CHANAKYA LAW REVIEW (CLR)

Vol VI, Issue I January- June, 2025 pp. 14-37

DATA GOVERNANCE IN DATA-DRIVEN COMPANIES' DECISION-MAKING: BALANCING PRIVACY CONCERNS, LEGAL OBLIGATIONS AND DIRECTORIAL LIABILITY

Akriti Trivedi [1]

Anushka Rohilla [2]

ABSTRACT

"*Data is useful only when it is protected and its context, content, and quality can be trusted". Through the processes of gathering, organising, and analysing data, information has become a valuable asset that helps businesses compete and operate more quickly in a global marketplace. 48.5% of respondents to a 2021 poll of Fortune 1000 businesses stated that they base their innovations on data. Additionally, by employing structures to manage data, data-driven firms are optimising growth strategies and process flows. It is a crucial procedure for every firm trying to obtain a competitive advantage in the market nowadays. But only if you can manage these data assets well, which necessitates a data governance framework, can you leverage them for digital transformation. Firstly, the authors have attempted to outline a data-driven decision-making process by analysing the various facets of the process of incorporation of data into decision-making, the benefits of the same, etc. Secondly, the importance of data privacy in a data governance structure has been emphasised upon, bringing to light the issues that come up with the mining of personal data. In the second part, the existing governance regime has also been scrutinised to provide for the results and liability in the event of a breach of data. Furthermore, whether data breach can be considered a corporate breach, has been deliberated upon. Thirdly, the authors have analysed directorial liability when it comes to such breaches in data-driven companies, by the analysis of the existing regime and other considerations attached therewith. Lastly, a workable framework has been provided for by the authors, to account for such concerns and liabilities in the instance of a data breach.*

[1] Student NLU, Jodhpur.
[2] Student NLU, Jodhpur.

***Key Words**: Personal Data, Directorial Liability, Privacy, Data Breach*

The Following are the tentative research questions sought to be answered:

1. How is data incorporated in decision making of a company?
2. What are the primary concerns with the increased mining of personal data with respect to the governance structure? Moreover, can the data breach be regarded as a corporate fraud?
3. What could be the possible legal regime concerning the liability in case of a data breach?
4. What should be the governance structure of a company vis'-a-vis' protection of personal data?

INTRODUCTION

The importance of data as an asset becomes significantly clear when the historical concept of Highest Paid Person's Opinion (HiPPO) comes in picture. When HiPPO is in operation, the members of a company need to be aware because this would mean that data is not being utilized in the company to make informed decisions. These are the persons with most power and experience, and hence when no analysed data or data in general is available to determine the right course of action, the boardroom tends to rely on HiPPO's judgement, which often curbs dissent. And when such acquiescence comes from other persons in the room, it adds to the confidence of the highest paid individual and a cycle is created for decisions taken with no influence of data.[3]

The dangers of this HiPPO effect is that these opinions, in the absence of any data backing them, are represented to be facts, and since employees are eager to please the person who is paid the highest and has the most influence, other logical solutions are ignored, even if the HiPPO turns out to be wrong. This has to be resolved through the process of depersonalization of decision-making, and this is when data comes into picture to separate emotions that creep in through HiPPO.[4] When information regarding products, operations and customers of

[3]Bernard Marr, *Data-Driven Decision Making: Beware Of The HIPPO Effect!* FORBES (Oct 26, 2017,12:28 am EDT), https://www.forbes.com/sites/bernardmarr/2017/10/26/data-driven-decision-making-beware-of-the-hippo-effect/?sh=54858b8780f9
[4]*Ibid*

companies comes to them in the form of data, a new paradigm of decision-making is discovered which helps businesses to survive better in the market.[5]

Therefore, the Authors today take up the task of first explaining the decision-making process of data-driven companies, advantages of such utilization of data, the process of its incorporation into decision-making, amongst various other facets in the first Part.

The framework of data governance in data driven companies, encompasses the policies, procedures, and controls for handling data, and is essential in coordinating an organization's data privacy strategy. Therefore, in the second part, Authors establish that data governance structure has to guarantee that data privacy is not considered an afterthought but rather as an essential component of the whole data management lifecycle by promoting a culture of accountability and responsibility. Thus, an attempt has been made to highlight increased concerns that arise with mining of such personal data which is required for running of data-driven companies. Once such concerns have been brought forth, the current governance regime has been analysed to determine the scenario when a data breach happens and what would be the consequences and liability in such cases. Moreover, a question has been attempted to be answered: Whether data breach can be regarded as corporate breach? For this, the Authors have glanced at various Corporate rules and statutes like IT Act, CA, etc. allowing us to reach a conclusion that data breaches can be regarded as corporate fraud under Section 43 of the IT Act, 2000 and Section 447 of the CA, 2013.

Furthermore, in the third part, directorial liability is another area which is analysed as where data privacy concerning data driven companies comes in, this aspect is crucial. Data privacy breaches can subject directors to personal liability in addition to regulatory and other legal consequences for organisations, given the evolving litigation landscape surrounding data privacy issues. In order to better safeguard their firms and themselves, directors thinking about their data privacy policies should put data privacy oversight at the top of the risk register. They should also take the lead in managing the ever-evolving and dynamic risk of data privacy. For this, the legal regime has to suffice to hold them accountable to the entities, and to the consumers, along with a robust governance structure in general to handle a vast amount of personal data. For this, an analysis has to be undertaken of the current regime, which as per the

[5]ET Spotlight Special, *Data-driven decision making: Navigating the analytics landscape product decision making*, THE ECONOMIC TIMES (Dec 10, 2023, 02:30:00 PM IST), https://economictimes.indiatimes.com/jobs/c-suite/data-driven-decision-making-navigating-the-analytics-landscape-product-decision-making/articleshow/105877287.cms?from=mdr.

Author's examination, does not suffice. Hence, the last part consists of a proposal of a workable framework to undertake this task.

To understand data-driven companies, concept of *Big Data* becomes important. Due to ever-evolving discussions regarding *Big Data*, which refers to complex sets of data, *data-driven decision-making* comes in the loop, bringing all its good and bad sides in the emerging field of data science. It has been defined as "*practice of basing decisions on that analysis of data rather than purely on intuition,*"[6] and data science is seen as the bridge to connect this kind of decision-making with technologies to process data. When decisions based on data come into picture, it becomes significant to see what necessitates this? How can it be operationalized and what are its limits, along with its promises?

UNDERSTANDING DECISION-MAKING IN A DATA-DRIVEN COMPANY

Decision making in a data-driven company entails employing "*facts, metrics, and insights*" to maintain an alignment between business strategy and desired goals. It is a cyclic process of analysing maintained and collected data and interpreting it to benefit the company or an organization. It does not just solely rely on assumptions but cold, hard facts.[7] This requires that the data relied upon is coming from an updated source, is reliable, accurate, complete and consistent. When data-quality is high, greater dependency can be placed on decisions undertaken on the basis of analysis of such data. Another consideration for such companies is the timely accessibility of relevant data. The decision-makers should be able to get their hands on data and also have required training to interpret that data, adapt to fluctuating situations and make adjustments if and when necessary.[8] When such a process is undertaken, it should not and cannot be a one-time process but an ongoing event since data fluctuations are very frequent. This is because most data driven companies' main ingredient is consumer tastes and preferences which keeps on changing at a rapid pace. Hence, regular review of the data

[6]Srivatsa Maddoli and Krishna Prasad K., *Netflix Bigdata Analytics- The Emergence of Data Driven Recommendation*, 3(2) IJCSBE 41-51 (2019); Foster Provost and Tom Fawcett, *Data Science and its Relationship to Big Data and Data-Driven Decision Making*, LIEBERT PUB (Feb 13, 2013), https://www.liebertpub.com/doi/full/10.1089/big.2013.1508; Irving Wladawsk, *Data-Driven Decision Making: Promises and Limits*,THE WALL STREET JOURNAL (Sept. 27, 2013 4:50 pm ET)https://www.wsj.com/articles/BL-CIOB-2898.
[7]https://www.driveresearch.com/market-research-company-blog/data-driven-decision-making-ddm/
[8]https://maven.com/articles/data-driven-decision-making-in-leadership

collected, decisions based on that data is required, followed by comparison with desired results to elevate efficiency.[9]

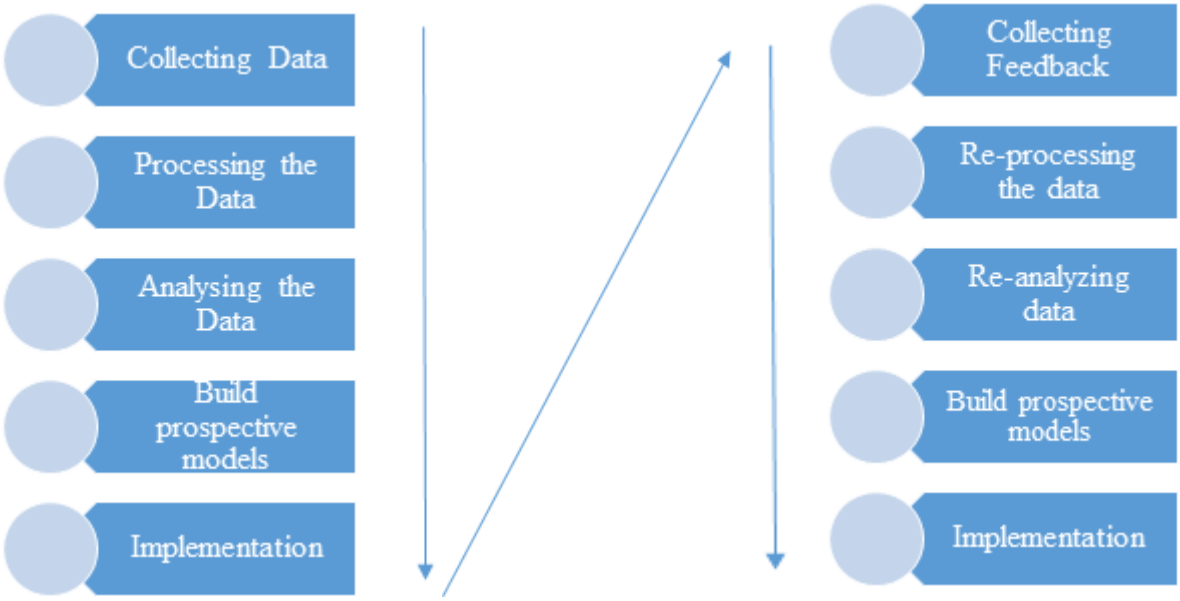
Going data-driven entails numerous benefits: it takes out the intuition that is relied upon in traditional decision-making, allowing the flow of more empirical data backing the decisions which then turn out to be comparatively more accurate and reliable; the decision-makers can get their hands on some real-time data and information enabling them to respond quickly and efficiently to the fluctuating market conditions and changing preferences of consumers. These response tactics offer such data-driven companies a competitive advantage to understand the customer needs better.[10] Data analysis upon collection also exposes potential risks and coming up with measures to mitigate them becomes comparatively easier, thus increasing the chances of effective implementation of decisions based on that analysis.[11] The significance of data to deal with unpredictable and emergency situations can be gauzed from the instance when experts such as Walmart Inc. did data mining and predicted that during warnings of flood in Atlantic coast, the need would be of products beyond flashlights: like Strawberry Pop Tarts. And when these products were stocked, they were sold out pretty quickly. Thus, data mining allowed the executives to develop a new perspective and assimilate twisted concepts.[12]

Incorporating Data into Decision-Making

- The first step to incorporating data in decision making is to look for patterns in the data scattered from which insights can be drawn. The patterns then have to be collated from various sources like internal and external datasets or interaction with customers. But since the data collected initially consists of misinformation or errors, pre-processing has to be done to filter out the genuine information which then has to be scrutinized in depth through visualization and statistical tools.
- The next step is to tie this data with any decision that is presented before the company, business-related or personal, instead of relying on HiPPO or intuition. This leads to building of effective prospective business models which are backed by evidential data guaranteeing successful results.

[9]https://maven.com/articles/data-driven-decision-making-in-leadership
[10]*Supra* note 5.
[11]*Supra* note 6.
[12] Irving Wladawsk, *Data-Driven Decision Making: Promises and Limits*, The Wall Street Journal (Sept. 27, 2013 4:50 pm ET), https://www.wsj.com/articles/BL-CIOB-2898.

- Once all this happens, just designing models is not enough, and its implementation has to be enforced and overseen, ensuring to gain as much insight from feedback with consumers as possible, which is again a form of data, continuing the cycle of decision-making, wherein each decision turns out to be better than the last one.[13]



CONCERNS OF MINING PERSONAL DATA W.R.T GOVERNANCE STRUCTURE

Data mining is a method applied to take out valuable data from a bigger group of other raw data. It means studying data patterns in big sets of data applying one or multiple software. It has use in various arenas like science and businesses. For e.g.: companies or entities can gather more information related to their clientele and form enhanced and effective models concerning various commercial functions and in return leverage assets in a highly favourable and enriching way. This aids businesses in getting nearer to their aim and formulating better policies and decisions. It is not illegal in itself. The issue comes with the point of origin of data and what is done with the information derived from such data. The data should either be of public importance like meteorological data or should have been taken with consent. This implies that consumers of websites and applications and individuals who are signing up or filling online or

[13] Talentelgia Technologies Pvt. Ltd., *The Power of Data: Transforming Decision-Making in Business*, LINKEDIN (Sept. 19, 2023), https://www.linkedin.com/pulse/power-data-transforming-decision-making-business/; Tim Stobierski, *The advantages of data-driven decision-making*, HARVARD BUSINESS SCHOOL (Aug. 26, 2019), https://online.hbs.edu/blog/post/data-driven-decision-making.

otherwise questionnaires should be informed that the entity or company will store their responses and data for analytics and research.[14] Organisations and entities that don't have consent to store and apply data could be in risk of contravening laws related to privacy, not just in that jurisdiction but also overseas, depending on where the data originated from. Additionally, many nations have restricted or banned the application of data derived from such mining in promoting discrimination on the lines of gender, colour, religion or age.[15]

A. Consideration while framing governance structure in data-driven companies

The most initial step to formulating viable strategic commercial choices is to make sure they are made based off of authentic, quality, value-laden data. A governance structure with regards to the decision making in a data-driven company aids entities and companies in assessing the data they possess, the address it is stored at and the manner in which its being utilised in order to be able to enhance the merit and value of the said data. This responsibility increases in today's world, which is primarily run on data, and thus the governance structure managing the same should be able to carry out the aforementioned functions at scale. A sound and effective governance structure comes up with useful and valuable data, and thus provides the transparency and understanding a data driven organisation requires to make efficient and sound decisions.

The governance structure with regards to the decision making in a data driven company needs to entail management of ownership of data. It should ensure that the required data is available to the relevant people at the appropriate instance. It also is required to monitor that the said data provides for sensible and effective outcomes. Thus to provide for a good governance structure in a data driven company, the whole of the organisation at multiple levels and across sectors, should strive to preserve the quality of data. Such a cooperation can result in benefits like increased amount of effective and thorough reports, based on authentic data, enhanced cooperation between various departments of the company owing to the distributed onus of preserving quality of data, increasingly precise predictions and plans and proposals, constant filtering and updating of data, among others. [16]

---

[14] Kanchan Bhave, *Data Mining and Corporate Governance*, 77 (2023), https://www.icsi.edu/media/webmodules/CSJ/june/18ArticleKanchanBhave.pdf.

[15] *Ibid*.

[16] *Dara Governance and Decision Making*, Informatica, https://www.informatica.com/in/resources/articles/data-governance-and-decision-making.html

B. Governance Structure in India

India did not have comprehensive privacy legislation prior to 2022. In 2017, SC talked about the right to privacy in the case of *Puttaswamy v. Union of India* and held it to be a constitutional right.[17] The court therein, also took into consideration the absence of a comprehensive law related to privacy and the limitations of the SPDI Rules, which came out in 2011.[18] Post the Puttaswamy decision, the Government came out with a draft legislation formulated to preserve the privacy of the citizens. Previous drafts of the Personal Data Protection Bill faced great criticism and failed to materialise in the end, like the Data Protection Bill 2021, which had some resemblance with European Union's General Data Protection Regulation, 2016 (*hereinafter* 'EU GDPR').[19] But this too was taken back in August 2022. Following this, the Union came out with the Digital Personal Data Protection Act, 2023 (*hereinafter* 'DPDP Act') which was passed and received President's assent.

As per the DPDP Act, all the entities are mandated to appoint a data protection officer, and an independent data auditor. These officials will aid companies to adhere to the legal mandates. The data protection officer will be from the side of the company when before the Data Protection Board (*hereinafter* 'DPB') and will be the adjudicatory body to deal with user complaints relating to privacy of personal data.[20] The conduction of data protection impact assessments is the responsibility of this office. In the event of a lapse, the consumer can move towards the DPB itself which functions digitally. The board provides solutions for these problems and operates akin to a civil court that also puts a fine in the case of non-compliance. If any of the parties is not satisfied with the decision of the DPB, they might go before the Telecom Disputes Settlement and Appellate Tribunal (*hereinafter* 'TDSAT' or 'Appellate Tribunal') in a period of sixty days. The tribunal will speed up the case to dispose of it in a period of six months.[21] This Act provides that the consent of the user should be followed or preceded by a notice. The consumers should be made aware of the data retrieved, the reason for which it is being applied, the process of taking back consent and the process of filing a

[17] K.S. Puttaswamy v. Union of India, (2019) 10 SCC 1.
[18] Ministry of Communications and Information Technology, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, 313 (Notified on April 11, 2011) (IND.); Chris Brook (2024) *What is India's Digital Personal Data Protection (DPDP) act? rights, responsibilities & everything you need to know*, DIGITAL GUARDIAN. Available at: https://www.digitalguardian.com/blog/what-indias-digital-personal-data-protection-dpdp-act-rights-responsibilities-everything-you (Accessed: 11 April 2024).
[19] Data Protection Act 2018, c. 12. Available at: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (Accessed: 4 April 2023).
[20] Digital Personal Data Protection Act, 2023, No. 25, Acts of Parliament, 2023 (India).
[21] *Ibid.*

complaint before the DPB. Any company that has gathered private data preceding this legislation ought to inform their consumers of the process or the manner in which their data is analysed and seek their permission for any more dispensation.[22]

India's first law to take into consideration personal data, has number of issues or loopholes with it that stand in between the law and effective protection of personal data:[23] the wide powers with the government to recuse itself, gather data from companies, and keep it for as long as it wishes in the light of welfare of the State, public order can end in the issue of mass surveillance. The government is permitted by the DPDP Act to furnish a notification to exclude its organisations from the Act's purview in light of welfare of the State, public order. etc.; Section 36 permits the government to gather individuals' data from private entities "for purposes of this Act," the terms of which have not been explained;[24] there is an inherent discharge for using private data for the deterrence, investigation, etc., of criminal activities, and the government doesn't have to release any circular for the same;

A glaring concern is that the personal data that has been shared publicly can be used freely. Section 3(c)(ii) of the DPDP Act provides that it shall not be applicable to personal data that has been shared publicly by the owner.[25] For example, social media posts, AI tools like ChatGPT applying the data available on the internet, facial recognition tools using profile photos of individuals, etc. This causes the issue of companies using this data without obtaining consent or compiling with other provisions of the Act. Additionally, considering an individual below 18 years of age a child results in access problems for them and a compliance issue for companies. The DPDP Act requires that the companies obtain "*verifiable consent*" from guardians before handling data concerning children. This restricts the ability of the children to access content without guardian's consent and also burdens the companies with the responsibility of "*age verification* (which anyways needs obtaining personal data like government IDs) *for making sure that they are not gathering personal data of any minors without guardian consent*."

[22]Veerabathini, G. (2023) *Digital Personal Data Protection Act & Impact on marketers in India*, CUSTOMERLABS. Available at: https://www.customerlabs.com/blog/digital-personal-data-protection-act-impact-on-marketers-in-india/ (Accessed: 11 April 2024).
[23] Sarvesh Mathi, *Fifteen Major Concerns with India's Digital Personal Data Protection Bill, 2023*, MEDIANAMA (Aug 4, 2023) https://www.medianama.com/2023/08/223-major-concerns-india-data-protection-bill-2023/.
[24] Digital Personal Data Protection Act, 2023, §36, No. 25, Acts of Parliament, 2023 (India).
[25] Digital Personal Data Protection Act, 2023, §2(c)(ii), No. 25, Acts of Parliament, 2023 (India).

Adding salt to injury is the on-absolute nature of consent-seeking. When asking for consent, an entity is not required to disclose things like for how long they will retain the data, what all third parties the data will be distributed to, if such third parties involve cross-border transfer, the source of the collection of data, etc. they are also not mandated to furnish their privacy policies on their sites. Also the safeguards with regards to data breaches have not been clearly provided. The DPDP Act provides the punishment in case of such breaches but doesn't clarify what steps ought to be adopted and what classifies as "*reasonable*" protections. Moreover, the victims whose data has been breached have not been provided compensation. The DPB has the authority to levy a fine of up to Rs 250 crores for a breach of data by a company, but no part of it goes to the victim. Section 43A of the IT Act, 2000, provided for a like compensation but the same has been done away with by this Act.[26] Sections 66-C, 66-E of IT Act too provides punishment for identity theft and for violation of privacy which takes care of instances when someone fraudulently uses "*unique identification feature*" of anyone or when someone circulates obscene pictures of someone without consent.[27] Furthermore, the users failing to fulfil the obligations provided under the Act are penalised: For example, if the users registers incorrect or insignificant complaints before "*a Data Fiduciary or the DPB*" a penalty of ₹10,000 can be levied. This could prevent them from registering complaints as a whole.

Furthermore, in the DPDP Act, debt recovery exemptions require safeguards. Exemptions like obtaining personal data for information related to assets and liabilities is permitted to banks for loan recovery. In the absence of safeguards, this can be an issue giving rise to happenings like fake loan applications performing false recovery measures by using phone number lists and photo compilations of borrowers and harassing them on account of the same. Also the safeguards for sensitive and crucial personal data under the Act is not in place. Data like health, biometric or financial records require more stringent regulations for using and retaining which are not there in the current Act. Finally, anonymised data isn't covered by the ambit of the Act. This could potentially be an issue because anonymised data can be de-anonymized and also placed above personal data to make inferences about persons.[28]

Thus, these glaring loopholes make the digital law of India fall flat before the Big Data Companies operating and undertaking the entire decision-making process only on the basis of consumers' personal data, which is 'apparently' obtained with their consent. These loopholes

[26] Information Technology Act, 2000, § 43A, No. 21, Acts of Parliament, 2000 (Ind.).
[27] Information Technology Act, 2000, § 66-C and 66-E, No. 21, Acts of Parliament, 2000 (Ind.).
[28] *Supra* note 22.

need to be remedied, because such data breaches amount to corporate fraud, as will be proved below, and hence, need to be taken care of in a more profound manner to *first*, develop a fiduciary relation between the consumers and the companies, *second*, to allow companies to function smoothly, and *third*, to ensure a proper remedial mechanism in case a corporate fraud ensues.

C. Corporate Fraud

Corporate fraud can be understood as performing any unlawful or dishonest act on the part of a person or corporate entity, to contravene regulations and the law to gain unethical profits. They are the unlawful practices adopted by the companies or their shareholders, etc. to benefit illegally, or get rid of losses or escape tax liabilities. For example, insider trading, incorrect financial data, data breaches, etc. These actions are undertaken to mislead stakeholders. The impacts of corporate fraud are big, constituting loss of capital to shareholders, loss of reputation to the company, the market is affected in general, and legal liabilities on the company and shareholders. Thus it's a grave and rampant issue in the commercial world around international borders, even including organizations like the European Union, G20, SAARC, QUAD, etc.

A data breach constitutes disclosing or sharing of sensitive, critical and personal or otherwise data in an illegal or unauthorised manner. Such breaches can happen in any entity or body corporate, from small companies to big corporations. These breaches can involve personal information like health details, biometrics, credit card details, social security numbers, etc., as well as corporate or commercial information like customer lists, trade secrets, source codes, etc. This unauthorised access of sensitive personal data makes the company or organisation it is stolen from and who was the one responsible for putting sufficient safeguards protecting the same is said to be liable for a data breach.[29]

In this light, provisions of IT Act and CA, 2013 come to light. Section 43 of the IT Act incorporates various offenses concerning unlawful access, storing, deriving and losses of data. In other words if an entity fails to put in place sufficient safeguards or carry out due diligence when it comes to protecting critical data, it can be held to be liable in the case of a breach of data.[30] Section 447 of the CA, 2013 defines fraud and also provides for the penalty regarding the same. The definition provided is that "*Fraud in relation to affairs of a company or any*

[29] Lalit Kumar, Companies Act, 2013 – A big leap to prevent and punish fraud, 279 (2014), https://www.icsi.edu/media/webmodules/companiesact2013/Annexure-B.pdf.
[30] Information Technology Act, 2000, § 43, No, 21, Act of Parliament, 2000 (India.).

body corporate includes any act, omission, concealment of any fact or abuse of position committed by any person or any other person with the connivance in any manner, with intent to deceive, to gain undue advantage from, or to injure the interests of, the company or its shareholders or its creditors or any other person, whether or not there is any wrongful gain or wrongful loss."[31]

It can be distinctly understood that all actions, omissions, hiding of facts or misuse of authority will not result in fraud. For them to be classified as fraud, these should have been carried out with an intention to mislead or to have unwarranted profit or to affect the welfare and needs of the company, and all its stakeholders, etc. Additionally, it would still count as fraud under Section 447, regardless of the fact that if such actions amounted to "*wrongful gain*" or "*wrongful loss*". Thus precisely the intention is most important here. Further on, the definition of fraud under this Section constitutes the phrase 'person' which provides it a very vast ambit. Therefore, it doesn't include only directors, employees, etc. under its ambit but any individual in connection to the operation of the company. [32] Also this definition provided in the Explanation part of the Section is an inclusive and illustrative one and doesn't define fraud exhaustively, providing space for other actions which can constitute "*fraud*". The concluding part of the section which takes into account the act of harming the "*interests*" of "*any other person*", and makes it culpable also has a very wide ambit.[33] Thus, owing to the wide ambit of the definition, it can be said to also include data breaches as it is nothing but unauthorised access to the database of a data driven company for using the obtained data to gain commercially with regards to other business or sale of the same. These breaches are with respect to the affairs of the company and well within the operation of the entities who are responsible for placing enough safeguards to prevent such an event. It can be a deliberate action on part of the company when the same is involved in selling of the data it is gathering through its operation, or an omission when the companies fail to put in adequate safeguards protecting their data asset from cyberattacks, or concealment in the form of vague and insignificant consent forms available on the websites of such data driven companies obtaining the consent of the users without clarifying their intention with regard to the use of that data and how and where it will be applied or processed.

[31] Companies Act, 2013, No. 18, § 447, Acts of Parliament, 2013 (India).
[32] *Supra* note 27.
[33] *Definition of "Fraud" under the Companies Act: A case of a blurred signpost to criminality*, 2021 SCC OnLine Blog Exp. 7.

Furthermore, the actions can be carried out on account of not just the company or its shareholders, but any individual in connection with the operation of the company and the same will constitute data breach on the part of the company. There might not always be wrongful gains or losses to account for in such breaches but they still end up causing damage to the interests of the stakeholders, the customers, the creditors and sometimes even the company as a whole. Corporate fraud necessitates the element of intention to be present for an act, omission, concealment, or abuse of position to amount to fraud, and in the instance of a cyberattack and a breach of data resulting from it, there might be absence of *mens rea* on the part of the company but still the onus of omitting to fulfil the responsibility of placing sufficient security measures and safeguards to prevent an attack will fall on the company, thus making it liable. Thus, in light of such contentions, data breaches can be regarded as corporate fraud under Section 43 of the IT Act, 2000 and Section 447 of the CA, 2013.

ACCOUNTABILITY FRAMEWORK IN DATA-DRIVEN ENTERPRISES

The concern relating to liability of directors has been highlighted due to the detainment of Stefan Schlipf, MD of Indian Financial Services, along with William Pinckney, CEO and MD of Amway India. As highlighted in the above parts, with enhanced exposure of consumers' and customers' data and its increased mining to implement effective decisions, comes the risk of this data being jeopardized, misused and hence, breached. This risk is "*cyber-risk*" and has surged over the past few decades. When such a breach happens, remedy has to come in frame too, and even though reports of companies incurring fines and penalties or facing lawsuits have been there, it is less explored that this remedy has to be related to directors or BOD because it contains within itself those members of the company who are involved in administrative functions and play an important role in day-to-day decision-making process. Thus, they have probable knowledge of the various transactions and activities happening in a company, putting them in a position to regulate and monitor if any data shared is being misused or breached.

"*If boards do not give cybersecurity and cyber resilience sufficient priority, this creates a foreseeable risk of harm to the company and thereby exposes the Directors to potential enforcement action by ASIC based on the Directors not acting with reasonable care and diligence.*"[34]

[34] Stewart Room, *Is Director Liability For Cybersecurity Failure An Immediate Risk?* FORBES (Sep 19, 2023,05:16 am EDT),https://www.forbes.com/sites/stewartroom/2023/09/19/is-director-liability-for-cybersecurity-failure-an-immediate-risk/?sh=212bdaa85c2d.

When the question of attaching personal liability to directors comes into question, *Re Caremark* gains relevance, which establishes that such liability can be imposed on a director for failing to "*appropriately monitor and supervise the enterprise*". The Court focused upon BOD's duty to put efforts in good faith for implementation of a system to impart adequate information and report necessary doings, and failure to do so is equivalent to failure to act under circumstances by consciously ignoring 'red flags', wherein loss could have been prevented with due attention.[35] This reasoning is furthered in *Stone v. Ritter* holding that conduct depicting non-exercise of good faith violates loyalty and fiduciary duty which is the foundation of a director's relation to the company.[36] Both these cases became important when in 2017, the exact personal data of 143 million USA customers that was aimed to be protected by *Equifax*, got compromised. The major cause was a software bug that Equifax failed to identify after caution was brought forth by Homeland Security Department, and thus hackers exploited this vulnerability. The senator described the behaviour of Equifax as constituting '*malfeasance*' or '*negligence*' because they had the requisite resources to fix the software and left the identity of half the public of America susceptible to theft. It was conscious neglect on the part of directors that materialized the risk.[37] But in cases like these where data breach is of a high threshold, *Re Caremark* cannot come to the rescue as aspects of the digital world were not discussed herein.

When debates concerning data breach amounting to corporate fraud come in picture, the analysis has to be different as be it Lilliput, Satyam or NSEL, various cases of promoter or director or management-driven frauds have come to light:[38] reviewing the current governance structure related to director's liabilities under different provisions of the CA to see if those provisions are worded such that they can be expanded to cover directorial liability for corporate fraud. And if this scenario isn't feasible, then, loopholes have to be identified, and a new framework has to be suggested or space for such liability has to be made under the new law.

[35] In re Caremark Int'l, Inc., 698 A.2d 959 (Del. Ch. 1996).

[36] Stone v. Ritter, 911 A.2d 362, 370 (Del. 2006); Brenda R. Sharton, Goodwin Procter and Gerard M. Stegmaier, *Breaches in the boardroom: What directors and officers can do to reduce the risk of personal liability for data security breaches*, THOMSON REUTERS, https://legal.thomsonreuters.com/en/insights/articles/board-liability-reduce-risk-for-data-security-breaches.

[37] Yoo Meena, *Director Liability in a Data Breach Era*, FORDHAM JOURNAL OF CORPORATE AND FINANCIAL LAW (Nov. 6, 2017), https://news.law.fordham.edu/jcfl/2017/11/06/director-liability-in-a-data-breach-era/#_edn15.

[38] Vyapak Desai and Ashish Kabra, *Director and Officer Liability in India*, NISHITH DESAI, https://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research%20Articles/Director_and_Officer_Liability_in_India.pdf#:~:text=Under%20section%20150%2812%29%20of%20the%202013%20Act%2C%20an,where%20he%20or%20she%20failed%20to%20act%20diligently.

A. Provisions under the CA, 2013, and the Rules.

As examined above, data breach does constitute corporate fraud which entails an undertaking of activities that are dishonest or illegal, either by the company or an individual (especially, director/s) to earn profits under the table, or avoid tax liabilities, by going against established rules and regulations. It generally includes displaying false financial data, insider trading, bribery, etc. and is generally done to deceive the shareholders and the customers. But as will be examined and analysed below, even though data breach can be covered under CA, the provisions are not sufficient to attach liability to the BOD.[39]

(i) Section 339 and 447.

In this light, sections 339 and 447 of the CA[40] 2013 are relevant. With a combined reading of these section, a type of corporate fraud that becomes of consideration is "Asset Misappropriation or Embezzlement" because for data-driven companies, data is the most significant asset, as explained in Part I. In this type of fraud, a person or a group intentionally misappropriate company's assets entrusted to them. The assets, in this case, are entrusted to such individuals in a lawful manner, i.e., he has the right to possess them and work in relation to them, but knowingly and intentionally goes on to use such assets for unintended purposes.[41] Section 339 takes care of this kind of commission, and provides that any person, who conducts the business of the company, knowingly, in a way to intentionally defraud anyone, undertakes fraudulent conduct. This includes misappropriating any property of the company, or any other person or discontinuing any activity that was supposed to be carried out, or gaining unlawfully, or inducing any other person to deliver any advantage to someone, or making a false representation of the affairs or accounts of the company, all undertaken with the same intention.[42] Under this section, a criminal liability of imprisonment of up to 5 years, has been attached.[43]

Under Section 447, fraud has been defined w.r.t a corp. body's affairs. It includes: commission or omission or concealing of facts or abusing a position an individual has in company, or with

[39] *Corporate Frauds under Companies Act, 2013*, GEEKS FOR GEEKS (Mar. 5, 2024), https://www.geeksforgeeks.org/corporate-frauds-under-companies-act-2013/#what-is-corporate-fraud-under-companies-act-2013.
[40] Companies Act, 2013, §339, §447, No. 18, Acts of Parliament, 2013 (India).
[41] Adam Hayes, *What Is Embezzlement, and How Does It Happen?* INVESTOPEDIA (Aug. 20, 2023), https://www.investopedia.com/terms/e/embezzlement.asp.
[42] Sharad Kumar Sharma, S*ection 339 of Companies Act 2013 – Fraudulent conduct of business*, TAX GURU (Feb 15, 2023), https://taxguru.in/company-law/section-339-companies-act-2013-fraudulent-conduct-business.html.
[43] *Ibid.* https://taxguru.in/company-law/section-339-companies-act-2013-fraudulent-conduct-business.html

connivance with others to deceive intentionally or take undue advantage purposely to injure.[44] This provision too provides for criminal liability and to establish this, *first,* the act undertaken has to fall within the scope of employment, and *secondly,* the act has to benefit the organization as the activity performed by an employee of the organization is not separate. Moreover, this provision provides that when fraud involves public interest, imprisonment has not to be below 3 years.[45] Complementing this is Section 86(2) which invokes Section 447 in case intentional false information is furnished or correct/material information is suppressed.[46]

Here under the consideration is data as an asset. Some forms of data breach can take the form of MD or WT directors utilising this personal data of the customers for their personal gain by selling it across pirated online platforms just to earn an extra something. This was seen in *Cyberabad data theft of 2023,* where Vinay Bhardwaj was arrested for selling personal information of over 60 crore people and companies all over India.[47] Another noticeable data breach occurred when "*personally identifiable information of 815 million Indian citizens, like their Aadhar numbers and passport details* were being sold on dark web."[48] But in this breach, the data had first been subject to theft constituting data leak of 1.8 terabyte of data, and was then offered for sale. Section 399 can be extended to cover such instances to a certain extent because it provides for a penalty when someone lawfully entrusted with an asset, goes on to misappropriate it intentionally for unintended purpose. In the decision-making process in a data-driven company, the part of BOD that is involved in daily activities is logically the one entrusted with the accessibility and protection of the data that such companies ask for and store to make their profit-related decisions and to design their services and products in line with such information. In this course, when the data is intentionally sold, either with the knowledge of such directors, or with their consent or connivance, on for example, dark web where it is being misused in a manner to endanger the privacy of consumers who had supplied their personal data with explicit or implicit consent, then such directors can be brought within the loop of liability provided under Section 339 and 447 of the CA, 2013. It would amount to misappropriating the property of consumers, which has now become an asset of the company,

[44] Bhavika Mittal, *Section 447 of the Companies Act, 2013,* IPLEADERS (May 4, 2023), https://blog.ipleaders.in/section-447-of-companies-act-2013/.
[45] *Ibid.*
[46] Companies Act, 2013, §339, §447, No. 18, Acts of Parliament, 2013 (India); Companies Act, 2013, §86(2), No. 18, Acts of Parliament, 2013 (India).
[47] Aditya Krishnan, *Top 7 data breach incidents in India,* INSIGHTS (May 9, 2023),https://etinsights.et-edge.com/top-7-data-breach-incidents-in-india/.
[48] The Hindu Bureau, *Top Cybersecurity Breaches in 2023,* THE HINDU (Dec. 16, 2023 01:22 PM), https://www.thehindu.com/sci-tech/technology/major-cybersecurity-data-breaches-in-2023/article67644589.ece.

provided such information has been taken with consent that is "*free, specific, informed, unconditional, and unambiguous, with a clear affirmative action*" as per the DPDP Act of 2023.[49]

In other forms and instances of data breach: theft, hacking into the system and leaking the data, omission on part of the directors come into picture. When such part of the BOD has stopped doing an activity which was required on its part or does not initiate such activity in the first place, that was necessary to ensure that the huge amount of data on which the company was operating is secured and not fall in wrong hands, then a civil liability can be imposed on such directors under Section 447 and 339. This is because it was their negligence, lack of due diligence, which allowed and enabled the hackers to get into the system and steal the data. It is the director's duty, who are the fiduciary agents of the company, to take care of the company's interests, because when such data gets out or is compromised, it is the company that has to face the social brunt of deteriorating reputation leading to decline in losses. This is where Section 166 also comes in.

(ii) Section 166.

Under Section 166, sub-sections 2 and 5 provide that the directors are required to act in accordance with the best interests of the company, and shall not accord an undue advantage to themselves. What is important is that these duties are not in relation to the customers but the company. If the directors gain undue advantage to themselves, they shall have to pay an amount equivalent to the loss caused to the company, but nothing has been stated about the liability to the consumers or customers of companies like Amazon, Netflix etc. which are operating for consumers, on the basis of their data. These are called fiduciary duties and are mainly to establish loyalty of the agents of the company to the company itself.[50]

Duties provided for in Section 166(2) and (3) can be primarily divided into two types: duty of skill, diligence and care, and fiduciary duties. While the latter relates explicitly to the company, the former can be interpreted to mean that a reasonable amount of skill and diligence has to be applied with care in performing a duty that has been endowed upon them, and hence, if directors intentionally overlook the instances of "*numerous red flags*" that could have been discovered by exercising due diligence and care of a level of a prudent person who was privy to such commission or omission, then as per the SC in *N. Narayanan* case, then such directors can be

[49] Digital Personal Data Protection Act, 2023, No. 25, Acts of Parliament, 2023 (India).
[50] Companies Act, 2013, §166, No. 18, Acts of Parliament, 2013 (India).

held liable for breach of duty.[51] This is the standard of a reasonable man generally followed in tort law, which is subjective and hence, is credible to be imported for assessment under Section 166(3): "*a reasonable man, guided by considerations that ordinarily regulate human affairs – in the shoes of the director.*"[52] If this duty of care is breached, liability is attracted: removal or paying of fines or indemnifying the company, etc. i.e., civil liabilities to the company.[53] Moreover, if the ratification of the liability has occurred by the vote of the shareholders, then power of the Tribunal under Section 463 comes into picture by considering relevant circumstances.[54]

Again the grey area or a loophole that arises is that whatever liability, in any form, is imposed, is w.r.t the company which is not enough in cases of data breach amounting to fraud. There has to be a sense of responsibility and liability towards the consumers/customers of Big Data companies, because even if loss is accrued to the company due to such data breach, at the end of the day, it is the consumers whose data is being jeopardized and misused for various purposes that might not even concern them, but harm them significantly. This is because all kinds of personal data of an individual float on online platforms due to different kinds of services provided by various data-driven companies, and such personal data can be applied to recognize a person: name, address, passport, identification cards, genetic or medical or even biometric data. If, for instance, a person's medical data is lost in data breach, it could have a serious impact on the treatment he/she is undergoing, and hence, impact his/her life.[55]

(iii)Rule 28 of the Companies (Management and Administration) Rules 2014.

This Rule requires for the Board of company to appoint a person who shall be taking responsibility to manage, maintain and secure electronic records, and a failure to abide by the duties that have been enlisted in the second part of this rule, would result in breach of their duty of care, and not 'data breach' which is what we are looking for. This responsibility, as per the provision, is endowed upon either the MD or CS or any other director or officer, and some such

[51]*An Analysis of the Duties of Directors in India,* INDUSLAW (May 2023), https://induslaw.com/publications/pdf/alerts-2023/infolex-article-an-analysis-of-the-duties-of-directors-in-india.pdf; N. Narayanan v. Adjudicating Officer, SEBI, (2013) 12 SCC 152.

[52] Rishabh Mohnot and Hrithik Merchant, *Analyzing Directors' Duty of Care under the Companies Act, 2013,* INDIA CORP. LAW (Mar 29, 2023),https://indiacorplaw.in/2023/03/analyzing-directors-duty-of-care-under-the-companies-act-2013.html.

[53]*What are the duties of a company director and what happens if they are breached?* LINCOLN & ROWE, https://lincolnandrowe.com/2023/06/15/duties-company-director/#Consequences_for_the_director_include_the_following.

[54]*Supra* note 50.

[55] James Mackay, *5 Damaging Consequences of Data Breach: Protect Your Assets,* META COMPLIANCE, https://www.metacompliance.com/blog/data-breaches/5-damaging-consequences-of-a-data-breach.

duty ensue to "*provide adequate protection against unauthorized access, alteration, or tampering of records; ensure that systems of recording are secure and validated; ensure that records are in a non-erasable format; ensure at least one back up.*" The most prominent responsibility comes forth: "*ensure and limit the access of the records to the person who is assigned the responsibility.*" [56]While this rule might raise our hopes for including directorial liability for data breach in here, this kind of provision becomes problematic because the Rules of 2014 provide for such duties, and then do not go on to talk about their breach to constitute as breach of 'electronic data' or 'data breach' but as 'breach of duties' which is punished in a less strict manner than the threshold of liability for a data breach. Electronic records mentioned here can be equated with data collected by data-driven companies, and its access, under this rule, has been provided only to MD or CS or any other person, without inserting a specific provision of their liability. Hence, this rule too falls flat when Big Data Companies handling personal data of people from all over the world come into picture. In such companies, attaching a simpler liability of furnishing a minimal fine would not suffice as *first*, it is, generally, not only a single person handling this data analysis, and *secondly*, the importance and risk related to such personal data is more (as explained above) and includes information of a more sensitive nature that the CA formulated in 2013 could have possibly envisaged.

B. Provisions under the DPDPA 2023.

The Act recently implemented becomes important because the subject-matter remains protection of personal data which is floating across the various social media platforms, is digitized, and is of concern when debates around 'directorial liability in data breach' take place. This act allows an entity to collect and process that data for which consent of the individual is taken or that which is required for 'legitimate reasons', notice regarding which has to be sent to the person. Legitimate use reasons, as per the act include: voluntary providing of data by individual for a specific purpose, provisioning of some benefit from the Indian state's department if previously that person had consented to it, security or sovereignty, fulfilment of legal obligation of disclosure, complying with court orders, medical exigencies, or breakdown of public order or a disaster. [57]

[56] Ministry of Corporate Affairs, Companies (Management and Administration) Rules, 2014, Rule 28, 22 (Notified on August 11, 2023) (IND.).

[57] Digital Personal Data Protection Act, 2023, No. 25, Acts of Parliament, 2023 (India); Anirudh Burman, *Understanding India's New Data Protection Law,* CARNEGIE INDIA (Oct. 03, 2023), https://carnegieindia.org/2023/10/03/understanding-india-s-new-data-protection-law-pub-90624#:~:text=Consent%20must%20be%20%E2%80%9Cfree%2C%20specific,necessary%20for%20the%20specified%20purpose.

This Act goes on to define Data Fiduciaries as someone who have the responsibility to collect, store, process the digital personal data, and certain duties have been imposed on them: security safeguards maintenance, informing about the data breach to the DPB, etc. There is a concept of SDFs who are designated by the government. keeping in consideration the sensitivity of the data and the risks involved and their additional duties entail: appointing a 'data protection officer' answerable to BOD, conducting impact assessment of data protection. An interesting section that comes up is Section 37 which provides the govt. with the power to prevent the public's right of entry to an information that has been allowing the data fiduciary to undertake supplying of goods or services in India while also providing a chance to him/her to be heard, based on essentially two requirements: *first,* the DPA had imposed penalties against such Data Fiduciary at least twice, and *second,* the blockage has been recommended by DPA. [58]

Even though this is the first law to establish a "*statutory framework for data protection*" in India, there are some problematic provisions which create loopholes in holding the Data Fiduciaries and the Board liable. Section 17(5) confers power upon the govt. to exempt, within five-years, from the provisions of this law, any "*business or class of business*"[59] but there has been no time frame provided as to how long this exemption would operate for or how it would operationalize. As per the Authors, this provision has been inserted unnecessarily because time for start-ups to comply with these provisions was already provided for in Section 17(3),[60] and hence, there is a potential for misuse for Section 17(5) by start-ups or other businesses so as to defeat the purpose of law: all of the duties mandated for data fiduciaries could be done away with and data breach would then proliferate. Moreover, there has been no discussion over the liability of the directors or the BOD in case Data Fiduciaries fail in their duty, and duties and responsibilities of them have not been outlined. A distinction has been made between the two as the latter is being held responsible to the former. The DPB has been constituted separately with functions and powers of its own, like imposing penalties in case of breach of private data, but no provision for liability of this board too, can be found. Hence, a single law in existence related to data protection and actually has the potential to deal with and take care of activities in data-driven companies, does not talk about liability of those in charge of securing that data and those empowered to oversee such act of securing. Moreover, consequences of personal data breach have not been discussed: recovery of such data when sold or leaked or

[58] Digital Personal Data Protection Act, 2023, No. 25, Acts of Parliament, 2023 (India).
[59] Digital Personal Data Protection Act, 2023, §17(5), No. 25, Acts of Parliament, 2023 (India).
[60] Digital Personal Data Protection Act, 2023, §17(3), No. 25, Acts of Parliament, 2023 (India).

compromised, liability of such data fiduciaries, DPB and BOD towards such individuals whose data has been compromised – only a penalty has been imposed in terms of fine, which does not suffice, and hence, governance structure has to be remedies, while also bringing BOD in the loop, and that too, in a proper manner. For this, either a special legislation has to come into existence or amendments have to be made to the existing CA and the DPDPA (Part IV).

RECOMMENDING A GOVERNANCE STRUCTURE

Even though the one digital law does not outline director's duties and liabilities, it becomes necessary to make space for the same as in case a company is facing an attack of ransomware, especially if it had been for the benefit of the Boardroom, then what is the extent to which such directors can attract a liability for negligently failing to take steps to mitigate the risk. This becomes important because, every 39 seconds, one data breach happens indicating, that an attempt is always there to access companies' consumers' personal data, which ultimately results in: compromising such data, bringing business operations to a halt as systems are encrypted and if that encrypted data cannot be restored, havoc can fall on such companies.[61]

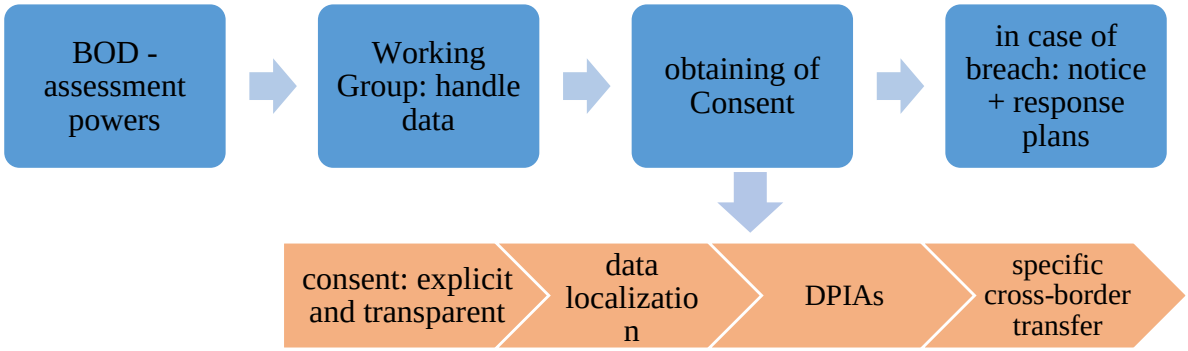
A. Outlining the Potential General Governance Structure.

In coming up with a comprehensive governance structure for data protection assurance, loopholes in DPDP Act have to be rectified: the government's authority leading to mass surveillance should be restricted by clearly providing for the conditions during exemption to its agencies can be granted; limitations on the use of publicly available data by body corporate have to be implemented and made subject to clear consent from the users, which has to be through a thorough transparent and an accountable procedure; companies need to clearly specify the time period of the storage of such data, third-party sharing plans, cross-border transfer objectives, and policies related to privacy, etc.; the Act needs to be amended to clearly lay out 'reasonable safeguards'; the DPB needs to ensure that the companies provide damages and relief to the victims in case of a data breach. They should also provide for reasonable penalties in case of a false complaint; stricter regulations and safeguards for the protection of sensitive data, like that related with health of individuals, biometric records or financial

[61] Pierluigi Paganini, *Have Board Directors any Liability for a Cyberattack against their Company?* SECURITY AFFAIRS (Nov. 14, 2022),https://securityaffairs.com/138507/security/board-directors-liability-for-cyberattack.html.

information; a space to deal with anonymised data thus preventing its misuse by de-anonymising it.

Thus, a proper governance structure has to be established to follow a specific procedure which works upon the sensitivity of the data collected and breached: the base for this purpose has to be stronger.



BOD with proper assessment powers and attached liabilities have to be instituted, overseeing the operations of the working group who shall be handling the data collected. The data collection has to happen through consent of the consumers, which is explicit, especially in case of sensitive information; no consent has to be presumed on the part of consumers and the consent forms need to be transparent, legible, understandable, and accessible. The scope of data localization has to be broadened to cover vast varieties of data categories, ensuring better security, control and privacy. Moreover, for international data transfers, a separate working group has to be instituted to follow guidelines of contractual clauses with a standard specified, binding corp. rules, techniques specific to certain type of data, etc. To ensure proper and enhanced privacy and avoid breach, protections have to be encouraged to be inserted in all systems and undertaking of DPIAs for "*high-risk data processing activities*". In the event of breach, organizations, specifically BOD, has to be ensued with duty to formally notify people and authorities with specified guidelines being followed w.r.t format, timing, type of notification. Moreover, strong "*incident response plans*" should be initiated and enforced.[62]

[62] Antima Tiwari, *Paradigm Shift In Data Protection: Analysing The Digital Personal Data Protection Bill In The Context Of India's Privacy Landscape*, MANUPATRA (Sept. 22, 2023), https://articles.manupatra.com/article-details/A-Paradigm-Shift-In-Data-Protection-Analyzing-The-Digital-Personal-Data-Protection-Bill-In-The-Context-Of-India-s-Privacy-Landscape.

B. Outlining the Director's Potential Role and Liabilities.

As per the scale of data utilized as an asset by the company, and the amount of estimated risks calculated, the director has to oversee actions the company undertakes to forestall the risk of data breach and take corrective reforms promptly. This includes: ensuring "*periodic penetration tests*" and measures to assess maturity of technical measures, handling the weaknesses identified immediately and not pushing them away for a later period, designing a response plan that can work efficiently in case an attack entails, and a detailed analysis of risks has to be undertaken by the directors, with a component of training and control processes for organizations, along with a comprehensive "*compliance program*".[63]

Whenever a data breach or a cyberattack entails, corrective actions have to be analysed by BOD to mitigate the adverse cyber-attacks, assessment of economic impacts to be undertaken, finding out and analysing what kind of personal data has been jeopardized and how it can personally affect the audience/customers of the company. Then attempts have to be made to recover that data, which requires peremptory preparedness monitored by the BOD. When a ransomware attack has been undertaken, a decision has to be made as to whether to pay the ransom or not depending upon the nature of data compromised. After everything goes down, the incident has to be reported to the public and the specific authorities, without a 'lie' or 'half-truth' or 'concealment of facts'. This should include assuring the public that their data is being recovered or that steps are being undertaken to not have their data further manipulated or to recognize the entity/individual behind such data breach in case it is intentional.[64]

These responsibilities of the BOD have been outlined by the Authors in the light of Section 166 of the CA, 2013. Thus, in a data-driven company, performing in good faith for the best interest of the company which handles a large amount of consumer data becomes crucial. The corrective actions highlighted helps in proper compliance with Sec 166(3) which necessitates directors to carry out with "*due and reasonable care, skill and diligence*".

But, what happens when there is a failure to undertake these roles and comply with the duties highlighted in Sec 166? These duties are breached in case a director wilfully ignores a security risk that floated and this results into a security gap which provided an opportunity to the outsiders to commit a data breach. Only proactive solution that can be found is in Sec 166(7) of the CA which provides that: "*If a director of the company contravenes the provisions of this*

[63] *Supra* note 61.
[64] *Supra* note 61.

section such director shall be punishable with fine which shall not be less than one lakh rupees but which may extend to five lakh rupees."

A penalty under this provisions holds directors or BOD liable and accountable towards the company. But what more is required is: an additional accountability towards the public in general. This is because in companies like Netflix, Hotstar, the amount of data that floats are enormous to sync the consumer tastes with their show recommendations. When data breach in such entities happens, directing directors to pay an amount of one to five lakhs is not enough, as it is not only the company which faces loss, but the consumers who are exposed to a much bigger risk. Keeping this in mind, either a chapter has to be inserted in the DPDP Act of 2023 as it is the only law concerned specifically to data/personal data, or a new law has to be brought in, which again would be too much of a hassle and too much of a delay.

CONCLUSION:

Thus, with the continuing rise of data-driven companies, concerns related to compromise of personal data, leading to privacy violations are all-time high. In such scenarios, the current governance regime of CA, DPDP, IT Act, even though reflect a potential shelter, do not suffice in providing a house these considerations need. The sensitivity of such data collected can be gauzed through an example of Netflix provided in Part I of the paper, where the Authors answer the first research question. The second research question then highlights the concerns that ensure due to enormous and quick use of personal data by drawing support from Puttaswamy judgement and concludes that the current structure, even by stretch of interpretation is not sufficient and is full of loopholes. The third question that navigates the role and liability of fiduciary agents of the companies and try to establish their liability towards the victims of data breach through the current laws, but discovers that this is rather not possible, which then leads to the fourth question, where Authors proceed to provide a recommendatory structure for general governance structure, and for director's roles and liabilities, in a hope that sometime in the future, this could be implemented or current regime could be amended and enforced in a manner to give full effect to the right of privacy enshrined in the ***Puttaswamy Judgement.***