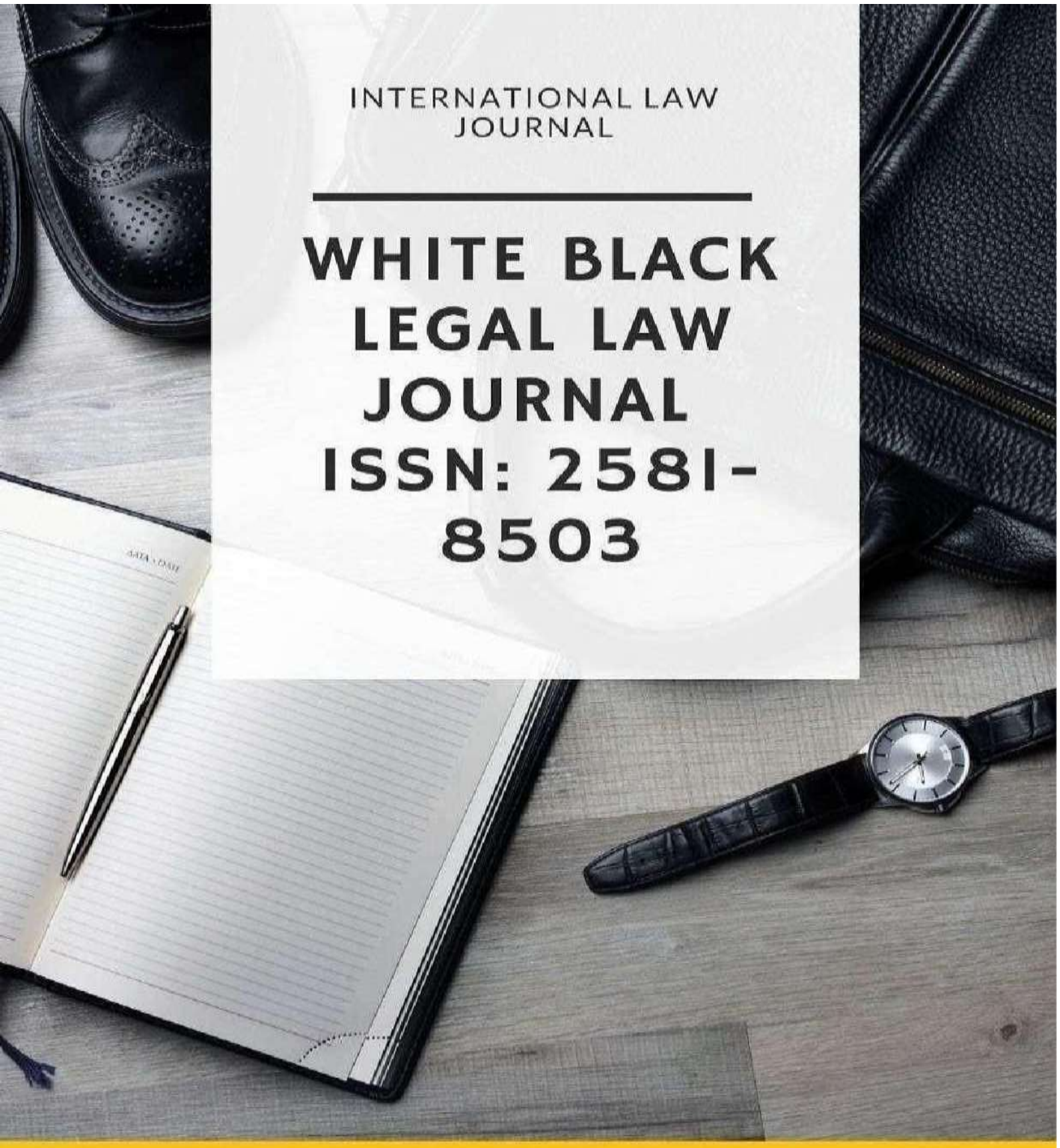

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in ‘Intercountry adoption laws from Uttranchal University, Dehradun’ and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

“DATA BREACHES: ANALYTICAL STUDY OF LIABILITY OF DIRECTOR'S IN COMPANY IN INDIA”

AUTHORED BY - RUBY SINGH

ABSTRACT

This research paper addresses a topical issue—data breach and privacy—with a focus on the business world. The lack of such laws has been the real cause of occurrences like the Aarogya Setu data issue or the Whatsapp data leak case, which have been briefly covered below, thus the researcher has highlighted on the necessity of a central level comprehensive regulation on data protection. A passing mention of the IT Act of 2002, which governs data protection, has been made, and proper emphasis has been placed on the Companies Act of 2013. The paper will do an analysis of director’s responsibility to prevent data breach in companies.

Keywords: data, breach, privacy, information, Company, Directors.

INTRODUCTION

The issue of data privacy has taken on additional perspectives in the current era of globalisation, when value and volume of data are continually expanding due to expansion of trade. As opposed to earlier, protecting data privacy is now a global legal requirement, not just a way to gain an advantage over rivals.1 Regulators and the marketplace put a lot of pressure on businesses to enhance their data gathering procedures, how they use and store all customer information, and most crucially, how they delete it. Data privacy is now more vital than ever because to the development of the internet.

The various rules and standards established for their respective sectors have long been the focus of many businesses' data protection efforts. But in light of the current circumstances, such industry-specific data policies were no longer useful. Businesses will benefit from a more methodical and organised approach to information governance, which must be inspired by the broadening data legislation as well as the rising significance and awareness of the data protection

issue. Large corporate organisations, especially those doing international trade, need a complex compliance management system that integrates all connected business operations. To keep the trust of their clients and staff and to reduce the liability risks for their directors and officers, they must design and implement company-wide implementation and data collection systems in accordance with cross-border legal standards, especially regarding data privacy legislation.

The case of Justice K.S. Puttaswamy (Retd) v. Union of India[1] elevated the right to privacy in India to the status of a basic right, and as a result, it is now covered by Article 21 of the Constitution of India, 1950. The right to privacy has therefore been accorded the highest priority by the Indian judiciary, and it can only be restricted for justifiable reasons like state protection and the general good. There is currently no definite law in India addressing the confidentiality of data and records. Separate laws governing information technologies, intellectual property rights, criminal law, and contractual connections can be used to access data and privacy rights. The IT Act offers for protection from these violations with relation to data from information networks. The aforementioned legislation includes measures to prohibit the unauthorised use of computers, computer operating systems, and the data they store. The aforementioned legislation includes measures to prohibit the unauthorised use of computers, computer operating systems, and the data they store. Data security violations and misuses are not specifically included under the Indian Penal Code, 1860. Responsibility for such crimes must be deduced from pertinent offences under the Indian Penal Code, 1860. For instance, Section 403 of the India Penal Code prescribes jail terms and proportionate fines for fraudulent theft or conversion of "movable property" for one's personal use. The Indian Copyright Act lays out required penalties for using copyrighted content without permission. Credit information about Indian citizens must be gathered in accordance with the privacy requirements outlined in the CICRA, also known as the Credit Information Companies Regulation Act of 2005.

WHAT IS DATA BREACH?

A data breach occurs whenever confidential, sensitive, or protected information is accessed by a person who is not entitled to view or use it. A data breach occurs when unauthorised parties read, copy, or otherwise distribute the files in question.

Any organisation, no matter how large or little, as well as any level of government, is susceptible to experiencing a data breach at some point. Even more importantly, if they are not protected,

[1] (2017) 10 SCC 1.

anyone has the potential to put others in risk.

How does a data breach take place:

- **An insider with no malicious intent**: An example of this would be if one person viewed files on another worker's computer while they did not have the appropriate authorization permissions. There is no information that has been revealed, and the access that was gained was unintentional. However, due to the fact that the material was viewed by a third party that was not authorised to do so, it is now considered to be compromised.
- **A cunning participant behind the scenes:** This person accesses and/or shares data knowingly with the intention of causing harm to another individual or business. Even if the malevolent insider is granted permission to utilise the data, their intention is to put it to some kind of unethical or illegal use.
- **Devices may go missing or be stolen:** Everything that could possibly contain vital information vanishes, including a laptop that is left open and unencrypted as well as an external hard drive.
- **criminals from the outside with malicious intent**: Hackers are those that use a range of intrusion techniques in order to obtain information from a computer network or an individual.

Even if a data breach was caused by an honest error, it might still lead to major losses if the person who got unauthorised access stole and sold personally identifiable information (PII) or corporate intellectual property (PIP) in order to make money or do harm. This is because PII and PIP refer to different types of information that can be used to identify an individual.

When aiming for a breach against an organisation, as is the case with the majority of criminals behaving maliciously, planning is required in order to be successful. They investigate the targets in order to identify the vulnerabilities in their security, such as outdated software, upgrades that have not been deployed, and staff employees that are credulous enough to fall for phishing schemes.

Hackers create a plan to deceive staff working inside the business into unintentionally downloading malicious software after identifying a target's vulnerabilities. Sometimes they specifically aim after the network itself.[2] Once inside, dishonest thieves have the freedom to look for the data they want and plenty of time to do so because it frequently takes more than five months

[2] Van Der Linde, K. (2008). The personal liability of directors for corporate fault-an exploration. *SA Mercantile Law Journal, 20*(4), 439-461.

to find a security breach.

The following are typical flaws that malevolent actors target:

- **weak qualifications:** The majority of data breaches are caused by stolen credentials or credentials that have been compromised. Criminals with nefarious intentions can gain access to your network by using a combination of your login and password. Because the majority of users recycle their passwords, fraudsters can use brute force assaults to gain access to email, websites, bank accounts, and other sources of personally identifiable information or financial information.
- **stolen identification:** Phishing-related security breaches are a serious problem, and if cybercriminals are able to get this Personal Information, they can gain access to things like your bank and internet accounts.
- **Compromise resources:** Malware assaults are used to undermine standard authentication procedures that would otherwise safeguard a computer.
- **Card fraud for payments:** When a card is swiped, data is stolen by card skimmers that are attached to ATMs or petrol pumps.
- **unauthorised access**: Even if you take all reasonable precautions to keep your network and data secure, malevolent hackers may still find a way into your system by using third-party suppliers.
- **Mobile technology: "**When employers permit employees to use their own devices at work (BYOD), it's simple for unprotected devices to download malware-filled apps that offer hackers access to the device's data. Along with the owner's PII, this frequently also includes work emails and files."

IT ACT AND SPDI RULES

"The Information Technology Act and the Statewide Data Protection Compliance Rules will have the most significant effect on the majority of firms in all sectors. The Information Technology Act requires that body corporates that handle sensitive personal data or information (such as businesses, firms, sole proprietorships, and other associations of people engaged in commercial or professional activities) be held liable for any loss that was caused by their negligence in putting in place and maintaining reasonable security practises and procedures. Examples of body corporates include businesses, firms, sole proprietorships, and other associations of people engaged in commercial or professional activities."

Although "reasonable security practises and procedures" are not defined in the IT Act, the SPDI

Rules, which were formed in compliance with the IT Act, outline the minimal standards for data protection for sensitive personal information. These rules were created to ensure that sensitive personal information is protected. Even though the purpose of the SPDI Rules is not to be exhaustive, they do require companies to have a privacy policy, obtain customers' consent before collecting or transmitting sensitive personal data, and tell customers about who will be receiving their information. The fact that consent continues to be the primary legal foundation for data processing is one of the most significant aspects that differentiates the SPDI Rules from other, more modern data regimes.

“In this regard, the IT Act also specifies criminal penalties for those who disclose particulars without the authorization of the person to with whom that information relates, where the communication is in violation of a contract or results in unjust loss or gain. These criminal penalties can include both fines and imprisonment for up to three years. In this regard, the IT Act also specifies criminal penalties for those who disclose particulars without the authorization of the person to with whom that information relates.”

DIRECTOR’S ROLE IN PROTECTION OF DATA BREACH IN CORPORATE

Unfortunately, the Companies Act of 2013 is vague on data privacy and data protection when it comes to issues of data protection relating to corporate houses. However, there are some legal provisions that are frequently cited in data privacy violations, particularly when the issue of the directors' liability for data protection and privacy is raised. A "director" is recognised as "a director appointed to the company's board" in accordance with Section 2(34) of the Companies Act, 2013, which is the law in effect. A director serves as the company's controller. The Companies Act of 1956 did not include any provisions for the legislative responsibilities of directors; instead, they were governed by the board's basic standards and established precedents. The following list of director responsibilities is included in Section 166 of the 2013 Companies Act:

- The director must conduct themselves in accordance with the AoA.
- The director must act in accordance with his or her moral principles to preserve the enterprise's interests for the benefit of all stakeholders, including the enterprise's shareholders, employees, society, and even the local ecology.
- The director must perform his duties and use good discretion with adequate care, skill, and effort.

- The director is prohibited from participating in any decision where they may have even the slightest investment or conflict of interest that interferes with or is likely to interfere with the interests of the firm.
- The director is prohibited from obtaining or even attempting to obtain any unauthorised benefit or gain for himself, his relatives, partners, or associates. If the director is found to have obtained an unauthorised gain, he will be required to reimburse the company for that gain.
- The director is not permitted to assign his office, and any such assignment is deemed illegitimate if it is made.

It is crucial to remember that all of the director's responsibilities fall into two categories: Duty of Care, skill, diligence and independent judgment, Fiduciary duties.

"A monetary penalty of not less than one lakh INR, but up to five lakh INR, is imposed for violating section 166. However, if a director is found to have made an unjust profit, he will be required to reimburse the corporation an amount equal to the profit."

The Companies Act of 2013 was passed to replace the outdated Companies Act of 1956 since it was not appropriate for the needs of the corporate world today. Unfortunately, the legislators overlooked a crucial concern for businesses in the state—data security and breach—in their legislation. However, it has been determined that cases of cyber security and data breach fall inside the purview of the directors' statutory duties under Section 166. Cybersecurity and data breaches fall under the heading of duty of care, skill, and diligence. In today's world, it is impossible to argue against the widespread belief that suitable safeguards for data should be included in the prudent care that any director must take when managing company risk. To what extent this perception is accurate under the law is still up for debate. The following considerations must be made by the judicial authorities while making their decision:

- Technology of the business's current organisational and technological framework;
- Business- and sector-specific principles and risk management;
- The intensity of debates on cyber security and data breach at the board or committee level;
- The application of guidelines at the organisational level.
- Third-party auditing and certification of security procedures;
- Background information and potential retention of earlier occurrences.

In addition to the directors' duty under Section 166 to maintain cyber security, some delegated legislation made available under the Act imposes explicit data security requirements on management that they must abide by. According to Section 28(1) of the Companies (Management

and Administration) Rules, 2014, the managing director, company secretary, or other appointed officers or agents are accountable for the preservation and protection of electronic data and documents. The following responsibilities are specifically the management's, as stated in Section 28(2) of these regulations:

- Ensuring adequate protection against any type of unauthorised access, deletion, or data use;
- Lack of documents as a result of system failure or interruption in which the data is stored;
- Computer systems, software, and hardware are properly safeguarded and assessed to ensure correctness, sustainability, and constant performance.
- Records that are accurate, usable, and trustworthy enough to be repeated for reference;
- That not more than one copy of updated documents maintained in electronic form is made every day at a minimum;
- Adequate steps must be taken to guarantee the confidentiality, integrity, and security of information;
- Access to information is restricted for the managing director, company secretary, and any other director or officer who has been given permission to act on the Board's behalf.

According to the aforementioned standards, “data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer-generated micro fiche” is what is meant by "electronic records." Despite the fact that directors have a duty to safeguard data privacy, the fine imposed for breaking the aforementioned criteria is small. Failure to comply may result in fines of up to 5,000 INR, and if the infringement is persistent, another fee may be increased to 5,000 INR each day after the first day on which the breach had started. Whether class action lawsuits are a practical means for impacted investors to obtain just compensation in the event of a data breach must be argued.

CODIFICATION OF DIRECTOR’S DUTIES

One of the most significant changes made by the 2013 Act was the codification of director responsibilities under Section 166. This clause makes an effort to bring much-needed clarity to a matter that was previously controlled by a patchwork of conflicting legal rulings. Despite widespread acceptance of the directors' fiduciary obligations under common law, definitive decisional law defining the breadth and depth of each obligation has proven elusive. It is therefore believed that codification will offer a blank canvas for judicial discussion of this important subject. In accordance with the new Act, directors have six broad obligations to the boards of the firms

they serve. “These obligations include (i) acting in accordance with the company's bylaws, (ii) acting in good faith to advance the goals and best interests of the company, (iii) carrying out duties with due and reasonable care, skill, diligence, and independent judgement, (iv) avoiding conflicts of interest, (v) not attempting to obtain an unfair benefit or advantage for himself or his family, and (vi) refraining from assigning his office. Of these, the responsibility of a director to discharge his obligations with care, competence, and diligence is particularly pertinent to cybersecurity concerns.”

It is difficult to refute the claim that proper cybersecurity measures should be included in the reasonable care that any director should conduct in managing company risk in the current paradigm, despite the fact that courts from around the world have not yet reached a consensus on this topic.[3] Legally, the situation might not be clear-cut. In the event of a breach, a court will probably need to determine whether the specific security measures implemented by a board were adequate to be regarded as good faith business judgements (see, for instance, the D&O Diary item on Palkon v. Holmes, et al.). Courts may take the following into account while making this decision:

- state-of-the-art of the technical and policy initiatives that a corporation has implemented;
- standards and best practises for both the entire industry and each sector;
- level of board or committee discussion on cyber issues;
- application of operational law suggestions.
- third-party security measure auditing and certification; and
- History of events' responses and remedies

Although these sums might appear insignificant, it should be remembered that the liability under this clause is likely to be of a personal character. Additionally, it might be possible for courts to impose the punishment on each of the several errors found in a post-breach scenario independently. The new Act recognises class actions, which gives shareholders and depositors the right to sue the firm or its directors for "any fraudulent, unlawful, or wrongful act or omission or conduct" and receive damages or compensation.[4] Although it hasn't been tested, this provision may significantly increase D&O risk in the future with regard to cybersecurity-related liability. Finally, it should be highlighted that any liability arising under this regime would be in addition to any liability arising under any parallel regimes, such as the Indian IT and data protection law.

---

[3] Black, B., Cheffins, B., & Klausner, M. (2005). Outside director liability. *Stan. L. Rev.*, *58*, 1055.

[4] Rhoads, C. B. (1916). Personal Liability of Directors for Corporate Mismanagement. *University of Pennsylvania Law Review and American Law Register*, *65*(2), 128-144.

LIABILITY OF DIRECTOR

According to the proportionality test, there are three criteria to use in judging whether a restriction or invasion of one's right to privacy is reasonable:

- The restriction imposed is lawful: must have legislative support.
- The restriction's suitability and necessity for the greater good.
- The degree of interference must be appropriate for the necessity for it to serve the greater good.

Therefore, in light of all the foregoing justifications, it is obvious that the right to privacy involves the right to protect private data. Accordingly, the criteria that must be met in order to restrict the right to privacy, which includes the privacy of personal data, must be met by anyone doing so.[5] Directors of numerous companies are thus included within its purview. It is important to note that the director will be held accountable for any violations of data privacy made by the company:

A. He or she was in charge of running the corporation's operations at the time the offence was committed; or

B. It was because of his or her negligence and consent that the offence was committed.

According to Section 150(12), an independent or non-executive director is only accountable for corporate omissions or commissions that occurred with their consent, permission, or full cooperation, or in situations where they refused to perform faithfully. “This somewhat lessens the concern of independent director responsibility. However, several issues, such as whether a director acted honourably and whether information may be linked to a director simply by their attendance at board meetings, remain unresolved. Additionally, the obligation that independent and candidate directors have under various other laws is still a serious concern. Liability may not always be restricted to the executive directors for actions such as dishonour of checks under the Negotiable Instruments Act of 1881, violations under the Income Tax Act of 1961, violations of currency exchange laws, violations of securities rules, non-payment of provident fund payments, etc.”

Additionally, several regulations addressing relevant issues do not distinguish between the various categories of directors in a business. The Honourable Supreme Court has ruled that the managing director, or MD, is ipso facto in charge and accountable for the operation of an enterprise and can be sued by the company for the commission of misdeeds in the cases of Nat'l Small Indus. Corp. Ltd. v. Harmeet Singh Paintal & Anr[6] and K.K. Ahuja v. V.K. Vora.[7]

---

[5] Dynkin, B., & Dynkin, B. (2017). Derivative liability in the wake of a cyber attack. *Alb. LJ Sci. & Tech.*, *28*, 23.

[6] (2010) 3 SCC 330.

[7] (2009) 10 SCC 48.

VIEWS OF INDIAN JUDICIARY

The topic of privacy has been addressed by Indian courts in a variety of cases. In the matter of Union of India v. Justice KS Puttaswamy (Retd).[8] Justices Bobde and Chandrachud said the following:

"At a normative level privacy subserves those eternal values upon which the guarantees of life, liberty and freedom are founded. At a descriptive level, privacy postulates a bundle of entitlements and interests which lie at the foundation of ordered liberty."

The Supreme Court acknowledged a person's right to protect his privacy in a variety of situations in "R. Rajgopal and Ors v. State of T.N"[9]. The right to privacy was acknowledged in "People's Union of Civil Liberties v. UOI"[10] in light of Art. 17 of the International Covenant on Civil and Political Rights and Art. 12 of the Universal Declaration of Human Rights. In "Ram Jethmalani and Ors v. UOI"[11], the SC acknowledged that Article 21 of the laws of India, 1950, includes the right to privacy as a fundamental right. covered by Article 21's protection of the right to life and personal liberty, which may be restricted by a legal process that is just, fair, and reasonable, as determined in "Maneka Gandhi v. Union of India"[12]. The Supreme Court ruled in "State of Maharashtra v. Bharat Shanti Lal Shah"[13] that the right to privacy might be restricted in accordance with the process legitimately established by law. In "Govind v. State of Madhya Pradesh"[14], it was determined that a citizen's explicitly granted fundamental rights cover a wide range of areas and that their right to privacy is a separate fundamental right that must be subject to limitations in order to protect compelling public interests.

It is evident from all the case laws cited that the Indian judiciary has expanded the definition of privacy to include a wide range of activities. Privacy should be interpreted broadly to include one's right to bodily autonomy, the ability to decide what is considered to be personal, and, of course, their own personal data. The right to privacy, which is protected by Article 21 of the Constitution of India, 1950, may only be restricted under exceptional circumstances, i.e., in the absence of a compelling governmental interest, and if it satisfies the proportionality test established by the Puttaswamy judgement.

[8] (2017) 10 SCC 1.
[9] 1995 AIR 264.
[10] (1997) 1 SCC 301.
[11] (2011) 1 SCC 560.
[12] 1978 SCR (2) 621.
[13] (2008) 13 SCC 5.
[14] 1978 SCR (2) 621.

In the wake of Puttaswamy, many High Courts have been arguing how to exercise various parts of privacy rights. Notable recent decisions by various High Courts on the parameters of the right to erasure and the right to be forgotten include Subhranshu Rout @ Gugul v. State of Odisha, Sri Vasunathan v. the Registrar General, High Court of Karnataka and Ors, and Dharamraj Bhanushankar Dave v. State of Gujarat and Ors. It is realistic to assume that judicial debate over the scope and implications of these rights will continue up until a new act is put into force because each of these courts had a distinct point of view.

COMPARISON WITH INTERNATIONAL LEGISLATION

The Data Protection Act of 2018 lays forth rules for how the government and private sector may utilise a person's personally identifiable information. All countries that are members of the European Union (EU) have implemented the General Data Protection Regulation (GDPR), which is an expansion of data protection legislation. The GDPR has been expanded in the UK by the Data Protection Act of 2018. The "principles of data security" are a set of guidelines that must be followed by everyone who handles a customer's personal information.

In matter of Google LLC v. Lloyd[15], The legislation and use of data security in the United Kingdom will be significantly impacted by this momentous decision. “The compilation and modification of browser generated information (or "BGI") by Google on Apple's Safari web browser is the subject of this representative argument, which is made on behalf of an estimated 4.4 million iPhone users. A representative lawsuit (sponsored by a litigation funder) can be an acceptable and efficient tool to use when suing for damages in relation to a multi-person infringement of privacy protection legislation, it was held in this particular case.”
Surprisingly, there are no data protection regulations in the United States. In contrast to the GDPR law of the European Union, there is no law at the Centre that will deal with data privacy and breaches at the central level.[16] Instead, there are a number of laws addressing privacy issues, including consumer-focused privacy legislation, that have been passed in different jurisdictions around the US.

[15] [2019] EWCA Civ 1599.
[16] Trautman, L. J., & Altenbaumer-Price, K. (2010). The board's responsibility for information technology governance. *J. Marshall J. Computer & Info. L.*, *28*, 313.

“The Federal Trade Commission Act exists in the United States and is somewhat similar to the Companies Act of 2013 in India. The Federal Trade Commission Act has significant influence over private businesses under its purview to prevent discriminatory or misleading marketing practises. The FTC uses its authority to set regulations, implement privacy laws, and conduct compliance actions to safeguard consumers, even if it does not directly dictate what information can be used in privacy policies for websites.”

Among these three countries, the United Kingdom is the only one with a national legislation protecting individuals' personal data. It is shocking to realise that the United States does not have any national legislation that governs data privacy, despite the fact that Facebook and Whatsapp were both founded in the United States. Different regulations governing the subject are in place in each state across the country. The Federal Trade Commission, on the other hand, acts as a national institution that addresses data privacy issues that are prevalent in the business world. The situation that currently prevails in India is both more tragic and horrible than it would otherwise be if there were central data protection regulations, state data protection legislation, or a central level authority that dealt with this matter. Liability can more easily be determined in countries like the United States and the United Kingdom because each state has its own set of laws to follow. The Indian judicial system has held several hearings on the subject of privacy, and these hearings have contributed to the formation of public perceptions on the confidentiality of personal data.

The Companies Act of 2013 and the related laws address data privacy in a roundabout approach; yet, they fall short of what Indians desire and fail to address their concerns regarding data privacy. One may say that the position held by the FTC in the United States is analogous to that of the Companies Act in India. In contrast, in India the requirements of the Act would be enforced by courts that are already dealing with backlogs of cases, whereas the FTC is a body that controls corporate matters, thus it will be significantly more effective.

CONCLUSION

Saving and transferring data is now lot simpler than it ever was in the current era of globalisation. The Aarogya setu case and the Whatsapp data breach case show that this has not only had beneficial consequences, but also a number of negative repercussions. Data exploitation and huge privacy breaches have grown simpler. “There is no specific law on the subject because it is a recent issue. A comprehensive center-level law on the subject was attempted with the introduction of the Personal Data Protection Bill of 2019 in the Parliament, but it has not yet materialised. In all areas of life, but especially in the business world, data privacy is crucial. Section 166 of the

Companies Act, 2013, has been construed to support data privacy needs and create the directors' liability in such circumstances." However, only the legislators know for sure if they meant for the statute to be interpreted in this way. India needs to address the problem seriously because it lags behind other developed countries in terms of concerns about data protection.

Even if D&O risk in relation to cybersecurity may be limited under existing Indian company law, it is largely uncertain how Indian courts would treat these issues using as-yet-untested mechanisms like class lawsuits. This is despite the fact that these methods have been tried. Given the problems with pendency that afflict the Indian legal system, however, it seems likely that judicial review of these concerns will not occur for at least a few more years. Up until that moment, businesses in India should make it a priority to implement security best practises that are relevant to their industries, in addition to rigorous organisational, technical, and managerial safeguards.