CYBER CRIME VIS-A-VIS DATA PRIVACY: DOCTRINAL INVESTIGATION

Sanjeev Kumar
Research scholar, Career Point University Hmairpur HP India
Sanjeevsanjeev292@gmail.com, Contact: 701850432

ABSTRACT

Aside from having consequences at the biological model's local level, the pandemic has repercussions at the national level, in that it has a negative impact on social union and access to public administrations and institutions that house people's socially stimulating groups of individuals. The suspension or reduction of activities in temples, childcare centres, schools, and social insurance administrations, as well as the shifting of needs in health-care administrations to activities focused on patients with respiratory side effects and cases associated and confirmed with COVID-19, endangers the quest for assistance, assurance, and alternatives. The consistency and disarray of previous conditions of viciousness are accentuated by each of these factors. The length of time spent in touch with the attacker is a critical element at the social level. In addition, due of the reduction in the casualty's social contact with family members, the chances of the woman establishing and strengthening a socially supportive network of individuals, seeking assistance, and breaking free from the vicious cycle are reduced. Day by day continuous interaction, especially in low-wage families living in cramped quarters with few rooms and a lot of traffic, reduces the chances for women to record demonstrations in a safe manner, discouraging them from making this option. One problem that has received little attention from analysts, directors, and other members of the COVID-19 emergency panels is the impact of social separation on relational relationships, especially between intimate partners and between guardians and children, which is discussed in this debate. Global associations specialists and the established press have expressed concern over evidence of increasing aggressive behaviour at home, where the home has frequently become a source of fear and mistreatment as a result of previous social removing circumstances and the unexpected increase in reports of viciousness in the pandemic's specific situation.

Keywords: Pandemic, Cybercrime, Women, Law, Covid-19, Data Protection

INTRODUCTION

The lockdowns that followed the COVID-19 epidemic have resulted in an increase in the number of domestic violence cases in several countries across the world. Because it has been shown to be an effective strategy in fighting the coronavirus, the people were instructed to remain inside in their individual homes. While preventing the spread of the virus, they have also drawn attention to the persistent gender disparities and dangerous dangers that women face throughout the globe, in addition to the potentially lethal ramifications of the pandemic itself.

In violent homes, women are afraid of the aggressor on the inside as much as the virus on the outside. When people are confined with violent relationships, they are more likely to experience physical and emotional abuse. Because of the restrictions that have been established, it is difficult for victims to flee from their abusers and seek assistance. Because of their cruel inlaws and abusive spouses at home, women are frightened to seek police assistance and to record incidents of domestic violence. Because of a lack of financial assistance, some are reliant on them for their daily subsistence. After losing their jobs during the shutdown, men in low-income families are more likely to be physically violent to their wives as a way of venting their anger on their wives. Their animosity is heightened even more by the removal of alcohol from their lives. The prolonged privateness of the house provides the abusers with a false sense of protection. Women are terrified of a variety of obstacles, including the possibility of being diagnosed by their abuser, the possibility of contracting coronavirus when outside their homes, and the ambiguity around the availability of current local services. On many families, the financial instability seen via the possibility of hunger has the potential to reflect and manifest itself in the form of verbal and physical violence. Many girls are unable to register a complaint or contact authorities since they are confined with their abusers and the coronavirus illness is prevalent outside their homes.

RESEARCH PROBLEM

People all across the globe have questions because the epidemic forced them to provide personal information to numerous organisations and post it online. In this paper, I will address some of the issues. What if, in response to COVID-19 (e.g., to the government and/or health organisations), we must reveal personally identifiable information ("PII") of our customers, visitors, or website users?

In exceptional cases, such as preventing the spread of COVID-19, the government may require a person to provide some PII. The policies that do identify the forms of PII often contain wording that specifies monitoring consumer purchase timing and location, tracking human movement through relocation data from applications, cookies, and pixels. Companies generally urge consumers to submit this information in return for future product or service discounts. Despite this phrasing, consumers seldom consider using PII for public health objectives. For now, businesses and organisations must examine their privacy policies to ensure they cover the sharing of PII to government and public health authorities for emergency reasons. Standard privacy policies should cover disclosing PII to safeguard someone's health or safety, or to comply with a legal duty. Customers and partners should also engage appropriate specialists to determine if their unusual revelation of PII will result in a new product, service, or a change in the organization's position.

OBJECTIVES

The main objective of research is to analyse the cyber security threat to data privacy during covid, different types of threats in the current scenario and need for introducing cyber security strategy for the safety of data protection.

RESEARCH METHODOLOGY

For the present research paper the doctrinal methodology has been applied. Researchers have taken the help of secondary sources. Secondary sources include articles, books, journals, newspapers and websites.

Responses and Measures at the International Level

At the time of the COVID-19 pandemic, the United Nations recognised domestic violence directed against women as a "shadow epidemic." Earlier this year, Antonio Guterres, the Secretary General of the United Nations, issued an advisory to countries, urging them to prioritise the protection of women in responding to the epidemic.

During the same period as thought about lockdown and social distance was developing, methods to protect women from being shut in with their abusers began to emerge in exclusive parts of the arena. The countries of Spain, France, Germany, Italy, Norway, and Argentina have all participated in a campaign dubbed Mask-19. After being subjected to domestic violence, a woman will go to the closest pharmacy and ask for Mask-19, which is a protective mask. Employees at the pharmacy take her phone number, as well as her address. They make the emergency offerings aware of the situation. The lady may either go down back to her household duties or gaze forward to the arrival of the police and direct people. The increasing number of reported instances during the first week of the lockdown prompted the French government to declare that it would pay for resort accommodations for victims of domestic abuse and establish pop-up counselling centres to assist them. It will also provide anti-domestic abuse organisations with an extra 1,000,000 Euros to help them in responding to an increased demand for services in the future. Domestic violence shelters in Canada will remain available for victims of domestic and gender-based abuse for the foreseeable future. It is providing them with a $50 million donation to assist them. The sponsoring groups have also received funding from the United Kingdom and Australia. The Italian authorities have developed an app that allows victims of domestic abuse to seek for assistance without having to create a telephone number in order to do so. There has been a fantastic effort made by them to address the general problem.

Indian Scenario

India is not always an exception to the worldwide trend of increased epidemic brought on by domestic violence, as has been the case in recent years. During the lockdown, the National Commission for Women in Delhi received a large number of distress calls, which were sent to them. It has made an emergency WhatsApp number available for the duration of the lockdown in order to register instances and assist victims of domestic abuse. Helplines and non-governmental organisations (NGOs) are working to find solutions for the victims, including relocating them to safer locations and providing counselling through smartphone or the internet. As a way to assist survivors of domestic violence, a company has set up a 24-hour hotline called 'Dhwani,' as well as a WhatsApp phone number, an email ID, and a chat function on its website.

An action for public interest has been filed in the Delhi High Court as a result of an increase in the number of domestic abuse cases in the country as a result of the countrywide lockdown, according to the filing. The petitioner has asked if the provisions of the Disaster Management Act may be utilised to provide further protection to the victims of the disaster. It has come to light that the Delhi Commission for Women has selected the finest 17 protection officers in Delhi, but their contact information is not publicly available. When the lockdown is lifted, the Delhi High Court has ordered the National Commission for Women (NCW), the Delhi Commission for Women (DCW), the Delhi government, and the Union Ministry for Women and

Child Development to submit written notes on the measures being taken to protect victims of domestic violence at a later stage. It further inquired as to whether the coronavirus pandemic had been designated a "catastrophe" under the term provided by the statute in question. The authorities have been instructed to maintain control over important documents as well as to examine the subjects of domestic violence and child abuse. The All India Council of Human Rights, Liberties, and Social Justice, a non-governmental organisation (NGO), has filed a petition with the court to ensure the adoption and implementation of urgent and effective measures to help victims of domestic violence and infant maltreatment. The court has ordered the Central Government, the Delhi Government, the Delhi Commission of Girls, and other government agencies to convene a conference at the highest level to discuss the issue of victims of domestic violence in this generation, which was previously ignored.

Soon after Prime Minister Narendra Modi declared a national lockdown to combat the epidemic, it became clear that the authorities had failed to account for the consequences of the pandemic on vulnerable sectors of society, including as migrant labourers and the homeless. Many victims of domestic abuse avoid visiting their parents' homes because they are concerned about infecting their elderly mother and father. They are also unable to attend refuge homes since they may be overcrowded and thus more susceptible to illness. The police department is already overloaded with the responsibility of ensuring that individuals adhere to the lockdown. When it comes to domestic abuse cases, hospitals simply do not have the resources or time to deal with them. Because of this, they are compelled to stay in abusive and violent situations with no opportunity for restitution. If they are fortunate enough to survive, those who do so will find themselves in a distant area without access to vital resources and services.

Since the lockdown started, many non-governmental organisations (NGOs) have been providing targeted helplines 24 hours a day to assist the ladies in the lack of a clear strategy from the Indian government. They are dealing with a problem in terms of providing help since they are unable to do more than telephone or online counselling. There is a desperate need for adequately financed and essential assistance programmes for survivors of abuse. It is impossible to overestimate the importance of psychological support and financial resources. Even while the spread of the radical Coronavirus (COVID-19) pandemic throughout the globe is increasing dread tremendously, the health concerns associated with this catastrophic catastrophe are not the most serious consequences of this event. It has been observed that during this period of social distance and erroneous information, the dark forces of society were given a chance to flourish. Criminal activity on the internet and coronaviruses- There has been an influx of spoof apps, domains, and web sites that are capitalising on two pieces of information: first, the widespread concern about the pandemic and their search for information about it; and second, the increasing number of corporations around the world that are turning to the internet to 'earn a living from home'. We will go through both situations in turn, one after the other.

The vast majority of people who have been confined inside their homes during this lockdown are attempting to stay on top of any COVID 19 statistics in an effort to be safe and away from incendiary individuals. The developers of malware are taking use of this situation to their advantage. A Coronavirus tracking software, "corona live 1.1," was available for download from the Google Play Store and purported to be a real-time tracker of Coronavirus cases. While the individuals who were making use of the programme believed that they were preserving a piece of the pandemic's history, the rogue software was completely violating their privacy by gaining access to the tool's photographs and videos as well as its location and digital camera. The data gathered may be utilised in a variety of ways, including to undermine your bank's ability to collect money due to you or even to blackmail the person who took the photographs and films. For example, the Android Playstore has removed numerous bogus applications from its store and continues to establish rules for these kinds of programmes. It has also put all such apps in the'sensitive events' category, which is intended to deter people from downloading false apps and using them. In recent years, the applications have been made accessible on bogus websites, one of which is the 'coronavirusapp. Web page,' which has a connection to the app's download page. Coronavirus has caused an increase in cyber-crime, which has been well documented throughout this time period.

Because of the lockdown, every commercial organisation, large or little, has been compelled to operate from a distant location. This may result in an increase in security risks when proprietary information is accessed from laptops and home PCs that may or may not be protected with the same level of firewall and protection as an in-office configuration. You may have noticed an increase in the number of emails seeming to be from the COVID-19 in your Junk Folder. These emails are posing as an alert about the COVID-19. These emails will entice the recipient to open the attachments, which may or may not be dangerous in nature, and the moment you do so, the malware writer may be able to get access to your computer system and take control. As soon as the virus has infiltrated one of your systems, there may be a potential danger that the security of the structures of your colleagues' systems will be compromised, as well. This may have a significant effect on the whole grid of systems that keeps the commercial organisation connected, and it can result in a significant loss of confidential information. As a result of the coronavirus epidemic in India and across the world, there has been an increase in cybercrime incidents. In such situations, companies may depend on the ISO/IEC 27000 circle of relatives for assistance. The ISO/IEC 27000 certification is an international benchmark certificate that is awarded to organisations that adhere to the Information Security Management System (ISMS) (ISMS). In addition to allowing you to enhance the structure and cognizance of your company, the ISMS allows you to safeguard your sensitive records as well as the confidential records of your clients from cyber assaults.

According to GR Radhika, Superintendent of Police, Cyber Crimes, AP Police, statistics from the National Crime Records Bureau (NCRB) in 2018 showed that 6,030 cyber crimes were reported by women, according to an online webinar organised by the AP CID and Cyber Peace Foundation on September 23, 2020. "In India, 71 crore individuals use the Internet, with 25 crore of them being women. According to her, 80 percent of individuals are victims of cybercrime, and 63 percent are unsure where to file a complaint "about online crimes.

A cyber-crime victim may report the incident on social networking platforms. Victims of cybercrime may file a complaint with Cyber cells, which have been set up specifically to help victims of cybercrime. They are under the jurisdiction of the police department's criminal investigation division. Each state's Nodal Cyber Cell Officers are listed below. At www.cybercrime.gov.in, you may also submit a complaint. A handbook on reporting cybercrime may also be found on the National Cyber Crime Reporting Portal to assist you with the procedure. An FIR may be filed with the local police station to file a complaint. The victim may seek assistance from the Ministry of Women and Child Development, which has a special email address (complaint- mwcd@gov.in) for complaints about abusive, harassing, or offensive behaviour on social media.

According to the Maharashtra Police's Cyber Security Crime Wing, fake URLs relating to COVID-19 are being disseminated on the internet through social media postings and WhatsApp. Through these false communications, the fear and vulnerability of the public are used in the direction of the coronavirus. According to police, the following messages are being distributed:

1. Assuring work to human people between the ages of 18 and forty, who possess Class certifications and receive a monthly salary of Rs. 3,500 during the lockdown,
2. Coronavirus remedies and extra insurance
3. Free Netflix or other video streaming service recharges, 4. Free internet records, and 5. Liquor sales offers.

Those communications, however, include dangerous links. These connections were designed to gather statistics, as well as sensitive and personal information saved on the user's devices. The links aid in the execution of various phishing and malware attacks, thus jeopardising the device's and data's security. Since the lockdown, people's online presence has grown, making them more vulnerable to similar assaults.

To alleviate the shortage of masks and hand sanitizers during the lockdown, many fraudsters have created phoney e-commerce websites offering these goods. These crooks are playing on the populace's anxiety in order to get the COVID-19. However, the devices are never released, and the website is eventually shut down.

In March 2020, according to Kaspersky's telemetry, the total number of bruteforce assaults against the remote desktop protocol (RDP) increased from 93.1 million in February 2020 to 277.4 million in March 2020, representing a 197 percent rise over the previous month's total. It increased from 1.3 million in February 2020 to 3.3 million in March 2020, according to the latest available data. The number of monthly assaults never dropped below 300 million from April 2020 forward, and they hit a new all-time high of 409 million attacks globally in November 2020. With 4.5 million assaults in July 2020, India set a new record for the most attacks in a single month.

In February 2021, almost a year after the outbreak began, there were 377.5 million brute-force assaults, a significant increase from the 93.1 million recorded at the start of the epidemic in January 2020. In the month of February 2021, 9.04 million assaults were recorded in India alone. Approximately 15 million assaults were reported in India during the months of January and February of 2021.

The Prime Minister's Citizen Assistance and Relief in Emergencies (PM Care) Fund receives a large number of human contributions. PMCARES@sbi is the Fund's UPI ID. However, police have discovered that fraudsters have created identical UPI IDs, such as pmcares@icici, pmcares@yesbank, and pmcares@ybi, in order to swindle individuals. The Indian Computer Emergency Response Team (CERT-In), in collaboration with banks, government agencies, and law enforcement agencies, issued warnings to deter fraudulent activity.

After being alerted to fraudsters' attempts to abuse the EMI Moratorium Scheme, Indian banks contacted their clients and strongly advised them not to give private information such as OTP and ATM PIN with imposters who began calling people and promising to help them in suspending the EMI charge.

The Indian government has launched a lawsuit against the person who advertised the sector's largest statue for $4 billion on OLX, a customer to consumer (C2C) marketplace. According to the ad, the money produced by the selling of the legislation would be used by the government to cover its medical costs during the coronavirus epidemic.

APT Groups Advanced Persistent Threat (APT) groups are defined as companies that conduct cyberespionage and cybersabotage against an overseas state's information pertaining to national security or financial importance. These businesses continue to comply and profit throughout the epidemic. They targeted hospitals with ransomware, spyware, and distributed denial of service (DDoS) assaults. Not only are the assaults carried out with the aim of generating revenue, but also to extract and get access to login passwords and sensitive intelligence data. Naikon, a Chinese-language APT institution, has been concentrating its efforts on the Asia Pacific region's worldwide destinations. According to IT security firms, their technique of attack is to penetrate a central authority frame and collect private information in order to launch a phishing assault on several government targets.

Zoom, a video conferencing application, enables professionals and students to have online conferences and participate in online training. However, concerns have been made regarding the app's security in the recent past. Zoom bombing is a term that refers to an action in which hackers get access to a particular gathering and bombard it with unwanted information. There have been instances in the recent past where inappropriate material, such as a pornographic video, was performed during an online lecture room session or a conference. The company has taken steps to minimise zoom bombing times by eliminating Personal Meeting IDs for scheduling or initiating meetings and requiring a password for all meetings. Additionally, display sharing rights may be restricted to the host by default.

Since the outbreak of the COVID-19 pandemic, the World Health Organization (WHO) has seen a dramatic increase in the number of cyber assaults aimed against its staff. According to WHO estimates, 450 current WHO e-mail addresses and passwords were stolen online, along with hundreds of others belonging to those affected by the extreme coronavirus response. However, the disclosed data did not endanger the WHO system since they were outdated, but the attack did impact an older extranet device that is used by current and retired staff members in addition to partners. The number of cyberattacks on the agency is fivefold that of the same period last year.

Data Privacy: Legal Framework

The EU General Data Protection Regulation (GDPR), which went into effect in May 2018, created a worldwide standard for personal data protection. The proposed bill incorporates the GDPR's principles while also trying to adapt the legislation to Indian requirements. Purpose restriction, data reduction, restricted grounds of processing, data quality and security, and privacy by design are some of the concepts evident in both frameworks.

However, the bill varies in key ways, indicating the particular Indian subtleties that the Expert Committee had to contend with when drafting the legislation. Data principals and data fiduciaries' connection is seen through the perspective of a trust expectation. Data fiduciaries have a responsibility to manage data in a fair and responsible way for the reasons that the data principals reasonably anticipate. This is a unique feature that has yet to be seen in any other privacy framework. The following are the key principles of a data protection law:

- Technology neutrality
- Comprehensive utility
- Consent with knowledge
- Data minimisation
- Controller responsibility
- Structured enforcement
- Dissuasive consequences

The law establishes criteria for ordinary consent's validity, including that it be free, informed, precise, unambiguous, and revocable, in order to provide a meaningful notice and consent system. The data fiduciary has the responsibility of demonstrating that the data principle has provided valid permission. Furthermore, permission requirements for sensitive personal data are more stringent. Passwords, financial data, health data, official identifiers, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious or political belief or affiliation, or any other category specified by the Data Protection Authority are examples of sensitive personal data.

The law places limitations on the transfer of personal data across borders. This is accomplished via a non-exclusive localization requirement, which requires a data fiduciary to guarantee that all personal data is stored in a single serving copy. Furthermore, an exclusive localization requirement mandates that essential personal data be handled exclusively on an Indian server or data centre. The federal government must declare what constitutes essential personal data. Localization requirements are an effort to establish data sovereignty, as shown by the Reserve Bank of India's order on payment system data storage (2018) and the proposed national e-commerce policy from the Department of Industrial Policy and Promotion (2019). It is worth thinking about whether the advantages of localisation might be delivered in a less restricted way. The bill also outlines requirements for cross-border transfers of non-sensitive personal data, such as the transfer being subject to standard contractual terms or intra-group schemes authorised by the authority, the authority's permission due to necessity, the data principal's consent, and so on.

The bill's passage will result in a change in India's data protection system. It will also set stringent compliance requirements on businesses that handle personal data. These include data trust scores, data protection impact assessments, yearly data audits, the designation of a Data Protection Officer, and a transparent data processing system that allows data principals access.

CONCLUSION

The Information Technology Act of 2008 has many restrictions in terms of protecting women against cybercrime. The Information Technology Act does not specifically address cyber defamation, which is still dealt with under Sections 499 and 500 of the Indian Penal Code, 1860, respectively.

The government, non-governmental organisations (NGOs), and other players in our democracy have yet to make significant progress in establishing strong mechanisms to combat cybercrimes against women.

Security standards have undoubtedly worsened as a result of many companies' unwillingness to work remotely, and cybercrime has seen an increase as a result of coronavirus. We shall protect our data and privacy with a little care and due diligence. It is generally prudent to err on the side of caution, but if, despite all measures, we succumb to a lure, a quick action may mitigate the loss. It is advisable to address a criticism to the appropriate authorities. With the lockdown being extended, the punishment for the victimised girls will only grow longer. While we take all necessary efforts to flatten the pandemic curve, we must also be vigilant to ensure that the curve of intimate terrorism does not aggressively ascend. The management and regulatory enforcement industries seek to comprehend the magnitude of the problem. It is essential for policymakers to consider the needs of abused women who contribute significantly to the fight against coronavirus as caretakers, health and sanitation workers, scientists, and suffering housewives. Girls' protection must be postponed till the epidemic is over. Priority actions must be implemented with the assistance of authorities while adhering to the COVID-19 action plan for assisting and protecting victims of domestic abuse.

REFERENCES

1. Nandini Tripathy, cyber crime against women and children during pandemic times, Pro bono India (2020).
2. Available at: https://www.firstpost.com/health/coronavirus-outbreak-anxiety-in-times-of-covid-19-domestic-violence-and-cyber-crime- (Last Modified July 27, 2021).
3. Available at: https://www.thehindu.com/news/national/andhra-pradesh/cyber-crimes-against-women-on-the- rise/article32399536.ece(Last Modified July 27, 2021).
4. Ibid.
5. Ibid.
6. Supra note 1 at 2.
7. Available at: https://www.bmj.com/content/369/bmj.m1712 (Last Modified July 02, 2021).
8. Supra note 6 at 4.
9. Available at: https://opengovasia.com/indias-initiative-for-cyber-crimes-against-women-and-children/ (Last Modified July 03, 2021).
10. Supra note 8.
11. Available at: https://www.hindustantimes.com/india-news/ncw-received-2-043-complaints-of-crimes-against-women-in-june-highest-in-8-months/story XXf69w 9jnWi0dSbw3PhTjJ .html (Last Modified July 27, 2021).
12. Dr.Dilipkumar A. Ode & Mr.Jigeshkumar D. Chauhan, Current Major Issues In India (BOOKLET-2) 88 (RED'SHINE PUBLICATION PVT. LTD, 2020).
13. Sharma, D. (n.d.). Cyber crime in India: Are women a soft target. Legal Service India - Law, Lawyers and Legal Resources. available at:

https://www.legalserviceindia.com/legal/article-639-cyber-crime-in- india-are-women-a-soft-target.html (Last Modified July 17, 2021).

14. Available at: https://www.ndtv.com/india-news/significant-increase-in-cyber-crimes-against-women-during-lockdown-experts-2222352 (Last Modified July18, 2021).
15. Supra note 8 at 2.
16. Available at: https://www.business-standard.com/article/technology/india-becomes-favourite-destination-for-cyber-criminals-amid-covid-19-121040501218_1.html (Last Modified July 27, 2021).
17. Supra note 16.
18. Available at: https://www.unwomen.org/en/news/stories/2020/4/statement-ed-phumzile-violence-against-women-during-pandemic (Last Modified July 27, 2021).
19. Ibid.
20. Ibid.
21. Available at: https://www.youthkiawaaz.com/2020/06/increasing-cases-of-cyber-crimes-against-women/ (Last Modified July 27, 2021).