the protocols will believe that the message came from the true sender. The original methods for sending email don't have any built-in ways to check who sent it. Because of this, "spoofing" can be used in "phishing" and "spam" emails to trick the person who gets them. Recent steps have made it tougher to spoof this way from the internet, but not impossible. Few internal networks can stop a fake email from a coworker's infected PC on that network. People and corporations who fall for fake emails can lose a lot of money. Spoof emails are regularly used to get ransomware onto computers, in particular.
5. Showing too much skin-When someone shows off parts of their body on purpose in a way that isn't regarded decent by local standards, this is called indecent exposure. These rules are different in each country. Religion, morality, and tradition often have an effect on these rules. They are fine as long as they are "needed to keep the peace." Indecent exposure is sometimes used to describe being naked in public or showing off without being sexual. Some people argue that showing or simply suggesting sexual conduct is indecent exposure. There may be times when this is clearly obscene. People frequently use this word to refer about a crime that is worse. distinct cultures have distinct opinions regarding what portions of the body should be exhibited in public. Not covering these portions could be considered as exposing yourself inappropriately. A picture. In a lot of Muslim nations, a lady who doesn't wear a veil could be considered as disrespectful. She might look like she has no shame. In a lot of places, it's disrespectful for women to reveal their breasts, but mothers can typically breastfeed their kids in public without getting in trouble.
6. Cyber Porn -Kids today, especially teens, are interested in everything and anything they may find online. Teens of days often use the internet and other electronic gadgets for schoolwork, and they also use the World Wide Web and the Internet and personal PCs at home. They are weak because they can use computers and the internet. Sometimes, kids want to know more about things that are really clear, like sex. Young people are focused on reaching their goals through the Internet and other means, and parents don't have much power over them. Sexual offenders take advantage of these situations to suit the requirements of the kids. The child doesn't know or appreciate how hazardous these encounters could be at this age. People who exploit children typically do so online. Cybercrime can happen to kids in India as more and more individuals there acquire access to the internet.
7. Hacking -When someone who isn't meant to be able to get into your computer system, that's hacking. Hackers, or persons who "hack," are basically just computer programmers who know a lot about computers and often use that expertise for undesirable reasons. They are ardent admirers of technology and usually know a lot about a specific piece of software or language. There could be a lot of causes, but most of them

are easy to comprehend and come from human tendencies like greed, wanting fame or power, and so on. Some people just want to show off how good they are with technology by doing things like modifying software (or even hardware) to perform things that the authors never meant for them to do. Some people just want to make things worse. A hacker might breach into a company's network to steal money, personal banking information, and other things out of greed or just to see what's going on.

8. Bullying online -Cyberbullying is when someone hurts another person using technology. Cell phones, chat apps, game apps, and social media sites are all at risk. It is a series of activities meant to scare, anger, or make the person who is being bullied feel bad. Two instances are posting false information about someone or posting embarrassing pictures or videos of them on social media. Sending rude, threatening, or abusive texts, pictures, or videos over chat apps. Sending rude messages to other people under a fake identity, either for that individual or for their fake account. Bullying happens a lot of the time both in person and online at the same time. But cyberbullying leaves a digital trail that can be used as proof that the abuse happened and to help stop it.

---

## LEGISLATIVE FRAMEWORK IN INDIA FOR CYBER CRIME AGAINST CHILDREN

"Until the great mass of the people shall be filled with the sense of responsibility for each other's welfare, social justice can never be attained." ~ Helen Keller

"Freedom is incomplete without social justice." ~ Atal Bihari Vajpayee

"Striving for social justice is the most valuable thing to do in life." ~ Albert Einstein

---

### History:

Baba Sahib Bhim Rao Ambedkar's ideas about social justice are what the Indian Constitution is based on. Social justice means giving everyone the same chance to develop their personality, which is related to equality and social rights. It is important for any country to have a social order based on fairness and to make sure that everyone has the same chances. They are regarded poorly since they are mostly illiterate and originate from poor parts of society. People are treated unfairly in society because of their size, colour, caste, religion, and race. This causes social unrest and inequality among them. Since of this, social justice is important since it is the only way to get people to take an active role in making society better and more inclusive. In a country like India that is so different, a fair social, economic, and political order is very important.<sup>2</sup>

Over time, we have seen big changes in legislation, rules, and how people recognize human and child rights. The common law ideas, which were unfair to the weak, have been replaced by a rights-based approach. The welfare of underprivileged groups, especially their kids, depended on how kind and kind the most powerful parts of society. The Indian Constitution, which entered into effect on January 26, 1950, protects the rights of kids. Article 21-A says that all kids between the ages of 6 and 14 have the right to a free (without charge) and required basic education (literacy). Article 24 (a) of the Indian Constitution says that people under the age of 14 are protected from any risky jobs. Also, kids enjoy the same rights as any other adult Indian citizen.

The "right to equality" (Article 14), the "right to personal freedom and due process of law" (Article 21), and the "right to protection from forced labour and human trafficking" (Article 23) are only a few examples of these rights. India's laws to protect children are based on constitutional protections for children's rights. The Union and State Governments in India have made more than 250 laws that affect children. In addition to these laws that protect children, there are also a number of criminal laws that do the same thing. The IPC of 1860, the Indian Evidence Act of 1872, and the Criminal Procedure Code of 1973<sup>3</sup> are some of these statutes.

The UNCRC says that child rights are the basic freedoms and chances that every person under 18 should have, no matter their race, nationality, wealth, origin, gender, opinions, language, religion, colour, birth status, or any other factor. These rights give kids more opportunities and help them be equal in society, in their families, and in their lives.

Important medical care and government help, as well as fun, social activities, and their incredible safety. The UNCRC's four broad categories cover all of a child's civil, political, social, economic, and cultural rights. Something amazing happened in 1989. As the international order changed, leaders from all across the world came together and made a historic commitment to the children of the world. The United Nations Convention on the Rights of the Child is a worldwide legal framework that promises to protect and fulfill the rights of every child. This treaty has a significant meaning: it says that kids are not just things that belong to their parents and for whom decisions are made, or adults in training. Instead, they are humans with their own rights. The Convention says that childhood is different from adulthood and lasts until the age of 18. It is a time when children must be allowed to grow, learn, play, develop, and prosper with dignity. The Convention has changed the lives of many children and is now the most widely accepted human rights agreement in history. The Convention has been ratified more times than any other human rights treaty. It has pushed governments to change laws and regulations and put money into programs that help more kids get the food and health care they need to live and grow, as well as better protections to keep them safe from abuse and exploitation. It has also given more kids a voice and a chance to be a part of their community. The Convention is not yet fully in place, and it is not commonly known or understood, even though significant improvements have been made.

---

### Child rights and Constitution of India

Article 15(3) of the Indian Constitution says that the government can make rules to safeguard women and children from abuse and stop them from working in jobs that are not appropriate for their age. The Constitution of India's Article 24 forbids hiring kids under the age of 14 in any business or mine. A new clause in the 42nd Amendment to the Indian Constitution protects minors. The State must make sure that kids have the chances and resources

<sup>2</sup> Sanjeev Kumar Bragta, Dr. Bhim Rao Ambedkar's views on social justice: an appraisal, 25 Technium Social Sciences Journal 583–589 (2021)

<sup>3</sup> Child Protection Laws in India The fans world

they need to grow up in a healthy way, with freedom and respect, and that kids and teens are protected from being used and abandoned morally and materially. The Indian Constitution says that children under the age of six should get early childhood care and education. As a parent or guardian, one of your most important duties as a citizen is to offer your child or ward between the ages of six and fourteen the chance to go to school. Article 14 of the Indian Constitution says that everyone is equal before the law. Article 21 guarantees children the right to life and personal freedom. Article 23 makes it illegal to traffic people, and Article 24 says that minors cannot work in mines, factories, or any other dangerous place. These rules make sure that people get enough food, have a good quality of life, and that public health improves.

### ***Indian Penal Code, 1860***

The Indian Penal Code (IPC) is meant to protect children's rights and punish anybody who break the law against them. Section 83 of these laws says that no act done by a juvenile between

Section 305 makes it a crime for someone under 18 to help someone else commit suicide, Section 317 makes it a crime for a parent or caregiver to leave a child, and Section 361 lays out the penalty for kidnapping a minor. The Indian criminal code of 1860 makes it illegal for minors to be prostitutes and gives them prison sentences of up to ten years. Section 293 of the IPC says that selling, publishing, or giving obscene material to minors is against the law. Defamation can get you up to two years in prison, a fine, or both. Any speech, gesture, or act meant to offend a woman's modesty is also against the law and can get you up to one year in prison or a fine. Section 507 says that people who use anonymous communication to threaten someone with violence can go to jail for up to two years.

### ***The Juvenile Justice Care and Protection for Children Act, 2000***

"This Act sets rules for minors who are in trouble with the law and need special care and protection." This law says that these kids have the right to care, protection, and treatment that is safe for them. It is certain that juvenile decisions are made based on their rehabilitation and what is best for them. The Probation of Offenders Act of 1958 This law is in line with the Juvenile Justice Act of 2000, which says that no one under 21 should be put in jail unless there are no other options. The Bonded Labor System (Abolition) Act of 1976: The main goal of this law is to end the indentured labour system that is common in India and hurts poor people, especially their children. Other legal frameworks that protect children's rights: Along with the legal frameworks already stated, there are also a number of other laws that have been passed to deal with specific child-related issues, such as: The Indian government passed this law in 1986 and put it into effect in 2000 to follow the rules of the 1992 agreement on the Rights of the Child, which India agreed to. It finds two groups of kids. Kids who need care and protection and teens who are in trouble with the law. The Juvenile Justice (Care and Protection of youngsters) Act of 2000 includes money for child care centers and rules for taking care of and rehabilitating youngsters. Chapter 2 of the law sets up a juvenile justice board to handle cases involving the legal system for kids. It also says that shelters for kids who break the law should be built. If a government worker finds out that a teenager has done something illegal, they have to take the teen to a special juvenile police unit. The unit will then tell the board right away about the minor.

### ***Government Policies About Keeping Kids Safe***

India is one of the few countries that has taken the lead and made a plan for kids. The Indian government has put in place a number of rules and regulations to help the country's physical, mental, and social growth. These kids have also been given different health and education plans. Some notable government policies that affect children are the National Policy for Children (1974), the National Policy on Education (1986), the National Policy on Child Labour (1987), and the National Health Policy (2002). India's legal system is made up of national and state laws, and different acts may define children in different ways. A child in India is someone who is less than 18 years old. The IT Act of 2000 has rules for dealing with cybercrimes, while the Protection of minors from Sexual Offenses Act (POCSO) of 2012 is an important statute that deals with sexual crimes against minors.

### ***The Immoral Traffic Prevention Act of 1956 (ITPA)***

The ITPA Act of 1956 defines prostitution and sexual exploitation or abuse for money. It punishes the sale, purchase, and use of anyone for prostitution. Crimes against people under the age of 16 face severe punishments. The immoral trafficking and preventive laws mostly deal with trafficking for prostitution. It says that a "Child" is somebody who is less than 18 years old. Section 5 of the Act says that anyone who gets a child for prostitution or encourages them to do so will go to imprisonment for at least seven years. This penalty can be raised to life in prison. People who operate trafficking rings are also responsible for what they do wrong. 139 The UNODC is training police officers to fight both cybercrime and human trafficking. The CBI, state police, and national police academy offer cyber law training to its officers in India on a regular basis. The 1986 law against showing women in an inappropriate way. (IRWA, 1986). The Indecent Representation of Women (Prohibition) Act of 1986 (IRWPA) makes it illegal to show women in an indecent way. The IRWPA says that doing indecent things and singing obscene songs is a criminal that can get you up to three months in jail.

### ***The IT Act of 2000***

The Indian Information Technology Act, 2000 is a law that controls things that happen online using mobile phones, computers, iPads, tablets, and other similar devices or gadgets. The Statute was passed in 2000, however the IT (Amendment) Act, 2008 made a lot of changes to it in 2008, making it clearer and broader in its scope and obligations. This meant that the definition of a computer network had to be changed to encompass any device that could

send, receive, or convey text, video, audio, or images. In 2008, a few more cybercrimes, like child pornography, were added to the changed law. These cybercrimes have something to do with the current issue.

### ***Sending or publishing obscene material***

Section 67A of the IT Act says that it is a felony to send or publish sexually explicit actions in electronic form, as well as to send or publish obscene digital information that includes sexually explicit acts. The layout of the segment is as follows: Anyone who publishes, sends, or causes to be published or sent electronically any content that is sexual in nature or appeals to the sexual interest, or whose effect is such that it tends to corrupt and deprave people who are apt to do so. Taking all relevant circumstances into account, to read, view, or hear the matter contained or embodied in it, shall be penalized on first conviction with imprisonment for a term not exceeding two years or a fine not exceeding ten thousand Rs. If you are convicted again, you must serve up to five years in prison and pay a fine of up to 10 Lacs.

### ***Sexual Exploitation and Child Pornography***

The IT (Amendment) Act, 2008, Section 67B makes child pornography, child exploitation, and child grooming illegal. If you publish or send electronic content that shows youngsters doing sexual things, Anyone who makes photos or text, gathers, searches for, downloads, advertises, promotes, or shares content that shows children in a sexual or obscene way can go to jail for up to five years and pay a fine of up to Rs. 10 Lacs. Additionally, anyone who entices children to perform explicit acts or in a manner that can offend a reasonable adult, or who facilitates the abuse of children online, or who records in electronic form the abuse or that of others relating to sexual explicit act with children is punishable on first conviction with imprisonment for a term of up to seven years. This category covers things like child pornography, sexual grooming, sexual predation, recording sexual acts on a webcam, and broadcasting sexual acts live on a webcam. If you publish or send out material that shows youngsters doing sexual things, you could go to jail for up to five years and pay a fine of up to 10 lacs rupees. This is only if the publishing is seen as being for the public benefit. For the purposes of this clause, everyone who is not yet 18 years old is a "child."

### ***Violation of Privacy***

Section 66E of the Information Technology Act, 2000 says that anyone can be punished for breaking privacy laws. If someone films, publishes, or sends pictures of a person's intimate area without their permission, whether on purpose or not. They might go to jail for up to seven years, pay a fine of up to two lakh rupees, or both. When someone has a good cause to think they can undress in private, that's what "circumstances violating privacy" means. If a child takes a picture of themselves or someone else with their permission and shares it online or through a mobile phone, it would still be against sections 67 (sending obscene content electronically), 67A (publishing or transmitting sexually explicit content), and 67B (child pornography).

### ***Computer-Related Crimes***

Section 66 of the IT Act, 2000 says that anyone who commits any of the crimes specified in section 43 in an unfair or dishonest way can go to jail for up to three years, pay a fine of up to Rs. 5 lakhs, or both. Section 67 says that anyone who publishes, sends, or causes to be published in electronic form anything that is sexually explicit, appeals to the prurient interest, or has the potential to corrupt and deprave people who are likely to read, see, or hear it will be punished with imprisonment of either descriptor or both descriptors.

### ***The Protection of Children from Sexual Offences Act, 2012***

The POCSO Act, which went into effect in 2012, protects people against sexual assault, sexual harassment, and child pornography. Sexual harassment is when someone with sexual intent says something, makes a sound, or does anything that a gesture, or showing an object or portion of the body with the goal of getting the kid to hear the word, hear the sound, see the gesture, or see the thing. Forcing a child to show any part of his or her body to another person is showing any pornographic material to children in any format or medium; following, observing, or otherwise regularly communicating with children; enticing a child for pornographic purposes or offering a reward for doing so; or threatening to use a real or fictional portrayal of any part of the child's body or the child's involvement in a sexual act. Sexual harassment is when someone shows a youngster anything sexual with the intention that it will be heard or seen by the child, make the child show his or her body, show a child an object in any way for pornographic purposes, follow or contact a child repeatedly in person, by phone, or by other means, or threaten to use real or imagined degrading or humiliating treatment against a child. It is against the law and can lead to up to jail for up to three years and a fine.

Child Porn Section 13 of the Act says that anyone who uses a child for sexual pleasure in any kind of media, including a TV show or ad, the internet, or any other electronic or printed form, whether for personal use or sharing, is guilty of child pornography. "Use a child" means getting a child involved in any form of media, such as print, electronic, computer, or any other technology, for the purpose of making, offering, sending, publishing, facilitating, or distributing pornographic materials. Section 14 of the IT Act says that using a child or minors for pornographic purposes can result in a fine and a jail sentence of up to five years. If you are convicted a second or third time, you might go to jail for up to seven years and pay a fine. If someone uses a child for pornographic purposes and breaks the laws in section 5 on purpose, they could go to jail for a long time and pay a fine. According to Section 14 of the IT Act, anyone who uses a child or minors for pornographic purposes can be fined and sent to jail for up to five years. If you are convicted a second time or more, you could go to jail for up to seven years and pay a fine. If someone acts in a pornographic way on purpose, they could face a long prison

sentence and a fine for breaking section 5's provisions. If they actively take part in pornographic actions that go against section 7's rules, they could also face fines and jail time of at least six years and up to eight years.

## JUDICIAL RESPONSE IN INDIA

Both the Indian constitution and its laws are written down. Its judicial system is the best in the world. The Indian government and courts are continuously trying to make things better for victims and make sure they get justice. This chapter talks about the steps the Indian judiciary has made to stop cybercrime against kids, as well as the role of the courts in this matter. Cybercrime is a problem that affects many countries. It has an effect on people all around the world. This kind of criminality is even worse because it doesn't have any borders. A person in India can be very easily targeted by someone in the USA and all it needs is a computer system and a decent internet connection. Cybercrime is a broad term that includes many different types of crimes that happen on the internet and using computers. There are many crimes that happen online, such as hacking, identity theft, phishing, scamming, ransomware, theft, and fraud. Because technology is changing so quickly, it's impossible to come up with a strict definition of cybercrime. The criminal is always changing as the internet changes, making it hard for governments and other groups to come up with a good definition. Simply described, cybercrime is any crime that happens online and involves computers, the internet, or computer systems.

It is a criminal to utilize a computer system or to go after someone online. The Internet has not only created a new type of crime, but it has also changed and expanded old ones like theft, fraud, and illegal gambling by making them available online. Some crimes have only moved from the real world to the non-physical and borderless online. But they still do the same bad things. So, we might say that cybercrime is a new type of crime, while regular crime is its genus.

Because it is the last authority on Indian law, the Indian Judiciary has been very important in the fight against cybercrime. The Supreme Court of India ruled in *State of Punjab and Others v. M/S Amritsar Beverages Ltd and others* said that computer-related crimes are hard for the courts and police to deal with. It is said that the court does not make new laws, but rather explains what the laws already say. The phrasing of a law determines its intent, and the main goal of legal interpretation is to figure out what the legislature really meant when it passed a law. The Indian court showed its technical side by saying that electronic media and distant conferencing can be used for meaningful consultation. Video conferencing is a new scientific and technological tool that lets you hear, see, and talk to someone far away as if they were right in front of you. The court gave electronic evidence a lot of weight in the cases of *Grid Corporation of Orissa Ltd. v. AES Corporation*, *State of Maharashtra v. Dr. Prathap B. Desai*, *Amitabh Bagchi vs. Ena Bagchi and Bodala*, *Murali Krishan vs. Bodala Prathima*, *Ponds India Ltd. vs. Commissioner of Trade Tax, Lucknow*, and *Mohammed Ajmal Mohammad Amir Kasab vs. State of Maharashtra*.

### *Cybercrimes that happen on computers*

In the case of *Kumar v. Whiteley*, it was thought that a hacker had broken into the Joint Academic Network (JANET) and deleted and added files and changed passwords to keep real users from getting on the network. The CBI started looking into Kumar after getting a report from the Press Information Bureau in Chennai about the illegal use of broadband Internet. The lawsuit says that Kumar's actions cost the subscribers a total of Rs 38,248. The Additional Chief Metropolitan Magistrate in Egmore, Chennai, sentenced Kumar to one year in prison and a fine of Rs 5,000 for cheating under Section 420 of the Indian Penal Code and Section 66 of the Information Technology Act. (Computer-related crime). On September 9, 2010, a scammer made a fake Facebook profile using the name of the Honorable President Pratibha Devi Patil. The Economic Offences Wing of the local police station got a complaint.

This team was in charge of looking into economic crimes, such computer crimes, and it got the complaint. Sending offensive messages through communication services and other means

*Shreya Singhal v. Union of India*<sup>4</sup> Because it violates the essential rights to free speech and expression that are protected by Section 66-A of the Information Technology Act, 2000 and Article 19(1)(a) of the Constitution are both illegal.

The IT (Intermediaries Guidelines) Regulations of 2011 say that content must be permanently removed without permission. The petition says that the actions of a government agency or court are unconstitutionally too broad. Section 230 was made to keep internet communications safe and stop the government from getting too involved.

Because it would let people utilize that power in an arbitrary and capricious way, which would be against Article 14 of the Constitution.

This court may declare Section 66-A to be unconstitutional since it introduces a new crime.

by making speech illegal for political reasons, which is against Indian law. This breaks Article 21 of the Indian Constitution: Section 66-A of the IT Act and Regulations 3(2) and 3 of the US Communications Decency Act, 1996. The US Supreme Court said that they are unconstitutional because they limit the First Amendment's promise of free expression. Section 66-A of the Constitution is bad for human rights and makes people afraid to speak their minds. People are saying that the Information Technology Act of 2000 is unlawful. Section says that

268 IPC, which is about nuisances, says that a person commits a public nuisance if they do things that "annoy the public" just to the extent to which they make it hard for them to enjoy their own property or any other public rights.

<sup>4</sup> AIR 2015 SC 1523: (2015) 5 SCC



The Honorable court said that any state law that doesn't follow the rules in Article 19(2) is not constitutional and therefore the whole section must be removed since it goes against Article 19(1)(a) of the Constitution because the idea of on free speech and expression is against the law. because it groups together minor and major crimes without drawing a difference between them. Section 80 violates Article 21 of the Constitution and goes against the protections in Section 41-A CrPC. Section 118(d) is about entries 31 and 93 of List I, the Kerala State Assembly couldn't put it into action. Because they are Entry 1 of List II of the Constitution covers the disputed Acts because they are meant to keep the peace.

The Seventh Schedule. Section 41-A plainly goes against Articles 14 and 21 because it doesn't protect against the exercise of the arrest authority like Sections 41 and 41-A of the Criminal Procedure Code (CrPC). It is also void and void because Articles 31 and 93 of List I deal with crimes (offenses) that happen through the media (means of communication), and The Kerala State Assembly did not have the power to pass the law. Article 19(1)(a) was taken into *Virendra v. State of Punjab* (1957 SCR 308) and *Bennett* both looked at print media in their decisions. *Coleman & Co. v. Union of India* (1972) 2 SCC 788. Most participants agreed that prior restraint censoring is not just desirable but also necessary.

### ***Stealing someone's identity***

The Indian court system is very important in the fight against cybercrimes that include stealing someone's identity. In *Sh. Vinod Kaushik and Others v. Ms. Madhika Joshi and Others*<sup>5</sup>, she sued her father-in-law and others for harassment over a dowry. She used their Gmail accounts to look at emails and chat session printouts as proof. Respondent No. 1 is the main party in this case. Dr. Ajay Bhushan Pandey heard the matter on August 9, 2010, and in the end, he turned down the application. The Cyber Appellate Tribunal made a decision on June 29, 2011, in response to an appeal from Complainant No. 1 (*Sh. Vinod Kaushik*) asking the adjudicating officer to look at the case again in light of the comments made in the judgment. The main issues in this case were whether or not *Sh. Neeraj Kaushik*, the second appellant, was representing the complainant's son, *Sh. Neeral Kaushik*, and whether or not Cognizant Technology Solutions Pvt Ltd. of Pune, the fourth respondent, had been appropriately charged.<sup>6</sup>

### ***Shreya Singhal vs. UOI***<sup>7</sup>

The Supreme Court of India threw out all of Section 66A of the Information Technology Act of 2000. The Petitioners said that Section 66A was unconstitutionally ambiguous and that its intended rights against annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, and ill will went too far beyond what Article 19(2) of the Indian Constitution allows. Article 19(2) of the Indian Constitution does not allow for limits on discomfort, danger, obstruction, insult, harm, criminal intimidation, or ill intent. The Court said that the rule against sending out information using a computer or phone with the goal of making someone angry, uncomfortable, or insulted did not fall within any exceptions to the right to free expression. The court also said that the section was too vague and broad because it didn't define words like "discomfort" or "irritation." This meant that "a very substantial quantity of protected and harmless expression" may be limited.

### ***Avnish Bajaj v. State (NCT) of Delhi***<sup>8</sup>

In the case of *Avnish Bajaj v. State*, Mr. Avnish Bajaj asked the Delhi High Court to throw out the summons order under Section 482. After the competent Court issued a summons order against the accused, The prosecution charged the then-Managing Director of Bazee, which was later bought by E-Bay, with breaking Section 292 of the Indian Penal Code (advertising/selling obscene objects) and Section 67 of the Information Technology Act (putting obscene objects on the internet). The court found that there was enough evidence to support a charge under Section 292 (2) (a) and 292 (2) (d) IPC against the website for the listing and the video clip, respectively. However, the Indian Penal Code does not recognize the idea of an automatic criminal liability attaching to the director when the company is an accused, so the petitioner can be acquitted under Sections 292 and 294 IPC.

### ***State of Tamil Nadu v. Suhas Katti***

The *Suhas Katti* case is the first in India to set a precedent for cyber-harassment." A woman sued the defendant for writing nasty things about her online. There were claims that a woman was being cyberstalked and harassed. The cybercrime section in Chennai finished the process of convicting the person after the case was filed in February 2004. The woman sued because someone sent her rude text messages. The case set a precedent for going after criminals who send rude texts that are dirty and profane and hurt the feelings of the person who gets them. It is particularly important because it is the first time that internet evidence has been allowed in court under section 65B of the Indian Evidence Act.<sup>9</sup>

<sup>5</sup> (2010) Cr. Comp 2, available at: <https://it.maharashtra.gov.in/Site/Upload/ACT/Madhika%20Vs%20KaushikRajesh%20Aggarwal.pdf>

<sup>6</sup> *Sh. Vinod Kaushik & Anr. v. Ms. Madhika Joshi & Others*, Cyber Appellate Tribunal, Judgment,

<sup>7</sup> AIR 2015 SC 1523

<sup>8</sup> (2008) 105 DRJ 721; (2008) 150 DLT 769

<sup>9</sup> C No. 4680 of 2004

## CONCLUSION AND RECOMMENDATIONS

In today's society, when technology is used, one of the most important things to talk about is how to teach kids about the internet and its effects. This study looked at how many Indian children use the internet a much and how many of them act inappropriately online. During the study, several elements related to the qualities were looked at in great detail, and the results were as mentioned earlier. The people who took part in the study were from diverse types of families, lived in different places, were different genders, ages, cultures, and so on. The investigation was aimed at school-age youngsters between the ages of 10 and 13 and 14 and 18. The survey looked at a lot of personal aspects that were important to the respondents. Even with all these problems, the study was done well and the results were found. The results show that most of the kids are utilizing the internet and cell phones. There are worries about how and when children use technology and how it affects their moral growth and ability to adapt. Some of the reasons why kids like the internet are that it makes it easy to find information, costs less, and lets them change their identity. Some of the reasons for cyber deviance among kids are low conviction rates, low rates of apprehension, a lot of money to be made, a lot of chances to do bad things, the ability to change their identity, the desire for instant gratification, an underdeveloped superego, a lack of supervision, a lack of technological knowledge, a lack of awareness, cyber addictions, a lot of deviant content, and the internet's role in teaching deviance.

The teacher who talks to students about security doesn't know enough about cyber awareness issues, especially when it comes to security. Teachers need to get training in technology so they can learn new skills and stay up to date. Hacktivists are a new type of cybercriminal that is on the rise. The existing record shows at least knowledge of cyber crimes at every level in India. Courses in several areas need to be offered right now.

The Department of National Security says that cyber security is "preventing, detecting, and responding to attacks." As more and more Indian people utilize social media and mobile devices, the Indian education system needs to teach students about cyber security.

India's cyber law framework is believed to be enough for now, but it may be better in several aspects. Especially, the cybersecurity rules of some sector regulators need to be revised so that they can keep up with the fast-paced changes in technology. Indian officials are aware of this requirement and are creating new policy frameworks to support these developments. It is believed that the parts of this new policy framework are strong enough to handle the problems that come with these new developments. That being stated, the effectiveness of these programs depends on the government putting them into action carefully and without corruption. As past events show, India is one of the places where cybercriminals are most likely to strike.

## Suggestions

In this time of globalization and liberalization, we need to realize that cybercrime is a very new phenomena that has consequences on politics, society, and the economy all around the world. The internet lets people from all over the world talk to each other gives organized criminals a way to talk to each other and their own groups in complicated ways. This lets them pay for and set up networks for a wide range of cybercrimes, such as drug trafficking, pornography, and the illegal trading of firearms.

There are three main ways to stop these crimes: cyber law, education, and creating rules. All of the above methods for fighting cybercrime work very well or a lot. Because of the lack of effort, the rules about how to handle cyberattacks need to be changed or enhanced.

**The Information Technology Act, 2000 needs to be more complete and useful in today's society**-The preamble to the "Information Technology Act of 2000, as amended by the Amendment Act of 2008," says that the law's purpose was to make transactions done through electronic data interchange and other forms of e-commerce legally valid. The Act has also changed the "Indian Penal Code of 1860," the "Indian Evidence Act of 1872," the "Bankers Book of Evidence Act of 1891," and the "Reserve Bank of India Act of 1934" to make it easier for them to be recognized by the law. The goal of this law is to name certain crimes and set consequences for them, not to stop people from committing crimes. Cybercrime is still a problem, and it has been shown that this law works better in principle than in practice. This is because the language it uses is exceedingly complex and hard for judges, prosecutors, police, and lawyers to understand. There are numerous right things that need to be done to make "the Information Technology Act" more valuable.

**Need for Clear and Settled International Law on Jurisdiction** -There needs to be a lot more clarity on two parts of cyber law: the correct and complete definition of cybercrime and the correct laws about who has jurisdiction at both the national and international levels. There aren't any in India. There aren't many cyber law cases, and there aren't any big rules on the books either. Most of the time, policymakers and judges that deal with cybercrime have to use the laws and cases that are already in place. The Information Technology Act of 2000 doesn't make it obvious what to do when hackers use fake names to keep information on other people's computers, websites, and personal email accounts. We need to talk about this and come to a solution because hacker cultures and methods are very much the same all over the world, including Russia, the United States, the United Kingdom, Canada, Australia, India, and other countries. The problem of cyberspace impacts everyone in the world. We need to have one set of guidelines about who can try a case because of this. Just having a link to one country might not be enough, since there could be links to more than one. Professional hackers (black hat hackers) broke into the company's systems and websites or The Cyber Crime Investigative Cell or other groups will require the aid of the people who did the crime if they wish to stop it from happening again. Countries need to cooperate together on a global basis to stop and control cyber hacking.

## We need to ratify and revise the Cyber Crime Convention

The Information Technology Act of 2000 also includes any crime or violation that happens outside of India, no matter where the person is from, as long as the illegal action or breach takes place in India. If a foreigner breaks the law in a way that is punishable by the IT Act of 2000, the government of that nation will have to aid with the investigation, search, seizure, arrest, prosecution, and extradition of cybercriminals. India can't do this because it hasn't signed the "Cyber Crime Convention," which was open for signatures in "Budapest" on November 23, 2001. This means that we can't work together on

cybercrime issues. The convention on cybercrime has made it possible to extradite people who commit cybercrimes. It could also discuss about how to send someone back to their own country. There aren't many cyber laws governing jurisdiction, and the extradition treaty hasn't been ratified yet, so it's still unclear who has the power to rule in cyberspace. People need to sign the cybercrime convention.

#### **We must follow the advice of the Governing Council on Digital Technologies**

On December 2, 2014, the Standing Committee on Information Technology published its "52nd report" on "Cyber Crime, Cyber Security, and The Right to Privacy." The description claimed that India's cyber security environment needs to be altered right away, and that the country also needs long-awaited privacy laws. The committee also noted that the "Information Technology Act" (IT) 2000 and "Indian policies" and practices don't do enough to protect people's privacy when it comes to government initiatives, dealing with complex data, and virtual substances. The agency also indicated that Section 43A of the IT (Information Technology) Law needs to be enforced at the level of organizations. The committee also says that the 2013 "National Security Policy" (NSP) has some aspects that could help establish a legislative framework that fills in any gaps that may arise. "The committee also concluded that the IT Act needs to be looked at again every so often because it doesn't do enough to protect against cybercrime and cyber security. This is especially significant because of the recent debate over section 66A of the IT Act. The Centre for Cyberspace and Civilization has also pointed out that we need to remember how vital working together with other countries is for fighting cybercrime and keeping the notion of dual wrongdoing in mind.

#### **The United Nations General Assembly's proposal must be put into action right away**

It is also suggested that the "United States and the United Kingdom" follow the "United Nations General Assembly's" advice and pass their own laws to fight cybercrime. To avoid The United Nations system should help create global ways to fight cybercrime and ways for countries to work together to do so. Also, all governments should be pushed to quickly change their criminal laws to deal with the unique problems that come with cybercrime. People are calling for either the development of completely new criminal laws or the revision or clarification of current ones because criminals are using new technology to perpetrate old crimes. The governments should pass laws that are as broad as the Council of Europe Convention on Cybercrime.

#### **There needs to be a modification to "The Indian Telegraph Act of 1885**

"The Information Technology Act of 2000" does not expressly deal with stealing internet time. Section 378 and Section 379 of the Indian Telegraph Act, 1885, which describe theft and its punishment, are still the same.

The Indian Telegraph Act of 1885 gave the government and any company or person with a license under Section 4 of the Indian Telegraph Act of 1876 the right to put up telegraph lines on or beneath private or public property. The Indian Penal Code of 1860, the Indian Evidence Act of 1872, the Bankers Book of Evidence Act of 1891, and the Reserve Bank of India Act of 1934 are the only laws that the IT Act of 2000 changed." The Indian Telegraph Act" is not one of them. The Indian Telegraph Act has to be updated so that it makes more sense in today's society.

#### **The rules against crime need to be updated so that they are clear and explicit and don't rely on hazy meanings**

Cyberspace has been increasing since the 1990s, and it's having a terrible effect on civilizations quickly. The criminal laws need to be as precise and specific as feasible in order to set moral norms in cyberspace. They can't be founded on ambiguous readings of the rules that are already in place, and those who break them need to be penalized for what they do. This has to happen on a national and global level.

#### **There needs to be a working partnership between government agencies and private firms.**

Cybercrime is a complicated issue that keeps getting worse. The police and the businesses won't be able to deal with this situation on their own. Businesses and law enforcement need to work together to stop cyber attacks and find hackers, and stop them. This partnership would build on the Government's Cyber Security Information Sharing Collaboration and other sector-based information sharing forums. It would also go further in encouraging people to report cybercrimes, as the National Crime Agency (NCA) has suggested.

An "announcement in the Official Gazette shall specify the effective date of The Children's Online Privacy and Protection Act of 2022." It is a criminal to hack into a network or processor system. Any illegal behaviour that employs an electronic device is considered online crime. The government makes sure that all Indians are safe from illegal conduct.

Indians can use the internet for free, safely, and with accountability. Sex education teaches about things like the anatomy of the human body, sexual activity, sexual reproduction, the legal age of consent, reproductive health, reproductive rights, sexual health, and safe sex. There are many ways to get information about kids. These include asking, begging, or pushing them to share it online and letting them make personal information public. The Internet, as defined in the proposed act, is a network of computers and communication tools that send data. You can't use content that is bad for kids. This guideline says that you can't use texts that aren't appropriate for kids, don't have any literary, aesthetic, political, or scientific value, or feature real or fake sexual actions. When it comes to cyberbullying, this is utilizing technology to bully someone, such as spreading false rumors about them or posting embarrassing pictures of them on social media. "When cyberbullying threatens to kill or seriously hurt someone, or to commit a crime that could lead to death or life in prison, or both, cyberbullying can be punished with up to two years in prison, a fine, or both." Cyber grooming is when someone befriends a young person online so they can mistreat, exploit, or traffic them for sex. Kids should know how to deal with harassment from other players and the risks of playing video games online. Section 2078 of the Computer Act says that it is illegal to employ children in pornographic media for commercial purposes. This includes sharing video, image, or audio recordings online using a computer, smartphone, or tablet device. Section 9 of the Act says that a kid cannot be "used for pornographic purposes," and anyone who is found with pornographic materials that show minors can be fined up to three years in prison or both. According to "Section 10 of the Privacy Act," violating someone's privacy can result in up to three years in prison, a fine of up to two lakh rupees,

or both. A cyber-stalker is someone, a group, or an organization that uses the Internet or other technology to stalk and bother someone else. This is a sort of cybercrime in which someone breaks into a computer system or device without permission with the goal of stealing, copying, changing, or destroying data or damaging the system by getting access without permission. "Section 13 Identity Theft carries a maximum penalty of three years in prison and a fine of one lakh rupees. Section 14 of the United Nations Convention on the Rights of the Child talks against recruiting, moving, transferring, hiding, or receiving a child for exploitation. People who encourage or help a youngster to become a prostitute will face a strict prison sentence of three to seven years if they are proven guilty of this crime. If someone is found guilty of "procuring" a juvenile girl under 18 to have sex with someone else, they could go to jail and pay a fine. As part of the notification required by Section 15 - Interactive Computer Service Obligations, service providers must tell customers that parental control protections are available for purchase and may assist them keep children from accessing hazardous content. The Commission on Online Child Protection did a research as part of Section 16 of the Online Child Protection Act to assist keep kids from seeing dangerous content online. There will be 19 people on the Commission: two from the sector, two from domain name registration, two from academic technology professionals, and four from the company that makes online content.

The Commission will think about a number of things when choosing how to limit kids' access to harmful information. These include the expense of these technologies and approaches, how they affect law enforcement, and how they affect privacy.

These are only a handful of the things it will think about when it makes its choice. The Commission shall show the Board the results of the study that this section talks about, including the conclusions and recommendations for each method or technology. Depending on the demands of each district or area, the government may set up one or more Privacy and Protection Boards for the areas or groups of districts indicated in the announcement. The goal of these groups is to make sure that kids' safety and privacy online are maintained.