SPRF.IN

The Omnipresent Pandemic

Cyber Crimes against women and children

05
22

| Natasha Singh

Issue Brief

TABLE OF CONTENTS

If you have any suggestions, or would like to contribute, please write to us at contact@sprf.in

© Social and Political Research Foundation^{TM}

May 2021

ISSUE BRIEF

The Omnipresent Pandemic:

Cyber Crimes against women and children

| Natasha Singh

ABSTRACT

India's cyberspace is expanding faster than ever before, especially in the context of the COVID-19 pandemic. People have started using the internet as a source of entertainment, work, education, and socialisation. However, with increased use, the risk of cyberattacks has also increased manifold. Women and children make a sizable proportion of the active internet user base of the country. They are also more invested in this platform due to the information they regularly share on it. This article seeks to identify the scale at which cyberattacks are increasing in India by taking women and children as the focus group. This piece also tries to understand and evaluate cyberattack complaints, investigation mechanisms, and how the absence of a proper law on cybersecurity leaves gaps for attackers. This piece concludes with an analysis of the existing laws and policies in this context and presents some recommendations to improve India's cybersecurity.

Keywords: Cybercrimes, women's safety, children's safety, internet safety, cyberspace

INTRODUCTION:

The World Economic Forum [WEF] (2022), in its Global Risks Report, declared cybersecurity, or protection against criminal or unauthorised use of electronic data, as one of its top three concerns globally. With the onset of the COVID-19 pandemic and the subsequent uptick in work-from-home setups and online education, the ambit of the digital world transcended from IT companies and complex government databases to every household. The total number of internet users amounted to 82.53 crores in the country in 2021, from just 68.76 crores in 2019 (Telecom Regulatory Authority of India [TRAI], 2021). As the number of internet users in India increased by 4.7 crores (8.2%) between 2020 and 2021 (Pinto, 2020), so did the threats to India's cybersecurity. In such a setting, women and children are at a greater risk of exploitation because of their increased exposure, the lockdown-induced creation of new online mediums, and the lack of an efficient complaint mechanism. Therefore, with about 42% of women (Kemp, 2021) and children between 5-11 years accounting for the 15% of active internet users of the country (The Hindu Bureau, 2019), it is time that we analyse their security in the vast cyberspace.

In 2021, the National Cyber Crime Reporting Portal run by the Ministry of Home Affairs received more than 6,00,000 complaints, including alleged crimes against women (Tripathi, 2022). Over 12,776 of which were First Information Reports [FIRs]. Here, it is important to understand that cyberattacks have a twofold impact, both at the macro and micro levels. Firstly, these attacks have a deep sociological impact, such as the social disruption caused to people's daily lives or loss of confidence in cyber technology (Bada and Nurse, 2019, Chapter 4). Cyberattacks also lead to the loss of private data like private pictures, contact details, and bank details which may lead to deep psychological trauma and stress.

Finally, these attacks have long-term consequences on the infrastructure and social fabric of any country. While attempts at prevention incur enormous costs, intangible risks such as misinformation and lack of digital safety create a deeper problem. There are also different levels (Complaint and Investigation) of dealing with a cyberattack complaint that affect the security of any country's digital space. Thus, in this piece, India's position on each of these elements will be analysed with the help of a few case studies along with mapping the policy framework for safeguarding them.

FIRST STEP: REPORTING ON CYBERCRIMES AND REGISTERING COMPLAINTS

India recorded 50,035 cases of cybercrime in 2020, which is a sharp 11.8% rise from the previous year's 44,735 cases (National Crime Records Bureau [NCRB], 2020). At the state-level analysis, the largest number of cybercrime cases were reported in Uttar Pradesh with a total of 11,097 cases, marking a 22.17% share of the total tally. Similarly, Karnataka stood second with 10,741 cases and Maharashtra third with 5,496 cases. However, the crime rate was highest in Karnataka with 16.2%, followed by Telangana at 13.4%, and Uttar Pradesh at 4.8% (NCRB, 2020). To put this into perspective, crime rate refers to the number of crimes reported to law enforcement agencies per 1 lakh total population (Members' Reference Service, 2015). This means that while some states have a low number of cases being reported, they may have a higher prevalence of such cybercrimes based on their population intensity.

Table 1: Statistics of 'reported' cybercrimes in India

Years	Cyber Crimes
2016	12317
2017	21796
2018	27248
2019	44735
2020	50035

Source: NCRB (2020)

Similarly, there was an exponential rise of over 400% in cyber crimes committed against children from 164 cases reported in 2019 to 842 cases reported in 2020 (NCRB, 2020). Out of the 842 cases, 732 were related to publishing and/or transmitting materials depicting children in a sexual act. Several child rights activists such as Puja Marwaha, Chief Executive Officer of CRY - Child Rights and You, expressed their concerns about the increasing exposure of children to the internet at large because of online education (Press Trust of India, 2021).

Table 2: Statistics of 'reported' cybercrimes against children in India

Years	Cybercrime against children
2017	79
2018	117
2019	164
2020	842

Source: NCRB (2020)

While there is an overall increase in the number of cases in the country, there are also specific categories of cyber crimes against women that have seen an increase. For instance, cases lodged for publishing sexually explicit content online have increased by 110% in the years 2018-2020. Similarly, cases for cyberstalking and bullying of women have also risen to 872 in 2020 from 739 in 2018.

Table 3: Statistics of 'reported' cybercrimes against women in India

Years	Cybercrimes against women
2017	4242
2018	6030
2019	8379
2020	10405

Source: NCRB (2020)

To understand these figures better, the NCRB also provides details of the intention behind the cybercrime committed and registered. Among the total, fraud emerged as the key 'motive' or intent in 30,142 or 60% of the total number of cybercrimes recorded in the country for the year 2020. The second was sexual exploitation, forming 7% of the total cases with 3,293 cases, followed by extortion (2,440 cases), causing disrepute (1,706 cases), and personal revenge (1,470 cases) (NCRB, 2020). These five motives collectively accounted for 78% of the total cybercrime cases reported in 2020.

Here, it is important to understand that these numbers barely represent 1% of the actual incidents (Das, 2017). People seldom come forward to report cybercrimes, either because of the loopholes in the legal system, or the general socioeconomic pressure that goes with the reporting of such incidents. Moreover, the police's response towards cybercrime complaints also forms a huge portion of this under-reporting. In some cases, the police are not technologically equipped to handle these cases and resort to hiring private investigators (Chandrashekhar & Mohanty, 2019). In other cases, their outlook on complaints by women and young teenagers on cybercrimes is not always in the most supportive tone, resulting in further hesitancy in reporting (Leukfeldt et al., 2020).

SECOND STEP: POLICE INVESTIGATION AND FOLLOW-UP

Table 4: Police Disposal of Cyber Crime Cases (State/UT-wise)

Total Cyber Crimes	Cases Pending Investigations from Previous Year	Cases Reported during the year	Cases Reopened for Investigation	Total Cases for Investigation
2020	53157	50035	796	103988
2019	32099	44546	24	76669
2018	22610	27248	22	49880

Source: NCRB (2020)

There are several obstacles with cybercrime investigations. One such obstacle is the privilege of anonymity that this technology offers to its users. With this anonymity, any individual's actions hold zero accountability and the encryption systems on some apps further make it impossible to track the offenders (United Nations Office on Drugs and Crime, 2020). In cases of crimes against women and children, where fake profiles are created with morphed images to blackmail the victim, tracing takes a lot of time. Another issue with the investigation is the attribution of who and/or what is responsible for that particular crime. As these types of crimes occur from one IP address to another, it is difficult to identify the cause and effect.

Several loopholes exist within the system due to which a gap continues between reporting of crime, arresting a criminal, and finally ensuring successful prosecution of the accused in cybercrime cases. For instance, the conviction rate for publication or transmission of sexually explicit content is 47.1% while in cases of cyberstalking and bullying, it is as lower as 27.6% (Tripathi, 2022).

Lastly, the police are often handicapped in undertaking effective investigation due to the absence of modern gadgets such as high-capacity data transfer tools, software designed for analysis of phones, tools for recovering passwords using brute force algorithms, etc. Forensic science laboratories which can render timely assistance to the investigating police are scarce at the district level (Agnihotri & Jha Associates, n.d.). The result is that the police depend heavily on oral evidence, instead of concentrating on scientific and circumstantial evidence which are fundamental to cybercrime investigations.

POLICIES AND RECOMMENDATIONS

Cyberattacks in India are not restricted to any specific medium, sector, or method, and are spreading faster than anticipated. What makes Indian cybercrime prevention even more complicated is the absence of a proper law that only deals with cyberspace and its components. Currently, it is governed by multiple legislations, which primarily constitute the Information Technology Act [IT] of 2000 (Ministry of Electronics and Information Technology, 2021), followed by additional rules such as the Indian Penal Code [IPC] 1980, and the Companies Act, 2013. Even the Data Protection Bill of 2019, which extensively talks about the right to access, correct, and port relevant user data, is still under the wraps of the Joint Parliamentary Committee.

Information Technology [IT] Act of 2000 and IT Amendment Act of 2008

The genesis of the IT Act, 2000 can be traced back to the era of globalisation when the internet penetration rate was 0.5% (World Bank, 2020), but there was an urgent need to establish a reliable framework for e-commerce (The Information Technology Act, 2000). Being the first legislation on technology, it was subjected to intense scrutiny in its initial years. Several advisory groups were formed and their recommendations led to the IT Amendment Act, 2008. Hence, this act was expanded to include data privacy, the role of the Computer Emergency Response Team [CERT-In], cyber terrorism, child pornography, digital guidelines for corporates, etc. This amendment also brought technological neutrality by recognizing electronic signatures as a legal way of executing signatures (Centre for Internet and Society, 2009).

However, even after all these provisions, this act has fallen behind the times in addressing cybersecurity. There have been no amendments in the act since 2008, and the cyberworld has developed since then by leaps and bounds. Even in the current format of the act, there are several blank spaces.

Firstly, Section 77B provides all offences punishable with imprisonment of 3 years and above as cognizable and all offences punishable with imprisonment of 3 years or less as bailable. There are only 4 offences under the said Act that have imprisonment of more than 3 years. But with a chargesheeting rate of only 47.5% in cybercrimes (NCRB, 2020), having a provision for easy bailable offences only increases the confidence of cybercriminals. Pavan Duggal, one of the top cyber laws experts in the world, said, “The 2008 amendment was built on an erroneous presumption that it would be better to reduce the quantum of punishment and increase the fine” (Ghosh, 2019). However, this amendment has only eliminated the deterrents to cybercrime (Ghosh, 2019). Next, the concept of ‘exemption for intermediaries’ also forms a significant part of this amendment. According to Section 79, an internet service provider shall not be held liable for any third-party information or link being made available by them unless there is a conspiracy or abatement claim proved against them. This means that the burden of proof has now shifted from the internet service providers to the complainant, which in this situation will be challenging to prove owing to the well-netted encryption systems. This will make the entire prosecution process even more difficult in cases of crimes against women and children, who are already at a position of disadvantage.

Nonetheless, there are also some monumental steps taken under this Amendment Act, such as broadening the term ‘communication device’ to include everything beyond simple phones and other devices. Or, redefining the role of adjudication officers under Section 46 (1A) where only a claim for injury or damage that does not exceed 5 crore will be heard. Beyond 5 years, the jurisdiction will fall within the competent court, thus giving a second forum of appeal to victims of cybercrimes.

Data Protection Bill, 2019

Data is one of the most valuable repositories for any individual or nation, and the majority of it is exchanged in cyberspace. This highlights the need for a robust data protection law that strikes a perfect balance between the right to privacy and keeping a check on misuse of data. The most recent development in this context is the Personal Data Protection Bill of 2019, as introduced in the Lok Sabha and now in the Joint Parliamentary Committee (The Personal Data Protection Bill, 2019). This bill reclaims the agency of users to erase personal data from the internet among other provisions (Katarki et al., 2020).

However, there are other aspects, such as processing data without an individual’s consent for ‘reasonable purposes’ that require more clarity. For instance, the bill allows the processing of data by fiduciaries only if the individual provides consent. But in certain circumstances, it can process personal data without consent, and one such clause is “if required by the State for providing benefits to the individual” (The Personal Data Protection Bill, 2019). This is a vague explanation that the state machinery can abuse to turn against its own citizens that disagree with its policies. Similarly, the central government can exempt any of its agencies from the provisions of the Act, as it quotes for the “interest of the security of state, public order, sovereignty and integrity of India” (ibid.). This clause offers a blanket cover for the State to cover its own tracks. Lastly, the Bill also amends the Information Technology Act, 2000 to delete the provisions related to compensation payable by companies for failure to protect personal data, exposing the ex-employees to greater risk with no financial backing (PRS Legislative Research, 2019). Thus, while this Bill is a step in the correct direction of providing supremacy to personal data and its privacy, there remain aspects of it that require greater clarity to make sure this does not put the citizen's access to free and fair cyberspace into jeopardy.

WAY FORWARD

The Act has played a pivotal role in setting fundamentals of cybersecurity in India, catering to the most pressing concerns in cyberspace. There is, however, a greater scope of improvement in enhancing the overall nature of cyber legislation in India. For instance:

Inclusion of new forms of technologies in cyberattacks

With technological developments, the methods of cyberattacking have also diversified. For instance, with the rise of digital payments, there has been an increase in digital transaction cybercrimes (Radhakrishnan & Singaravelu, 2020). The companies offer a frictionless user experience to their customers, which offers an inadequate window to the banks and the RBI to identify and respond to cyber threats. Similarly, concepts such as phishing and spamming are yet to see an isolated section in the IT Act, last amended 14 years ago in 2008. Thus, there is an urgent need to expand our scope of these laws to include recent forms of interactions in the digital space.

Central Cyber Response Entity

At present, there are few immediate Cyber Response Teams in the country at the state levels that have a recovery plan in place in case of an immediate attack, or can be consulted to draft future legislation on cybercrime. While the CERT-In was established under the IT Act, 2008 with a proactive role of risk analysis and vulnerability analysis. There is an urgent need to have a strong integrated system in place, at the state and district levels, to not only ensure a secured and timely response to cyber threats but to also conduct relevant training of the citizens in identifying and handling such instances. This decentralisation in the cyber security space will prove beneficial, especially in India, where there are a lot of socio-economic factors that come into play for the timely reporting of cybercrimes (Aggarwal & Shruti, 2018).

Thus, cybercrimes are a multifaceted issue that have a deep impact on both micro and macro levels. It not only psychologically impacts an individual but also affects the society on a larger socio-economic basis, further expanding the digital divide. It is therefore the need of the hour to democratise cyberspace, introduce reforms in the present legislations, and equip the state machinery and citizens to effectively fight the war against these invisible crimes.

BIBLIOGRAPHY

Aggarwal, V. & Shruti. (2018). Cybercrime Victims: A Comprehensive Study. *International Journal of Creative Research Thoughts*, 6(2), 640–648. https://ijcrt.org/papers/IJCRT1807078.pdf.

Agnihotri & Jha Associates. (n.d.). Cyber Investigation - How Prepared are the Indian Police? HG.org. *Legal Resources.* https://www.hg.org/legal-articles/cyber-investigation-how-prepared-are-the-indian-police-37384.

Bada, M. & Nurse, J. R. C. (2019). The Social and Psychological Impact of Cyber-Attacks. In V. Benson & J. McAlaney (Eds.), *Emerging Cyber Threats and Cognitive Vulnerabilities* (pp. 74–93). Academic Press. https://arxiv.org/ftp/arxiv/papers/1909/1909.13256.pdf

Centre for Internet and Society. (2009). Short note on IT Amendment Act, 2008 — The Centre for Internet and Society. *The Centre for Internet and Society.* https://cis-india.org/internet-governance/publications/it-act/short-note-on-amendment-act-2008.

Chandrashekhar, A. & Mohanty, S. (2019, December 13). Police in states across India are relying on private firms and consultants to solve cybercrime cases. *The Economic Times.* https://economictimes.indiatimes.com/news/politics-and-nation/police-in-states-across-india-are-relying-on-private-firms-and-consultants-to-solve-cybercrime-cases/articleshow/72499885.cms?from=mdr.

Das, S. (2017, December 13). Cybercrime cases in India are under-reported, say experts. *Mint.* https://www.livemint.com/Politics/kmE7EC9twVDn3DSIZlH8QM/Cybercrime-cases-in-India-are-underreported-say-experts.html.

Ghosh, S. (2019, November 12). *India's IT Act 2000 a toothless tiger?* CSO Online. https://www.csoonline.com/article/3453078/india-s-it-act-2000-a-toothless-tiger-that-needs-immediate-amendment.html.

Katarki, S., Viswanath, N., Chatterjee, I., & Reddy, R. (2020, January 6). *The Personal Data Protection Bill, 2019: Key Changes And Analysis - Privacy - India.* Mondaq. https://www.mondaq.com/india/privacy-protection/880200/the-personal-data-protection-bill-2019-key-changes-and-analysis.

Kemp, S. (2021, February 11). *Digital in India: All the Statistics You Need in 2021 — DataReportal – Global Digital Insights.* DataReportal. https://datareportal.com/reports/digital-2021-india.

Leukfeldt, E. R., Van de Weijer, S. G. A., & Van der Zee, S. (2020). Reporting Cybercrime Victimization: Determinants, Motives, and Previous experience. *Policing: An International Journal of Police Strategies & Management,* 43(1), 17–34. https://doi.org/10.1108/PIJPSM-07-2019-0122.

Members' Reference Service. (2015). *CRIME SCENARIO IN INDIA.* Parliament Library. http://164.100.47.193/Refinput/New_Reference_Notes/English/crime.pdf.

Ministry of Electronics and Information Technology. (2021, November 1). Cyber Laws | Ministry of Electronics and Information Technology, Government of India. https://www.meity.gov.in/content/cyber-laws.

National Crime Records Bureau [NCRB]. (2020). *Crime in India.* https://ncrb.gov.in/sites/default/files/CII%202020%20Volume%202.pdf.

Pinto, V. S. (2020, May 9). Covid-19 lockdown effect: Every second Indian now on internet in cities. *Business Standard.* https://www.business-standard.com/article/economy-policy/covid-19-lockdown-effect-every-second-indian-now-on-internet-in-cities-120050801805_1.html.

Press Trust of India. (2021, November 14). Over 400% rise in cyber crime cases committed against children in 2020: NCRB data. *The Economic Times.* https://economictimes.indiatimes.com/news/india/over-400-rise-in-cyber-crime-cases-committed-against-children-in-2020-ncrb-data/articleshow/87696995.cms.

PRS Legislative Research. (n.d.). *The Personal Data Protection Bill, 2019.* PRS India. https://prsindia.org/billtrack/the-personal-data-protection-bill-2019

Radhakrishnan, V. & Singaravelu, N. (2020, September 25). Data | Significant rise in digital transactions met by surge in cyberfrauds. *The Hindu.* https://www.thehindu.com/data/significant-rise-of-digital-transactions-met-by-increase-in-cyberfrauds/article32696340.ece.

Telecom Regulatory Authority of India. (2021). *The Indian Telecom Services Performance Indicators January – March, 2021.* https://www.trai.gov.in/sites/default/files/QPIR_27082021.pdf.

The Hindu Bureau. (2019, September 26). 66 mn children aged 5-11 years are active Internet users in India. *The Hindu Business Line.* https://www.thehindubusinessline.com/info-tech/66-mn-internet-users-in-india-aged-between-5-and-11-years/article29518418.ece.

The Information Technology Act, act no. 21, (2000). https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf.

The Personal Data Protection Bill, bill no. 371, (2019). http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

Tripathi, R. (2022, January 6). Cases targeting women with explicit content double in 3 years. *The Economic Times.* https://economictimes.indiatimes.com/news/india/cases-targeting-women-with-explicit-content-double-in-3-years/articleshow/88719638.cms?from=mdr.

United Nations Office on Drugs and Crime. (2020, March 14). *Cybercrime Module 5 Key Issues: Obstacles to Cybercrime Investigations.* United Nations Office on Drugs and Crime. https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/obstacles-to-cybercrime-investigations.html.

World Bank. (2020). *Individuals using the Internet (% of population) - India | Data.* World Bank Data. https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=IN.

World Economic Forum. (2022). *The Global Risks Report* (17th Edition). https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf.

SPRF.IN