"LEGAL IMPLICATIONS OF CYBERSECURITY BREACHES IN INDIA: FRAMEWORKS AND LIABILITIES"

Author's Name – Kritin Sardana & Dikshant Sharma

ABSTRACT NOTE

This legal research note delves into the critical subject of the legal Implications of Cybersecurity Breaches in India, offering a comprehensive analysis of the existing legal frameworks and liability issues surrounding cybersecurity breaches and data breaches. The study explores the complexities organisations face in safeguarding personal and sensitive information, emphasising their responsibilities in upholding data protection standards. By examining relevant statutes, regulations, and judicial precedents, the note identifies key legal obligations, potential liabilities, and the impact on affected individuals. This study also addresses the liability issues organisations face in the event of cybersecurity breaches. It delves into the potential consequences organisations may encounter, such as penalties, fines, and reputational damage, for failing to protect personal and sensitive information adequately Furthermore, it investigates the evolving landscape of cybersecurity laws in India, considering recent developments and proposed reforms. The note also discusses the duty of care and fiduciary obligations that organisations owe to their customers and stakeholders in ensuring the security of data entrusted to them. To basically enclose this research in a nutshell, this research if divided into two parts where the legal framework regarding cyberspace is discussed with the responsibilities of organisations in safeguarding the data. This research note is a valuable resource for organisations seeking to comprehend and enter Indian Cyberspace by addressing the multifaceted challenges posed by cybersecurity breaches in the Indian context.

TABLE OF CONTENTS

RESEARCH METHODOLOGY

- **FUNDAMENTAL LEGAL ANALYSIS:** Fundamental legal analysis serves as a pivotal research method in the legal field. This approach involves dissecting legal principles, statutes, and precedents to comprehend the foundational aspects of a subject. By critically evaluating legal concepts, historical context, and judicial interpretations, researchers gain a comprehensive understanding. This method aids in crafting well-informed arguments, shaping legal reforms, and contributing to jurisprudential discussions, thereby playing a vital role in advancing the field of law.

- **DOCTRINAL LEGAL RESEARCH:** Doctrinal legal analysis, a core research method in law, involves scrutinizing legal principles, statutes, and case law. This method interprets and analyses existing legal materials to deduce principles and draw conclusions. By examining the evolution of legal concepts, it provides a solid foundation for legal research, enabling scholars to grasp the intricacies of legal doctrines and their application.

- **CONTENT ANALYSIS:** Content analysis, a vital research method in legal studies, involves systematic scrutiny of textual, visual, or audio materials to extract meaningful insights. In legal research, it aids in comprehending legal documents, statutes, case law, and public discourse. By categorizing and interpreting content, researchers discern patterns, trends, and attitudes. This method facilitates a nuanced understanding of legal concepts, societal perceptions, and legislative impacts, contributing to informed and comprehensive legal analyses.

RESEARCH QUESTIONS

1. What are the key legal frameworks in India governing cybersecurity breaches, and how do they address issues related to data breaches and the protection of personal and sensitive information?
2. How does the legal landscape in India define and attribute liability in cases of cybersecurity breaches, and what factors determine the responsibilities of organizations in safeguarding personal and sensitive data?

INTRODUCTION

In the case of ***WhatsApp LLC Vs. Competition Commission of India and Ors.*** while adjudicating Hon'ble Chief Justice of Delhi High Court S.C. Sharma gave an apt definition of how data is the new godsend for corporations. As to quote from the original judgement "By and large, to ensure retention of its user base and to prevent any other disruptive technology from entering the market, data is utilised by tech companies to customise and personalise their own platforms so that its userbase remains hooked. When data concentration is seen through this prism, it does give meaning to the new adage that **"data is the new oil"**.[1]

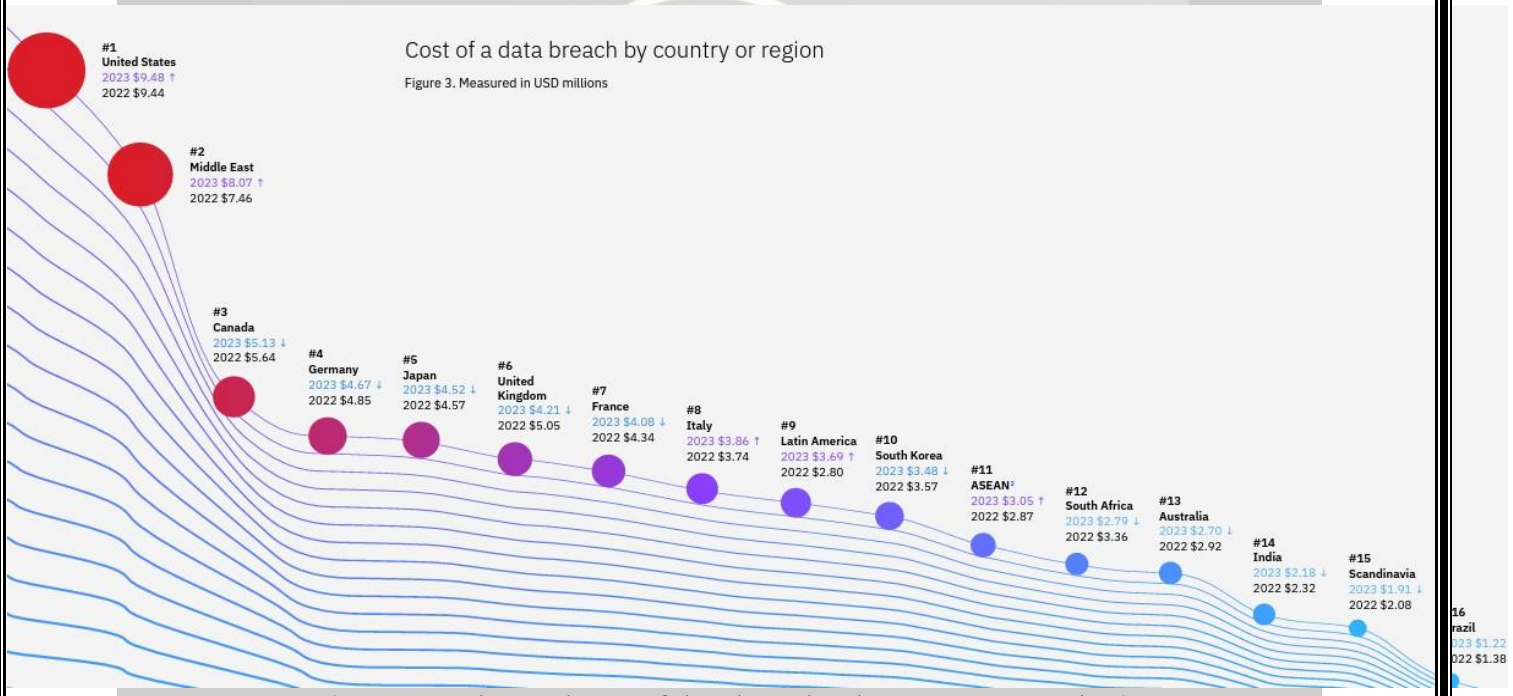
India being the vast entity it is with an ever-expanding digital database is a scrumptious marketplace to set foot in for multi-national & multi-lateral corporations but, along with it being a land of opportunity for these businesses, it is also the apple of the eye for cyberspace

[1] Whatsapp LLC vs. Competition Commission of India and Ors. 293 (2022) DLT 616.

exploiters. Alarmingly the extent of damages through data breaches and cyber hackings has been on the rise since the start of the century. Although after presenting the Digital Personal Data Protection (DPDP) Bill 2022, India has shown its seriousness towards the data of its citizens but has yet to completely pass any overachieving national law regarding the collection of personal data of its citizens. The personal data and the liability, if it is breached or compromised, is overlooked by a web of different laws and acts which construct the framework governing the protection of data in cyberspace.

In an article titled "Data Protection Laws and Regulations in India"[2] by Manisha Singh & Swati Mittal, it is mentioned that "In India, relevant government departments oversee the enforcement of data protection instead of a separate Authority. However, the draft DPDP Bill envisages setting up of a Data Protection Board of India (DPBI) to regulate the entire regime of digital personal data protection in the country."

As per a global report of IBM titled **Cost of Data Breach Report 2023**[2] India ranks 14th in the total cost of data breaches of countries at 2.32 million USD. The detailed global scenario per the report (Figure 1.) is mentioned below.



(Figure 1. The total cost of data breaches by country or region*)*

As per Data-monitoring Firm Surf shark's **Global Data Breach Stats**[3], which displays the page containing publicly available information about personal data that's been copied, transmitted, viewed, and stolen from data holders or otherwise illegally used since 2004, India has had a total of 292,052,503 breached accounts in public knowledge with an average of 21 accounts being breached out of every 100 accounts. The topmost leaked data point in India has been Password, according to the same detailed report. The Full Real-time Global

[2] Cost of Data Breach Report 2023 by IBM https://www.ibm.com/downloads/cas/E3G5JMBP (Accessed 4th August 2023).

[3] Global Data Breach Stats https://surfshark.com/research/data-breach-monitoring ("Data breach monitoring") (Accessed 5th August 2023).

Interactive Map of Surfshark Global Data Breach Stats can be accessed through <https://surfshark.com/research/data-breach-monitoring >. India has faced its fair share of data breaches in the past decade, with many government facilities and personal sensitive data being put at risk. Examples of organisations that have fallen vulnerable to cybersecurity breaches are SBI, JustDial, Unacademy, Bigbasket, Upstox-KYC hack, Air India (4.5 Lakhs accounts compromised), Covid report results of 1500 patients by the Indian Government and FireEye-Healthcare reports (68 lakh patients & doctors).

As per an article by Captain Sanjay Chabbra titled "INDIA'S NATIONAL CYBERSECURITY POLICY (NCSP) AND ORGANISATION: A CRITICAL ASSESSMENT [4]", the CERT-In, which is a response team and regulatory body of MeITY for computer emergencies, registered a total of 22060 attacks in the year 2012 [5]. In the latest Annual report 2021 [6] of CERT-IN, the total number of security incidents handled by CERT is 1402809. That's an increase of 63.59 times in less than a decade. As per CERT-IN's official annual report of 2021, "The types of incidents handled were Website intrusion & Malware propagation, Malicious Code, Phishing, Distributed Denial of Service (DoS) attacks, Website

Defacements, Unauthorized Network Scanning/Probing activities, Ransomware attacks, Data Breaches and Vulnerable Services." The detailed breakdown of security breaches and issues handled by CERT-IN is described in Figure 2 above.

In the case of ***Ajit Mohan and Ors. Vs. Legislative Assembly, National Capital Territory of Delhi and Ors***[7] which was a proceeding regarding the Delhi riots & summoning of Facebook Managing Director by the Peace and Harmony Committee of Delhi Legislative Assembly, the Hon'ble Supreme Court of India mentioned that ". A testament to the wide-ranging services which Facebook offers is the fact that it has about 2.85 billion monthly active users as of March 2021. This is over 1/3rd of the total population of this planet. In the national context, Facebook is the most popular social media platform in India with about 270 million registered users. **Such vast powers must necessarily come with responsibility. Entities like Facebook have to remain accountable to those who entrust them with such power.** While Facebook has played a crucial role in enabling free speech by providing a voice to the voiceless and a means to escape state censorship, we cannot lose sight of the fact that it has simultaneously become a platform for disruptive messages, voices, and ideologies. The successful functioning of a liberal democracy can only be ensured when citizens are able to make informed decisions. Such decisions have to be made keeping in mind a plurality of perspectives and ideas. The information explosion in the digital age is capable of creating new challenges that are insidiously modulating the debate on issues where opinions can be vastly divided. Thus, while social media, on the one hand, is enhancing equal and open dialogue between citizens and policymakers; on the other hand, it has become a tool in the hands of various interest groups who have recognised its disruptive potential. This results in a paradoxical outcome where extremist views are peddled into the mainstream, spreading

[4] *Captain Sanjay Chabbra* "India's national cybersecurity policy (NCSP) and organisation: a critical assessment" Naval War College Journal (55) (Accessed 5th August).
[5] Annual Report 2012 https://cert-in.org.in/s2cMainServlet?pageid=PUBANULREPRT (Accessed 4th August 2023).
[6] Annual Report 2021 https://cert-in.org.in/s2cMainServlet?pageid=PUBANULREPRT (Accessed 4th August 2023).
[7] *Ajit Mohan and Ors. Vs. Legislative Assembly, National Capital Territory of Delhi and Ors* AIR 2021 SC 3346.

misinformation. Established independent democracies are seeing the effect of such ripples across the globe and are concerned. Election and voting processes, the very foundation of a democratic government, stand threatened by social media manipulation. This has given rise to significant debates about the increasing concentration of power in platforms like Facebook, more so as they are said to employ business models that are privacy-intrusive and attention soliciting."

ANALYSING THE LEGAL FRAMEWORK & LIABILITY ISSUES BY OVERVIEWING LAWS GOVERNING THE CYBERSECURITY and DATA BREACH REALM IN INDIA.

1.1) THE INFORMATION TECHNOLOGY ACT, 2000

The IT Act 2000 is tagged as India's first-ever landmark cybersecurity law. With its scope being as wide as defining different types of data & resources to creating governing bodies & penalising cyber offences. Here are some specific provisions dealing with data breaches and other such issues which hold the wrongdoer liable.

● The Section 43 of IT Act, 2000 mentions the, [Penalty and compensation] for damage to computer, computer system, etc.[8]

Section 43 provides for the liability & compensation of several types of data breaches of individual or common entities by payment of damages by compensation to the person affected.[9]

Section 66 of the IT Act 2000 says that "If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to *three years* or with fine which may extend to *five lakh rupees* or with both."[10]

As per an article titled 'Offences and Penalties under Information Technology Act, 2000'[11], the IT Act 2000, sections ranging from *Section 65 to Section 76* provide different types of offences and their penalties. To look at some relevant ones regarding data breaches and cyberspace.

- As per **Section 72** of the IT Act 2000, "**Penalty for Breach of confidentiality and privacy.**–Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic

[9] Section 43, *THE INFORMATION TECHNOLOGY ACT, 2000* https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfv sbdihbgfGhdfgFHytyhRtMjk4NzY= (Accessed 3rd August 2023).

[10] Section 66, *THE INFORMATION TECHNOLOGY ACT, 2000* https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfv sbdihbgfGhdfgFHytyhRtMjk4NzY= (Accessed 3rd August 2023).

[11] Deepak Joshi, Offences and Penalties under Information Technology Act, 2000, 11 march 2019. https://taxguru.in/corporate-law/offences-penalties-information-technology-act-2000.html (Accessed 3rd August 2023).

record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to *two years*, or with fine which may extend to *one lakh rupees*, or with both."[12]The section 72 provides a penalty for the basic construe of data & privacy breaches under the IT Act.

- **Section 45** of the IT Act 2000 gives the residuary power to the adjudicating body, which can hold any party breaching any provision of the act liable, saying that " **Residuary penalty**.–Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding *twenty-five thousand rupees* to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees. "[13]

- **Section 64** of the IT Act 2000 says, "**Recovery of penalty or compensation**. –A [penalty imposed or compensation awarded] under this Act if it is not paid, shall be recovered as an *arrear of land revenue* and the licence or the [electronic signature] Certificate, as the case may be, shall be suspended till the penalty is paid."[14] Therefore, if any liable party refuses to pay damages or compensation, it can be recovered in other ways as arrears of land revenue or penalty of suspension of digital signature licence can be done till the liable party pays damages.

- Section 75 of the IT Act 2000 makes any wrongdoer liable to the provisions of this act by saying, "Act to apply for offence or contravention committed outside India.[15]Therefore, any International or Multi-National company can be held liable through this provision in case of involvement in cyber offences or cybersecurity breaches.

The **Chapter XII** of the IT Act 2000 provides an exemption from liability of intermediaries in certain cases. Firstly to understand what an Intermediary is we refer to the **Section 2(1)(w),** which defines "**intermediary** , with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes."

[12] Section 72, *THE INFORMATION TECHNOLOGY ACT, 2000* https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfv sbdihbgfGhdfgFHytyhRtMjk4NzY= (Accessed 3rd August 2023).

[13] Section 45, *THE INFORMATION TECHNOLOGY ACT, 2000.* https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfv sbdihbgfGhdfgFHytyhRtMjk4NzY= (Accessed 3rd August 2023).

[14]Section 64, *THE INFORMATION TECHNOLOGY ACT, 2000.* https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfv sbdihbgfGhdfgFHytyhRtMjk4NzY= (Accessed 3rd August 2023).

[15]Section 75, *THE INFORMATION TECHNOLOGY ACT, 2000* https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfv sbdihbgfGhdfgFHytyhRtMjk4NzY= (Accessed 3rd August 2023).

- Now **Section 79** defines the "**Exemption from liability of intermediary in certain cases**. –

In the case of ***Myspace Inc. Vs Super Cassettes Industries Ltd.***[16], it was held, "both under Copyright Act and Information Technology Act, 2000/IT Act, "actual" knowledge and not just suspicion is essential to fasten liability."

It was also particularly mentioned that "Appellant falls within Section 2(1)(w) of IT Act, and qualifies as an intermediary/Internet service provider because it acts as a "conduit"/portal for information where users can upload and view content. It acts as a service provider by allowing users to upload, stream, share and view content which it hosts. MySpace clearly places an embargo on its users from uploading content in which they do not possess relevant rights and at same time gives content owners option of notifying them in event that they find content hosted on its website is without due license. It claims immunity from liability, as an intermediary following due diligence as well complying with provisions of Section 79 of IT Act. Under circumstances, it is difficult to conceive how one would pose a barrier in applicability of other. Further true intent of Section 79 of IT Act, is to ensure that in terms of globally accepted standards of intermediary liabilities and to further digital trade and economy, an intermediary is granted certain protections. Section 79 of IT Act, is neither an enforcement provision nor does it list out any penal consequences for noncompliance. It sets up a scheme where intermediaries have to follow certain minimum standards to avoid liability; it provides for an affirmative defence and not blanket immunity from liability". Now as to move forward to the liability of a company or corporation entering the Indian Cyberspace, Section 85 of the IT Act 2000 governs and provides for who will be held liable if a 'Company' commits offences.[17]

Therefore, if a data breach or cyber offence takes place through a 'body corporate', every person at the time of the contravention who was in charge of the functioning of the company, including the director, manager, secretary or any other officer of the corporation.

- **The Cyber Regulations Appellate Tribunal (CRAT)**[18] was formed under **Section 48** of the IT Act firstly as 'Appellate Tribunal', which was later substituted by the Finance Act 2017 [19] by **Section 169** into **'Cyber Appellate Tribunal'** with its major role being present as an appellate ground for a person aggrieved by the orders of an adjudicating officer.

1.2) THE INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008

The IT (Amendment) Act 2008, a crucial piece of legislation in India, introduced notable features to strengthen the country's cybersecurity and data protection framework. It expanded

[16] Myspace Inc. Vs Super Cassettes Industries Ltd. 236 (2017) DLT478.
[17] Section 85, *THE INFORMATION TECHNOLOGY ACT, 2000* https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfv sbdihbgfGhdfgFHytyhRtMjk4NzY= (Accessed 3rd August 2023).
[18] https://www.meity.gov.in/content/ministry-law-justice-and-company-affairs-legislative-department-0 ("Ministry of Law, Justice and Company Affairs (Legislative Department) | Ministry of Electronics and Information Technology, Government of India") (Accessed 3rd August 2023).
[19] (Sec. 169) "THE FINANCE ACT, 2017 NO. 7 OF 2017 An Act to give effect to the financial proposals of the Central Government for the financia." *Ministry of Civil Aviation*, http://www.civilaviation.gov.in/sites/default/files/MoL%26amp%3BJ%20%28Legislative%20Deptt%29%20The%20F inance%20Act%20.pdf. (Accessed 3 August 2023).

the definition of "cybercrime" and empowered authorities to prosecute offenders effectively. The act mandated data protection measures, compelling companies to implement reasonable security practices to safeguard sensitive information. It granted power to the Indian Computer Emergency Response Team (CERT-In) to handle cybersecurity incidents and coordinate response efforts. Additionally, the act introduced stringent penalties for various offences, aiming to deter cybercriminals. These salient features aimed to fortify India's digital landscape and protect individuals and organisations from cyber threats.

Section 43 of the IT Act 2000 provided for the liability & compensation of several types of data breaches of individual or common entities by payment of damages by way of compensation to the person so affected, but the insertion of a new section, namely **Section 43(A)** for describing the compensation that is to be paid the liable party who fails to protect data.

- **Section 43(A)** of the IT Act 2000 is a provision which targets compensation if an entity fails to protect data & thus causes a cybersecurity breach.[20] This particular section 43A gave an explanation for the word 'Body Corporate' engulfing companies and corporations into the ambit of liability if involved in cyber offences and data breaches. The maintenance of reasonable security practices and procedures was also made mandatory for body corporates by this insertion in the IT Act 2000.

- Insertion of new sections namely **Section 70(A) for** "**National nodal agency** [21] which gave birth to the National Nodal Agency of India known as the **National Critical Information Infrastructure Protection Centre (NCIIPC),** which itself mentions that "National Critical Information Infrastructure Protection Centre (NCIIPC) is an organisation of the Government of India created under Sec 70A of the Information Technology Act, 2000 (amended 2008), through a gazette notification on 16th Jan 2014 based in New Delhi, India. It is designated as the National Nodal Agency in respect of Critical Information Infrastructure Protection" [22] The **Critical Information Infrastructure** is defined briefly as, "Under IT Act, 2008, Critical Information Infrastructure is a computer resource, whose incapacitation or destruction shall have a deep impact on national security, economy, public health, or safety."[23] **Also, Section 70(B)- "Indian Computer Emergency Response Team to serve as national agency for incident response.**[24]

Indian Computer Emergency Response Team: CERT-IN[25]

[20] Section 43(A) "*THE INFORMATION TECHNOLOGY (AMENDMENT) ACT 2008*" https://www.meity.gov.in/writereaddata/files/itact2000/it_amendment_act2008.pdf (Accessed 3rd August 2023).
[21] Section 70(A) "*THE INFORMATION TECHNOLOGY (AMENDMENT) ACT 2008*" https://www.meity.gov.in/writereaddata/files/itact2000/it_amendment_act2008.pdf (Accessed 3rd August 2023).
[22] "National Critical Information Infrastructure Protection Centre (NCIIPC)".
[23] *Siq, Manish*. "Critical Information Infrastructure News Articles." *Study IQ*, 9 November 2022, https://www.studyiq.com/articles/critical-information-infrastructure/. (Accessed 3 August 2023).
[24] **Section 70(B)** "*THE INFORMATION TECHNOLOGY (AMENDMENT) ACT 2008*" https://www.meity.gov.in/writereaddata/files/itact2000/it_amendment_act2008.pdf (Accessed 3rd August, 2023)
[20] Indian - Computer Emergency Response Team, https://cert-in.org.in/s2cMainServlet?pageid=PUBWEL01. (Accessed 3 August 2023).
[25] Information Technology (Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013." *MeitY*, https://www.meity.gov.in/writereaddata/files/G_S_R%2020%20(E)2_0.pdf . (Accessed 3 August 2023).

Functioning under the Information Technology (Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013, the main functions that CERT-IN performs are:

1. "CERT-In is an acronym for 'Indian Computer Emergency Response Team'. CERT-In is the National Incident Response Centre for major computer security incidents in its constituency i.e., Indian cyber community.
2. CERT-In's primary role is to raise security awareness among the Indian cyber community and to provide technical assistance and advise them to help them recover from computer security incidents.
3. CERT-In provides technical advice to System Administrators and users to respond to computer security incidents. It also identifies trends in intruder activity, works with other similar institutions & organisations to resolve major security issues, and disseminates information to the Indian cyber community.
4. CERT-In also enlightens its constituents about the security awareness and best practices for various systems; networks by publishing advisories, guidelines and other technical documents"[26].

Another major function that CERT-IN performs is the formulation of **The Cyber Crisis Management Plan (CCMP)**[27] for Countering Cyber Attacks, and Cyber Terrorism is a framework document for dealing with cyber-related incidents.

CERT-IN on 28 April 2022 issued directions under the IT Act relating ("Directions")[28]. As per an article published in Linklaters, "These Directions are effective from 27 June 2022, 60 days from the date of its issuance. One of the most significant obligations imposed by the Directions is the obligation to mandatorily report identified cyber incidents to CERT-IN within six hours."

1.3) RESERVE BANK OF INDIA ACT 1934.

The breach of data or cybersecurity breach of any information held under the RBI Act is imposed as a liability on the person that discloses such confidential information.

The **Section 58B (4)**[29] of the Reserve Bank of India Act 1934 provides the "penalty if any person/company discloses any credit information, the disclosure of which is prohibited under section 45E (**Section 45E** provides for the prohibition of discloser of any credit information contained in any statement submitted by a banking company under section 45C or furnished by the Bank to any banking company under section 45D, shall be treated as confidential and shall not, except for the purposes of this Chapter, be published or otherwise disclosed), he shall be punishable with imprisonment for a term, which may extend to six months, or with fine, which may extend to one thousand rupees, or with both. **Section 58C** applies these same provisions of penalties to offences by a company in a similar manner to Section 85 of the IT Act 2000.

[26] https://cert-in.org.in/s2cMainServlet?pageid=WHATWELIST.
[27] CCMP, May 4, 2023, https://cert-in.org.in/s2cMainServlet?pageid=CCMP (Accessed 3rd August 2023).
[28] www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf ("Page 1 of 8 No. 20(3)/2022-CERT-In Government of India Ministry of Electronics and Information Technology (MeitY) Indian Compute") (Accessed 3rd August 2023).
[29] Section 58B (4), "*Reserve Bank of India Act 1934*" https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/RBIA1934170510.PDF (Accessed 3rd August 2023).

1.4) THE CREDIT INFORMATION COMPANIES (REGULATION) ACT, 2005

Section 20 of the CICRA 2005 provides for privacy rules that every credit information company, credit institution and specified user, shall adopt for collection, processing, collating, recording, preservation, secrecy, sharing and usage of credit information.

Section 22 of the CICRA 2005 prohibits unauthorized access to credit information held by credit information companies, credit institutions, or specified users. Violators can face fines of up to one lakh rupees for each offense, and if the unauthorized access persists, an additional fine of up to ten thousand rupees per day may be imposed. Unauthorized credit information cannot be used for any purpose.[30]

1.5) THE DIGITAL PERSONAL DATA PROTECTION BILL, 2022

The DPDP Bill 2022[31] is a positive step presented by the MeITY for providing of protection of personal data present digitally from the breach. Some salient features which will empower the legal framework regarding the cybersecurity and personal data of Indian citizens present in the cyberspace are:

- General obligations & additional obligation of Data Fiduciary under **Section 9,10 & 11** of DPDP Bill, 2022 (According to **Section 2(5)** "**Data Fiduciary** means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data")
- Right to information about personal data (**Section 12**), Right to correction and erasure of personal data (**Section 13**), Right of grievance redressal (**Section 14**) & Right to nominate (**Section 15**) given to Data Principal (According to **Section 2(6)** "Data Principal means the individual to whom the personal data relates and where such individual is a child includes the parents or lawful guardian of such a child")
- Creation of **Data Protection Board of India** under **Section 19.**
- **Section 24** grants the power to the board to accept any voluntary undertaking in respect of any matter related to compliance with provisions of this Act from any person at any stage. As per **Section 24 (4)** "Where a person fails to comply with any term of the voluntary undertaking accepted by the Board, the Board may, after giving such person, a reasonable opportunity of being heard, proceed in accordance with section 25 of this Act."
- **Section 25** provides for the **Financial Penalty,** saying that "If the Board determines on conclusion of an inquiry that non-compliance by a person is significant, it may, after giving the person a reasonable opportunity of being heard, impose such financial penalty as specified in Schedule 1, not exceeding rupees five hundred crore in each instance."

[30] Section 22, "*THE CREDIT INFORMATION COMPANIES (REGULATION) ACT, 2005 ARRANGEMENT OF SECTIONS"* https://financialservices.gov.in/sites/default/files/CIC%20Act%202005.pdf (Accessed 3rd August 2023).

[31] (MeITY), "The Digital Personal Data Protection Bill, 2023." *PRS Legislative Research*, 29 July 2023, https://prsindia.org/files/bills_acts/bills_parliament/2023/Digital%20Personal%20Data%20Protection%20Bill,%202 023.pdf. (Accessed 4 August 2023).

As of 3rd August 2023, the MeITY has presented the Digital Personal Data Protection Bill, 2023 in the Lok Sabha for assent. The 500 Cr. penalty cap has been removed in this version of the DPDP Bill.

RESPONSIBILITY OF THE ORGANISATION IN SAFEGUARDING PERSONAL AND SENSITIVE INFORMATION

In the case of ***'X' Vs. Union of India and Ors.***[32] , which was a case where data was breached from private Instagram & Facebook accounts and published on a pornographic website, it was held that "if the intermediary fails to fulfil the conditionalities and obligations cast upon it, both in the positive and in the negative, as set out above, such intermediary is liable to forfeit the exemption from liability available to it under section 79(1) of the IT Act."

Para 86 of the said judgement gave an insight into the liability of an intermediary regarding the data of Indian citizens as "**86**. While appreciating the indisputably anarchic nature of the internet as a medium and accepting that the world-wide-web is intractable by reason of its global expanse, interconnectedness and the fact that content, including offending content, can be very easily placed on the world-wide-web by people from the farthest corners of the world, which it is almost impossible to control, it cannot be ignored that the law and judicial opinion in India as also in several other jurisdictions, as gathered from the foregoing discussion, **mandates intermediaries to remove and disable access to offending content once they receive 'actual knowledge' by way of a court order or upon being notified by the appropriate government or its agency, failing which the intermediary is liable to lose the exemption from liability available to it under section 79(1) of the IT Act.** "

The Delhi High Court also directed that " A direction is issued to the search engines Google Search, Yahoo Search, Microsoft Bing and Duck Duck Go, to globally de-index and de-reference from their search results the offending content as identified by its Web URL and Image URL, including de-indexing and de-referencing all concerned web-pages, sub-pages or sub-directories on which the offending content is found, forthwith and in any event within 24 hours of receipt of a copy of this judgment along with requisite information from the Investigating Officer as directed below;" thus making it intermediary's liability to look after the aftermath of data breach from their platforms.

This above judicial precedent is a befitting example of how organisations working in the cyberspace with the data of Indian citizens are responsible for safeguarding the same in the event of breaches or other offences. With these judicial precedents, many acts and rules have been posited by the authorities making data handlers, body corporates, data fiduciaries, intermediaries, CISOs, organisational managers and many other such people responsible for safeguarding personal & sensitive information and also liable for cases of lapses in security.
Some major statutes regarding this are: -

[32] 'X' Vs. Union of India and Ors. 2021 IVAD (Delhi) 28.

3.1) INFORMATION TECHNOLOGY (REASONABLE SECURITY PRACTICES AND PROCEDURES AND SENSITIVE PERSONAL DATA OR INFORMATION) RULES, 2011 (PRIVACY RULES). [33]

As per the powers conferred to the central government to make rules regarding the IT Act 2000 under clause (ob) of subsection (2) of section 87 read with section 43A of the Information Technology Act, 2000 (21 of 2000), the **Information Technology (Reasonable Security Practices And Procedures And Sensitive Personal Data Or Information) Rules, 2011 (Privacy Rules)** were made to ensure that a data handler of an Indian citizen is responsible for maintaining a certain standard of security and reasonable protection of the entrusted sensitive and personal data. Some of the salient rules of this statute are:

- **Rule 4** provides for every Body corporate that collects, receives, possesses, stores, deals or handles information of provider of information to provide policy for privacy and disclosure of information.
- **Rule 5 (4),** which is regarding the collection of data by a body corporate, says that "Body corporate or any person on its behalf holding sensitive personal data or information shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force."
- **Rule 6(1)** makes it mandatory to have permission from the data provider first to share such information. **Rule 6** goes as "**Disclosure of information. —** (1) Disclosure of sensitive personal data or information by body corporate to any third party shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise, unless such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation". **Clause 3 of this Rule 6** says, "The body corporate or any person on its behalf shall not publish the sensitive personal data or information".
- **Rule 3** of these rules defines the Sensitive Personal Data or Information (SPDI) as "Sensitive personal data or information of a person means such personal information which consists of information relating to; — **(i)** password;
  - **(ii)** financial information such as Bank account or credit card or debit card or other payment instrument details;
  - **(iii)** physical, physiological and mental health condition;
  - **(iv)** sexual orientation;
  - **(v)** medical records and history;
  - **(vi)** Biometric information;
  - **(vii)**any detail relating to the above clauses as provided to body corporate for providing service; and
  - **(viii)** any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:"

The liability clause under the IT (RSPP and SDPI) Rules 2011 can be marked as the **Rule 8 (1)** which says that " A body corporate or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security

[33] "INFORMATION TECHNOLOGY (REASONABLE SECURITY PRACTICES AND PROCEDURES AND SENSITIVE PERSONAL DATA OR INFORMATION) RULES, 2011" *MeitY*, https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf (Accessed 3 August 2023).

programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business. In the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies." Therefore, after a security breach, it is the duty of the corporate body or the person to show that RSPP were deployed and due diligence was done otherwise, he/she/they will be held liable for such lapse in security.

- **Rule 8(4)** requires the body corporate or a person to have "The audit of reasonable security practices and procedures shall be carried out by an auditor at least once a year or as and when the body corporate or a person on its behalf undertake significant upgradation of its process and computer resource."

Therefore, The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, commonly known as Privacy Rules, outline guidelines for organizations handling sensitive personal data. These rules establish standards for data protection, mandating reasonable security practices to ensure the privacy and security of individuals' sensitive information in India's digital landscape.

3.2) INFORMATION TECHNOLOGY (INTERMEDIARY GUIDELINES AND DIGITAL MEDIA ETHICS CODE) RULES, 2021. [34]

As per **Section 2(1)w** of the **IT Act 2000, "intermediary",** with respect to any particular electronic records, means any person who, on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes;]**".**

Now, the **INFORMATION TECHNOLOGY (INTERMEDIARY GUIDELINES AND DIGITAL MEDIA ETHICS CODE) RULES, 2021** makes rules for the diligence of an intermediary while handling data for any reason, thus making him liable for any losses and breaches.
Rule 3(1) of the abovementioned rules makes it a duty of an intermediary to perform due diligence in a specified manner. **Rule 3(2)** makes it a responsibility of an intermediary to set up a grievance redressal mechanism for people affected, and the intermediary shall employ every feasible and reasonable step to eliminate or deactivate access to content that is hosted, stored, disseminated, or transmitted through its platform within 24 hours of the publishing of the complaint.

[34]KUMAR, ALOK. "MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY NOTIFICATION New Delhi, the 25th February, 2021 G.S.R. 139(E). —In exercise." *Ministry of Information and Broadcasting*, 25 February 2021, https://mib.gov.in/sites/default/files/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20 Code%29%20Rules%2C%202021%20English.pdf. (Accessed 3 August 2023).

Under **Rule 4(a),** a **Chief Compliance Officer** is to be appointed "who shall be responsible for ensuring compliance with the Act, and rules made thereunder and shall be liable in any proceedings relating to any relevant third-party information, data or communication link made available or hosted by that intermediary where he fails to ensure that such intermediary observes due diligence while discharging its duties under the Act and rules made thereunder."

Under **Rule 4(b),** a **nodal contact person** must be appointed "for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders or requisitions made in accordance with the provisions of law or rules made thereunder."

Under the **Rule 4(c)** the intermediary must "appoint a **Resident Grievance Officer,** who shall, subject to clause (b), be responsible for the functions referred to in sub-rule (2) of rule 3." Clause (b) in sub-rule (2) of rule 3 is for the grievance redressal mechanism's reporting within 24 hours, and therefore he/she should be an Indian resident.

As previously discussed, an intermediary is protected from action under **Section 79(1)** of the IT Act, 2000, but **Rule 7** of the Intermediary guidelines says that "**Non-observance of Rules.** —Where an intermediary fails to observe these rules, the provisions of sub-section (1) of section 79 of the Act shall not be applicable to such intermediary and the intermediary shall be liable for punishment under any law for the time being in force including the provisions of the Act and the Indian Penal Code."
Therefore, if there is non-compliance with these intermediary guidelines and rules, it makes an intermediary liable for action in regards to safeguarding data it handles.

A major case which developed clarity regarding the intermediary's responsibility in case of IP violation and copyright infringement is ***Neetu Singh and Ors. Vs. Telegram FZ LLC and Ors.***[35] 2023 (93) PTC 515 (Del) which was a case of Intellectual Property & Copyright infringement and dissemination of plaintiff's copyright work. The issue of this case, as per the judgement by the Delhi High Court, was "The short but vexed legal issue that is to be decided in I.A. 8461/2020 is whether Telegram can be directed to disclose the identity of the creators of the infringing channels which unauthorisedly and illegally disseminate the Plaintiffs' copyrighted works." While adjudicating this case, the Hon'ble court said that "In respect of Telegram's data centre being located in Singapore and it being unable to disclose the details of the devices used, mobile number used, IP addresses etc., of the infringers - It is a fact of which judicial notice can be taken that Telegram is one of the most popular messaging applications in India. Its subscription base runs into millions of users and by merely locating its servers abroad, it cannot escape the rigours of orders passed by competent Courts in India. Indian courts would be the natural forum of jurisdiction in this dispute." Therefore, Indian Courts hold jurisdiction over organisations situated or registered outside of India but working concerning Indian databases. There are several tests like the effect test, purposeful availment test, zippo test or minimum contact tests, which are used for determining the jurisdictional matters of Indian courts regarding companies situated outside of India.
The Hon'ble Delhi High Court, in this case, held that "In view of the above factual and legal position, in the opinion of this Court, merely because Telegram chooses to locate its server in Singapore, the same cannot result in the Plaintiffs' - who are copyright owners of course materials - being left completely remediless against the actual infringers, especially in order to claim damages and avail of other legal remedies in accordance with the law. In the facts and circumstances of the present case, Telegram-Defendant No. 1 is directed to disclose the details

[35] Neetu Singh and Ors. Vs. Telegram FZ LLC and Ors.[35] 2023 (93) PTC 515 (Del).

of the channels/devices used in disseminating the infringing content, mobile numbers, IP addresses, email addresses, etc., used to upload the infringing material and communicate the same, as per the list of channels filed along with the present application."[36]This caselaw is a fitting example of how intermediaries are to be held accountable and put to work in cases of data breaches or misuses.

3.3) CISO- Roles & Responsibilities[37]

- CISO stands for **Chief Information Security Officers,** which are to be appointed in every Ministry/Department/Organisation.
- CISOs are liable in organisations to identify and implement an '**Information Security Management System (ISMS)'.**
- CISO is responsible for the "**Vulnerability Assessment & Penetration Testing (VAPT)** of all websites, portals and IT systems, on a quarterly basis at a minimum; ensuring that websites are GIGW compliant." GIGW stands for the Guidelines for Indian Government Websites [38].
- CISO needs to perform **Web Application Security Assessment (WASA)** and white-listing of all web applications in use by the organisation, annually at a minimum.
- CISO has a duty to do the **Software Development Lifecycle (SDLC) Audit** and periodic Code Reviews to ensure that applications continue to be secure.
- As per the above-mentioned notification defining the CISOs roles and responsibilities, he has to perform an **Information Security Audit** of IT Systems and controls, including site audits as appropriate, where online operations span multiple locations.
- The same notice defining CISOs roles and responsibilities requires a CISO to "Establishing a **Cyber Crisis Management Group** with the head of organisation (or his appointed representative) as its chairman and to prepare a list of contact persons to be contacted during crisis e.g., internal: financial, personnel etc. and external: law enforcement agencies, CERT-In etc. complete with up-to-date contact details. CCMG should authorise a **Cyber Crisis Management Plan (CCMP)** outlining roles and responsibilities of organisational stakeholders. Implementing the CCMP, including security best practices and specific action points."

As per an article titled **Cybersecurity litigation risks: 4 top concerns for CISO**[39], "The risk of litigation is not limited to corporations. CISOs themselves face being subject to legal action for breach of duty where insufficient steps were taken to prevent a breach, or the aftermath of the breach was handled badly, says Simon Fawell, partner at Signature Litigation LLP." He adds that "The role of the CISO has never been more critical for mid/large enterprises, and potentially more in the crosshairs and held accountable for security incidents and data breaches, as illustrated by the ongoing class action against SolarWinds' CISO and other executives following the devastating supply chain attack in 2020." Therefore, a CISO is also liable for safeguarding personal and sensitive information.

[36] Neetu Singh and Ors. Vs. Telegram FZ LLC and Ors. 2023(93) PTC 515 (Del).
[37] CERT-IN Notif No. 6 (12)/ 2017-PDP-CERT-In, "MeITY", 14/03/2017, www.meity.gov.in/writereaddata/files/CISO_Roles_Responsibilities.pdf (Accessed at 4th August, 2023).
[38] Guidelines for Indian Government Websites (GIGW) | India, https://guidelines.india.gov.in/. (Accessed 5 August 2023).
[39] *Hill, Michael*. "Cybersecurity litigation risks: 4 top concerns for CISOs." *CSO Online*, 19 April 2022, https://www.csoonline.com/article/572499/cybersecurity-litigation-risks-on-the-rise-what-cisos-should-worry-abo ut-the-most.html. (Accessed 5 August 2023).

CONCLUSIVE REMARKS

The complex legal landscape of cybersecurity breaches in India highlights the need for a flexible legal framework. Key legislations, primarily the Information Technology Act of 2000, provide a foundation for addressing cybercrimes and data breaches while balancing digital security and individual privacy rights. Determining liability for individuals and organizations is challenging due to evolving cyber threats and relies heavily on judicial interpretations. Organizations must meet "reasonable security practices" standards, yet the lack of universal guidelines complicates safeguard assessments. Collaboration among government, private sector, and individuals is essential for creating a cohesive legal ecosystem. Ultimately, this inquiry explores the intricate web of legal ramifications tied to cybersecurity breaches and emphasizes the need to harmonize legal, technological, and ethical considerations for a secure digital future in India.

SUMMARY

The legal implications of cybersecurity breaches in India revolve around establishing resilient frameworks and addressing liabilities. India's legal landscape combines the Information Technology Act of 2000 and its amendments to tackle cybercrimes and data breaches while preserving individual privacy rights. However, the evolving nature of cyber threats necessitates ongoing legal adaptability. Determining liability for individuals and organizations remains complex and largely dependent on judicial interpretations. To enhance this framework, several key improvements are essential:

1. Regularly updating legislation to keep pace with evolving technology and emerging threats.
2. Developing standardized guidelines for "reasonable security practices" to help organizations gauge the adequacy of their safeguards.
3. Encouraging a collaborative approach involving government bodies, private enterprises, and individuals to foster a synchronized legal ecosystem.

4. Promoting public awareness and education initiatives to emphasize the importance of cybersecurity practices and the potential consequences of oversight.
5. By addressing these aspects and harmonizing legal, technological, and ethical considerations, India can better protect personal and sensitive information in the digital age and uphold privacy, innovation, and the rule of law.

BIBLIOGRAPHY

1. LEGISLATIVE MATERIAL

- THE INFORMATION TECHNOLOGY ACT, 2000
- THE FINANCE ACT 2017
- THE INFORMATION TECHNOLOGY (AMENDMENT) ACT 2008
- RESERVE BANK OF INDIA ACT 1934
- THE CREDIT INFORMATION COMPANIES (REGULATION) ACT, 2005
- THE DIGITAL PERSONAL DATA PROTECTION BILL, 2022
- THE DIGITAL PERSONAL DATA PROTECTION BILL, 2023 (Draft)

- INFORMATION TECHNOLOGY (REASONABLE SECURITY PRACTICES AND PROCEDURES AND SENSITIVE PERSONAL DATA OR INFORMATION) RULES, 2011 (PRIVACY RULES).
- INFORMATION TECHNOLOGY (INTERMEDIARY GUIDELINES AND DIGITAL MEDIA ETHICS CODE) RULES, 2021.
- CISO- Roles & Responsibilities (Notification)

2. BOOKS

- DUGGAL, PAVAN. CYBER LAW 3.0: AN EXHAUSTIVE SECTION-WISE COMMENTARY ON THE INFORMATION TECHNOLOGY ACT ALONG WITH RULES, REGULATIONS, POLICIES, NOTIFICATIONS, ETC. Universal Law Publishing, 2018.

3. ARTICLES & BLOGS

- Manisha Singh & Swati Mittal, Data Protection Laws and Regulations in India, https://iclg.com/practice-areas/data-protection-laws-and-regulations/india (Singh and Mittal) (accessed on 4th August 2023).
- *Captain Sanjay Chabbra* "India's national cybersecurity policy (NCSP) and organisation: a critical assessment" Naval War College Journal (55).
- Deepak Joshi, Offences and Penalties under Information Technology Act, 2000, 11 march 2019 https://taxguru.in/corporate-law/offences-penalties-information-technology-act-2000.html (Accessed 3rd August 2023).
- Siq, Manish. "Critical Information Infrastructure News Articles." *Study IQ*, 9 November 2022, https://www.studyiq.com/articles/critical-information-infrastructure/. (Accessed 3 August 2023).
- Christopher, Deepa, et al. "India - A new and onerous cyber security framework, with breach reporting obligations." *Linklaters*, 25 May 2022, https://www.linklaters.com/en/insights/blogs/digilinks/2022/may/india-new-and-onerous-cybersecurity-framework-and-breach-reporting-obligations. (Accessed 3 August 2023).
- Hill, Michael. "Cybersecurity litigation risks: 4 top concerns for CISOs." *CSO Online*, 19 April 2022, https://www.csoonline.com/article/572499/cybersecurity-litigation-risks-on-the-rise-what-cisos-s hould-worry-about-the-most.html. (Accessed 5 August 2023).

4. LIST OF CASES

- Whatsapp LLC Vs. Competition Commission of India and Ors. 293(2022) DLT 616.
- Ajit Mohan and Ors. v. Legislative Assembly, National Capital Territory of Delhi and Ors AIR 2021 SC 3346.
- Myspace Inc. Vs Super Cassettes Industries Ltd. 236 (2017) DLT 478.
- 'X' Vs. Union of India and Ors. 2021 IVAD (Delhi) 28
- Neetu Singh and Ors. Vs. Telegram FZ LLC and Ors. 2023 (93) PTC 515 (Del).