### **Cyber Crimes During the Coronavirus Pandemic in India**

#### **Overview of Cyber Crimes During the Pandemic**

The coronavirus pandemic brought about a significant increase in cyber crimes in India, especially as more people, including women and children, spent time online due to lockdowns and restrictions. Cybercriminals took advantage of the situation, using the fear and uncertainty around the virus to launch various types of attacks.

#### **Increase in Cyber Crime Rates**

* **Targeting Women and Children:** With schools and workplaces moving online, women and children became prime targets for cybercriminals. There was a sharp rise in cases of online harassment, cyberbullying, and exploitation. Children were particularly vulnerable as they spent more time on the internet, often unsupervised.
* **Types of Attacks:** Common cyber crimes included phishing scams where criminals pretended to offer information about COVID-19 or vaccines, leading people to malicious websites. Additionally, there was an increase in the spread of "coronavirus malware" – malicious software disguised as COVID-19-related information that could steal personal data or install spyware on devices.

#### **How These Crimes Were Reduced**

* **Government and Police Action:** The Indian government and cybercrime units took several measures to combat the rising threat. Awareness campaigns were launched to educate the public about the risks of sharing personal information online and how to recognize phishing scams.
* **Reporting Platforms:** The Indian government also strengthened its online reporting platforms, making it easier for victims to report cyber crimes. This included a special focus on crimes against women and children, with dedicated helplines and support systems.
* **International Cooperation:** Since many cyber criminals operated from different countries, Indian authorities worked closely with international law enforcement agencies to track down and arrest these criminals.

#### **How Criminals Were Caught**

* **Tracking the Criminals:** Law enforcement agencies used advanced technologies to track down the sources of these cyber attacks. This often involved tracing IP addresses, analyzing malware patterns, and working with social media platforms to identify and shut down fake accounts.
* **Countries Involved:** Many of the cybercriminals were found to be operating from countries with a high level of cybercrime activities. These included some Eastern European countries, where organized cybercrime groups are known to operate, as well as individuals in countries like China and Nigeria.

#### **UNICEF's 2021 Report on Online Exploitation**

The United Nations Children's Fund (UNICEF), originally known as the United Nations International Children's Emergency Fund, was created by the United Nations General Assembly on 11 December 1946, to provide emergency food and healthcare to children and mothers in countries that had been devastated by World War II.

* **UNICEF's Findings:** In 2021, UNICEF released a report that highlighted a worrying increase in online exploitation during the pandemic. The report pointed out that a significant number of children had become victims of predators who exploited the increased online activity during lockdowns.
* **Key Points:** The report emphasized the need for stronger online protections for children and called for global cooperation to combat the rise in online child exploitation. It also highlighted the importance of educating children and parents about online safety to prevent such exploitation.

### **Summary**

During the COVID-19 pandemic, cybercrime rates in India increased, with a notable rise in crimes targeting women and children. However, through government action, public awareness campaigns, and international cooperation, many of these crimes were reduced, and several criminals were caught. The UNICEF 2021 report further underlined the dangers children faced online during the pandemic, emphasizing the need for continued vigilance and protection.

##### 

**detailed explanation on how exactly they were attacking and what they were doing by these attacks**

### **Detailed Explanation of Cyber Attacks During the COVID-19 Pandemic**

#### **1. Phishing Scams**

Phishing was one of the most common forms of attack during the pandemic. Cybercriminals would send emails or messages pretending to be from legitimate organizations, such as the World Health Organization (WHO) or local health authorities. These messages often contained urgent information about COVID-19, like updates on vaccines, lockdown measures, or health guidelines.

* **How They Worked:**
  + **Fake Websites:** The messages typically included links to websites that appeared legitimate but were actually designed to steal personal information. When users entered their details, such as usernames, passwords, or bank information, the data would be captured by the attackers.
  + **Malware Delivery:** In some cases, the emails contained attachments that, when opened, would install malware on the victim's device. This malware could then be used to spy on the victim, steal data, or gain control of their device.
* **Purpose of the Attack:**
  + **Data Theft:** The primary goal was to steal sensitive information that could be sold on the dark web or used for further attacks.
  + **Financial Gain:** Attackers often targeted financial information, leading to unauthorized transactions or identity theft.

#### **2. "Coronavirus Malware"**

This was a term used to describe various types of malware that were spread under the guise of COVID-19-related information.

* **How They Worked:**
  + **Fake Apps and Software:** Cybercriminals created fake apps that claimed to provide updates on the spread of the virus, or tools to help with remote work. Once installed, these apps would infect the device with malware.
  + **Infected Files:** Documents claiming to provide vital COVID-19 information were circulated, especially in emails. When opened, these documents would trigger the installation of malware.
* **Purpose of the Attack:**
  + **Spying:** Some malware allowed attackers to monitor the victim’s activities, capturing keystrokes, taking screenshots, and even recording video or audio from the device.
  + **Ransom:** In some cases, ransomware was used to lock the victim’s files or system, with the attackers demanding payment to restore access.

#### **3. Online Harassment and Exploitation**

As more people, especially women and children, spent time online during the pandemic, there was a significant increase in cases of online harassment and exploitation.

* **How They Worked:**
  + **Cyberbullying:** Children and teenagers were particularly vulnerable to cyberbullying on social media platforms. Bullies would use threats, insults, and even blackmail to torment their victims.
  + **Exploitation:** Predators used social media, chat rooms, and gaming platforms to exploit children. They would often pretend to be someone the child could trust and gradually manipulate them into sharing personal information or inappropriate content.
* **Purpose of the Attack:**
  + **Power and Control:** For cyberbullies, the goal was often to assert power over their victims, leading to emotional and psychological harm.
  + **Sexual Exploitation:** Predators aimed to exploit children for sexual purposes, sometimes leading to cases of child pornography or human trafficking.

#### **4. Fake Charities and Fundraisers**

Cybercriminals exploited the goodwill of people who wanted to help those affected by the pandemic.

* **How They Worked:**
  + **Fake Charity Websites:** Fraudulent websites were set up to look like legitimate charities. These sites would solicit donations, but the money would go directly to the criminals.
  + **Crowdfunding Scams:** Attackers also used crowdfunding platforms to create fake campaigns, claiming to raise money for COVID-19 relief efforts. Once they collected enough donations, they would disappear.
* **Purpose of the Attack:**
  + **Financial Gain:** The primary goal was to steal money from people who thought they were donating to a good cause.

#### **5. Targeting Remote Workers**

With the sudden shift to remote work, many employees were using personal devices and unsecured networks, making them easy targets for cybercriminals.

* **How They Worked:**
  + **Brute Force Attacks:** Cybercriminals used brute force attacks to guess the passwords of remote work platforms like Zoom or Microsoft Teams. Once inside, they could disrupt meetings or steal sensitive company information.
  + **Credential Stuffing:** If an employee’s password from another account had been leaked, attackers would use that password to try to access work accounts, a technique known as credential stuffing.
* **Purpose of the Attack:**
  + **Corporate Espionage:** The attackers could steal intellectual property or sensitive business information to sell to competitors.
  + **Disruption:** Some attacks were intended to disrupt business operations, causing financial losses and damaging reputations.

#### **How These Attacks Were Carried Out**

Cybercriminals used a variety of methods to carry out these attacks, often taking advantage of people’s fear, uncertainty, and the increased online presence during the pandemic. They operated from different parts of the world, making it difficult for authorities to track them down. The anonymity provided by the internet, combined with the lack of cybersecurity awareness among many users, made it easy for these criminals to succeed in their attacks.

#### **How the Criminals Were Caught**

* **Collaboration Across Borders:** Law enforcement agencies from different countries collaborated to track down the criminals. They used advanced tools to trace the origin of attacks, analyze malware patterns, and follow the money trail from the scams.
* **Cyber Forensics:** Investigators used cyber forensics to gather evidence from devices, track down IP addresses, and decrypt communications used by the criminals.
* **Public Cooperation:** Awareness campaigns encouraged victims to report cyber crimes, providing valuable information that helped in catching the perpetrators.

#### **2021 UNICEF Report Summary**

The UNICEF report from 2021 highlighted a sharp increase in online exploitation of children during the pandemic. As children spent more time online, often unsupervised, they became easy targets for predators. The report called for stronger protections and international cooperation to address this growing issue, emphasizing the need for better education and awareness to protect vulnerable groups online.

### **Challenges in Prosecuting Cyber Crimes in India**

Prosecuting cyber crimes in India comes with a unique set of challenges. These challenges arise due to the nature of cyber crimes, the rapid evolution of technology, and the complexities of the legal system. Here's a detailed look at the key issues:

#### **1. Jurisdictional Issues**

* **Nature of the Problem:** Cyber crimes often cross state and national borders. For example, a hacker in one country can attack a system in another, making it difficult to determine which country's laws apply.
* **Why It’s a Challenge:** Indian law enforcement agencies may struggle to investigate crimes that involve multiple jurisdictions. International cooperation is required to trace criminals, gather evidence, and prosecute them, which can be time-consuming and complicated.
* **Example:** If an Indian company is hacked by someone in another country, Indian authorities need to work with foreign governments to track down the perpetrator, which can be difficult due to differing legal systems and priorities.

#### **2. Lack of Awareness and Training**

* **Nature of the Problem:** Many law enforcement officials, prosecutors, and even judges may not have specialized knowledge about cyber crimes and digital evidence.
* **Why It’s a Challenge:** Without proper training, it can be hard to understand the technical details of cyber crimes, which may lead to delays in investigations, weak cases, and even wrongful acquittals.
* **Example:** In some cases, law enforcement officers may not know how to properly collect digital evidence from computers or mobile devices, leading to issues in court where the evidence is challenged by defense attorneys.

#### **3. Rapidly Evolving Technology**

* **Nature of the Problem:** Technology changes at a rapid pace, with new methods of committing cyber crimes emerging all the time. Law enforcement and legal frameworks often lag behind.
* **Why It’s a Challenge:** The legal system may not be equipped to handle new types of cyber crimes, such as those involving cryptocurrencies, AI, or sophisticated malware, because existing laws may not cover these areas adequately.
* **Example:** Crimes involving cryptocurrencies like Bitcoin can be difficult to trace and prosecute because the technology is relatively new and regulations are still being developed.

#### **4. Digital Evidence Collection**

* **Nature of the Problem:** Digital evidence, such as emails, logs, and data from devices, is crucial in prosecuting cyber crimes, but collecting and preserving this evidence can be tricky.
* **Why It’s a Challenge:** Digital evidence is easily altered, deleted, or corrupted, making it difficult to use in court. Additionally, there are strict legal procedures for handling such evidence, and any mistake can render it inadmissible.
* **Example:** If an investigator fails to follow the proper protocol when seizing a suspect's computer, the defense could argue that the evidence was tampered with, leading to its dismissal.

#### **5. Privacy Concerns and Encryption**

* **Nature of the Problem:** Many cyber crimes involve encrypted data, which is difficult to access without violating privacy rights.
* **Why It’s a Challenge:** Balancing the need to investigate crimes with the protection of individuals' privacy rights can be difficult. Decrypting data without the proper legal authorization can lead to accusations of privacy infringement.
* **Example:** In cases where suspects use encrypted messaging apps to plan crimes, law enforcement may need court orders to access communications, but even then, breaking encryption can be legally and technically challenging.

#### **6. Underreporting of Cyber Crimes**

* **Nature of the Problem:** Many cyber crimes go unreported due to the stigma attached, fear of reputation damage, or lack of awareness about how to report such crimes.
* **Why It’s a Challenge:** If victims don't report cyber crimes, law enforcement cannot investigate, and the criminals remain free to commit more crimes. Underreporting also leads to a lack of reliable data on the prevalence of cyber crimes, making it harder to allocate resources effectively.
* **Example:** A small business that suffers a data breach might choose not to report it to avoid damaging its reputation, allowing the criminals to go undetected and possibly target other businesses.

#### **7. Overloaded Judicial System**

* **Nature of the Problem:** The Indian judicial system is already burdened with a large number of cases, and cyber crime cases add to this load.
* **Why It’s a Challenge:** Cyber crime cases are often complex and require specialized knowledge, leading to longer trials and delays in delivering justice. This can frustrate victims and make it harder to deter future crimes.
* **Example:** A case involving a complex online fraud might take years to resolve due to the need for technical expertise and the backlog of cases in the courts.

### **Conclusion**

Prosecuting cyber crimes in India involves overcoming significant challenges, from jurisdictional issues to the need for specialized knowledge. Addressing these challenges requires better training for law enforcement, updated laws that keep pace with technology, international cooperation, and increased awareness among the public about cyber crimes. By tackling these issues, India can strengthen its ability to combat cyber crime and protect its citizens from digital threats.

**Prevention Strategies for Individuals in India**

To protect yourself from cyber crimes in India, it's important to follow certain strategies and be aware of common threats. Here’s how you can stay safe:

### **1. Education and Awareness**

* **Stay Informed**: Keep yourself updated about the latest types of cyber crimes and how they occur. Knowledge is your first line of defense.
* **Cyber Safety Education**: Learn about safe online practices. Schools and organizations often provide programs on internet safety, which can be very helpful.

### **2. Strong Passwords**

* **Use Complex Passwords**: Create strong passwords that are a mix of letters, numbers, and symbols. Avoid using easy-to-guess passwords like "password123" or your birthdate.
* **Change Passwords Regularly**: Update your passwords frequently and don’t use the same password for multiple accounts.

### **3. Two-Factor Authentication (2FA)**

* **Enable 2FA**: This adds an extra layer of security. Even if someone gets your password, they would need a second form of verification, like a code sent to your phone, to access your account.

### **4. Privacy Settings**

* **Control Your Information**: On social media and other platforms, adjust your privacy settings to control who can see your information. Limit the amount of personal data you share online.
* **Be Cautious About Sharing**: Think twice before sharing personal information online. Scammers can use this information to target you.

### **5. Secure Your Devices**

* **Use Antivirus Software**: Install reputable antivirus software to protect your devices from malware and viruses. Keep it updated.
* **Update Regularly**: Make sure your operating system, apps, and security software are always up to date. Updates often include patches for security vulnerabilities.

### **6. Safe Internet Practices**

* **Avoid Suspicious Links**: Don’t click on links or download attachments from unknown or suspicious emails and messages. These could be phishing attempts or contain malware.
* **Use Secure Connections**: When shopping online or accessing sensitive accounts, ensure the website is secure (look for “https” in the URL).

### **7. Be Careful with Public Wi-Fi**

* **Avoid Public Wi-Fi for Sensitive Transactions**: Public Wi-Fi networks are often not secure. Avoid using them for banking or any transaction that requires entering sensitive information.
* **Use a VPN**: If you must use public Wi-Fi, consider using a Virtual Private Network (VPN) to encrypt your data.

### **8. Report Cyber Crimes**

* **Know Where to Report**: Be aware of how to report cyber crimes. In India, you can report incidents to the Cyber Crime Cell or use the National Cyber Crime Reporting Portal (<https://cybercrime.gov.in/>).
* **Act Quickly**: If you suspect you’ve been a victim of a cyber crime, report it immediately. Quick action can help prevent further harm and assist in catching the criminals.

### **9. Financial Safety**

* **Monitor Your Accounts**: Regularly check your bank statements and credit reports for any suspicious activity.
* **Use Secure Payment Methods**: When shopping online, use secure payment methods like credit cards, which offer more protection against fraud.

### **10. Educate Family Members**

* **Teach Safe Practices**: Make sure your family members, especially children, understand these safety practices. Children are often more vulnerable to cyber crimes, so educating them is crucial.

By following these strategies, individuals in India can significantly reduce the risk of falling victim to cyber crimes. Staying vigilant and proactive is key to maintaining your online safety.

### **NGOs in India Fighting Cyber Crimes**

1. **Cyber Peace Foundation**
   * **Focus**: Cybersecurity, education, and assistance to victims of cybercrimes.
   * **Website**: [cyberpeace.org](https://www.cyberpeace.org)
2. **Cyber Crime Awareness Society**
   * **Focus**: Educating people about cybercrime, legal assistance, and advocacy.
   * **Website**: [cybercrimeawareness.org](http://www.cybercrimeawareness.org/)
3. **Rakshit Tandon's Cyber Security Awareness Initiatives**
   * **Focus**: Educating people about cyber threats and safety, offering training programs.
   * **Website**: [cybergyan.in](http://www.cybergyan.in/)
4. **Childline India Foundation**
   * **Focus**: Helping children in distress, including those affected by cyber crimes.
   * **Helpline Number**: 1098 (Toll-Free)
   * **Website**: [childlineindia.org.in](https://www.childlineindia.org/)
5. **End Now Foundation**
   * **Focus**: Preventing cyberbullying, online harassment, and promoting digital wellness.
   * **Website**: [endnowfoundation.org](https://endnowfoundation.org)
6. **CRY – Child Rights and You**
   * **Focus**: Protecting child rights, including safeguarding them from online exploitation.
   * **Website**: [cry.org](https://www.cry.org)

### **Helpline Numbers and Websites to Report Cyber Crimes in India**

1. **National Cyber Crime Reporting Portal**
   * **Website**: [cybercrime.gov.in](https://www.cybercrime.gov.in/)
   * **Purpose**: A centralized platform to report cybercrimes, especially against women and children.
2. **Cyber Crime Helpline Number**
   * **Helpline Number**: 1930 (formerly 155260)
   * **Purpose**: To report financial frauds and other cybercrimes.
3. **Indian Computer Emergency Response Team (CERT-In)**
   * **Website**: [cert-in.org.in](https://www.cert-in.org.in/)
   * **Purpose**: National nodal agency to respond to cybersecurity incidents.
4. **Ministry of Home Affairs (MHA) Cyber Crime Division**
   * **Website**: [mha.gov.in](https://www.mha.gov.in)
   * **Purpose**: Policies and resources related to cybercrime in India.
5. **National Commission for Women (NCW) – Online Complaint Registration**
   * **Website**: ncw.nic.in
   * **Purpose**: Specifically for women to report cyber harassment and other crimes.
6. **Cyber Crime Cells in Various States**
   * **Purpose**: Every state in India has its cyber crime cell where victims can report incidents. You can find contact details on state police websites.
7. **Aarambh India Initiative**
   * **Focus**: Child protection online, including cyberbullying and exploitation.
   * **Website**: [aarambhindia.org](http://www.aarambhindia.org)

### **History of NGOs and Reporting Systems for Cyber Crimes in India**

#### **1. Cyber Peace Foundation**

* **History**: Founded in 2013, Cyber Peace Foundation aims to address cyber threats through education, awareness, and response. They provide training and resources to help people protect themselves from cyber crimes.
* **Mission**: To create a safer digital space through peace-building efforts and by raising awareness about cyber security.
* **Website**: [cyberpeace.org](https://www.cyberpeace.org)

#### **2. Cyber Crime Awareness Society**

* **History**: Established to tackle the increasing threat of cyber crimes, this NGO focuses on educating the public about online safety and legal measures.
* **Mission**: To promote cyber crime awareness and help victims navigate the legal system.
* **Website**: [cybercrimeawareness.org](http://www.cybercrimeawareness.org/)

#### **3. Rakshit Tandon's Cyber Security Awareness Initiatives**

* **History**: Rakshit Tandon is a renowned cyber security expert who has been working on raising awareness about online threats since the early 2000s. His initiatives provide education and practical advice on staying safe online.
* **Mission**: To educate individuals and organizations about cyber threats and safety practices.
* **Website**: [cybergyan.in](http://www.cybergyan.in/)

#### **4. Childline India Foundation**

* **History**: Established in 1998, Childline India Foundation provides emergency support to children in distress. They expanded their services to include protection from online exploitation.
* **Mission**: To ensure that no child is left without support, including protection from cyber threats.
* **Helpline Number**: 1098 (Toll-Free)
* **Website**: [childlineindia.org.in](https://www.childlineindia.org/)

#### **5. End Now Foundation**

* **History**: Founded to combat online harassment and promote digital wellness. They focus on providing resources and support for those affected by cyberbullying.
* **Mission**: To prevent and address issues related to online harassment and ensure a safer digital environment.
* **Website**: [endnowfoundation.org](https://endnowfoundation.org)

#### **6. CRY – Child Rights and You**

* **History**: Established in 1979, CRY works on various child rights issues, including protection from online exploitation. They focus on ensuring children's rights are upheld both offline and online.
* **Mission**: To protect and improve the lives of children, including safeguarding them from online threats.
* **Website**: [cry.org](https://www.cry.org)

### **Helpline Numbers and Reporting Systems**

#### **1. National Cyber Crime Reporting Portal**

* **History**: Launched in 2019 by the Ministry of Home Affairs, this portal provides a centralized platform for reporting cyber crimes. It aims to make reporting easier and more accessible for the public.
* **Purpose**: To collect and manage reports of cyber crimes, particularly those affecting women and children.
* **Website**: [cybercrime.gov.in](https://www.cybercrime.gov.in/)

#### **2. Cyber Crime Helpline Number**

* **History**: This helpline was introduced as part of India's efforts to combat rising cyber crime. It provides a direct line for individuals to report financial frauds and other cyber crimes.
* **Purpose**: To offer a quick and accessible way for victims to report cyber crimes.
* **Helpline Number**: 1930 (formerly 155260)

#### **3. Indian Computer Emergency Response Team (CERT-In)**

* **History**: Established in 2004, CERT-In is the national agency responsible for responding to cyber security incidents. It helps in handling and mitigating cyber threats.
* **Purpose**: To provide support and guidance for managing and responding to cybersecurity issues.
* **Website**: [cert-in.org.in](https://www.cert-in.org.in/)

#### **4. Ministry of Home Affairs (MHA) Cyber Crime Division**

* **History**: The Ministry of Home Affairs oversees various aspects of internal security, including cyber crime. Their cyber crime division works on policy development and implementation.
* **Purpose**: To coordinate national efforts against cyber crime and develop related policies.
* **Website**: [mha.gov.in](https://www.mha.gov.in)

#### **5. National Commission for Women (NCW) – Online Complaint Registration**

* **History**: The NCW was established in 1992 to address issues related to women’s rights, including online harassment. They offer a platform for women to report cyber crimes.
* **Purpose**: To provide support and legal recourse for women who face cyber harassment.
* **Website**: ncw.nic.in

#### **6. Aarambh India Initiative**

* **History**: Aarambh India focuses on child protection from online abuse and exploitation. They work to raise awareness and provide resources for preventing cyberbullying and other online threats.
* **Purpose**: To safeguard children from online abuse and provide support for affected individuals.
* **Website**: [aarambhindia.org](http://www.aarambhindia.org)

These organizations and helplines play a crucial role in protecting individuals, especially women and children, from cyber crimes and offering support when such crimes occur.

### **1. Information Technology Act, 2000 (IT Act)**

* **Overview**: The primary legislation governing cyber crimes and electronic commerce in India. It provides legal recognition to electronic transactions and digital signatures and addresses various cyber offenses.
* **Key Sections**:
  + **Section 66**: Cybercrimes related to hacking and unauthorized access to computer systems.
  + **Section 66A**: Punishment for sending offensive messages through communication service, etc. (Note: Section 66A was struck down by the Supreme Court in 2015 for being unconstitutional, but similar offenses are covered under other sections).
  + **Section 66B**: Punishment for dishonestly receiving stolen computer resources or communication devices.
  + **Section 66C**: Identity theft, including the use of someone else's identification details without permission.
  + **Section 66D**: Cheating by personation using computer resources.
  + **Section 67**: Punishment for publishing or transmitting obscene material in electronic form.
  + **Section 67A**: Punishment for publishing or transmitting obscene material containing sexually explicit acts.
  + **Section 67B**: Punishment for publishing or transmitting material depicting children in sexually explicit acts.

### **2. Indian Penal Code (IPC), 1860**

* **Overview**: The IPC includes provisions that deal with crimes related to technology and digital platforms, alongside traditional crimes.
* **Key Sections**:
  + **Section 292**: Obscene publications or representations.
  + **Section 293**: Sale of obscene books, etc.
  + **Section 354D**: Stalking, including cyberstalking.
  + **Section 503**: Criminal intimidation.
  + **Section 509**: Word, gesture, or act intended to insult the modesty of a woman (cyber harassment).

### **3. The Indian Telegraph Act, 1885**

* **Overview**: Regulates telecommunications in India and addresses offenses related to unauthorized access to communication networks.
* **Key Sections**:
  + **Section 25**: Prohibition of unauthorized interception of communications.

### **4. The Copyright Act, 1957**

* **Overview**: Protects the rights of authors and creators of original works, including software and digital content.
* **Key Sections**:
  + **Section 63**: Penalties for infringement of copyright, including unauthorized copying and distribution of software.

### **5. The Protection of Children from Sexual Offences (POCSO) Act, 2012**

* **Overview**: Provides protection to children from sexual offenses and includes provisions for handling online exploitation.
* **Key Sections**:
  + **Section 12**: Punishment for using children for pornographic purposes.

### **6. The National Identification Authority of India Act, 2010**

* **Overview**: Establishes the Aadhaar system for identity verification, including provisions for data protection and misuse.
* **Key Sections**:
  + **Section 32**: Penalties for unauthorized use of Aadhaar data.

### **7. The Unlawful Activities (Prevention) Act, 1967 (UAPA)**

* **Overview**: Deals with unlawful activities, including those related to terrorism and cyber terrorism.
* **Key Sections**:
  + **Section 15**: Definition of terrorism, including acts that threaten the sovereignty, integrity, and security of India, which may include cyber terrorism.

### **8. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021**

* **Overview**: Provides guidelines for intermediaries like social media platforms and digital media in addressing grievances and regulating content.
* **Key Sections**:
  + **Rule 4**: Requirements for intermediaries to act on user complaints and remove offensive content.

### **9. The Consumer Protection Act, 2019**

* **Overview**: Protects consumers from unfair trade practices, including those related to digital goods and services.
* **Key Sections**:
  + **Section 2(1)(r)**: Definition of unfair trade practices, which includes fraudulent practices in online transactions.

These laws collectively form the legal framework for addressing various types of cyber crimes in India, ensuring that victims have avenues for redress and that offenders are held accountable.

LEGAL ACTS ONLY FOR CHILDREN AND WOMEN

### **1. Information Technology Act, 2000 (IT Act)**

* **Section 66E**: **Violation of Privacy**
  + **Explanation**: It punishes anyone who captures, publishes, or transmits images of a person's private parts without their consent.
* **Section 67**: **Obscene Material**
  + **Explanation**: It deals with publishing or transmitting obscene material in electronic form. This includes explicit content that can be harmful to women and children.
* **Section 67A**: **Sexually Explicit Content**
  + **Explanation**: It specifically targets the publication or transmission of sexually explicit content online.
* **Section 67B**: **Child Pornography**
  + **Explanation**: It targets those who publish or transmit material that depicts children in sexually explicit acts.

### **2. Indian Penal Code (IPC), 1860**

* **Section 354D**: **Stalking**
  + **Explanation**: It punishes anyone who repeatedly follows or contacts a woman, causing her fear or distress. This includes cyberstalking through social media or other digital platforms.
* **Section 509**: **Insulting Modesty**
  + **Explanation**: It criminalizes the use of words, gestures, or acts intended to insult a woman's modesty, including online harassment.

### **3. Protection of Children from Sexual Offences (POCSO) Act, 2012**

* **Section 12**: **Using Children for Pornography**
  + **Explanation**: It punishes anyone who uses children for pornographic purposes, including creating or sharing child sexual abuse material.

### **4. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021**

* **Rule 4**: **Grievance Redressal**
  + **Explanation**: Requires social media platforms and digital media companies to address complaints of harassment and exploitation, which helps protect women and children online.

These laws are designed to protect women and children from various forms of cyber abuse, including harassment, stalking, and exploitation. They provide mechanisms for addressing and prosecuting such crimes effectively.