Page 2168 - 2175 **DOI:** *https://doij.org/10.10000/IJLMH.116369*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 6

2023

Explaining the Role of CSR in Promoting Data Privacy: An Analytical Research

MEERA SRIKANT[1] AND KEERTHANA SRINIVASAN[2]

ABSTRACT

This research paper examines the role of Corporate Social Responsibility Policies in promoting data privacy for its customers in the wake of digitalization of the economies. By analyzing the existing data protection laws and its compliance by the companies, especially in the Indian context it seeks to argue that the fundamental right of privacy is not protected completely and is still under threat due to various reasons such as data loss or data breaches, etc. CSR Policy, aimed at protecting data privacy, by companies which deal with data, especially in AI and IoT, will prove to be more effective in protecting privacy and seeks to further argue that it should be made obligatory for the companies which deal with data to include data privacy as part of the CSR Policy given the amount of power that they are endowed with. This research seeks to examine how the gap, which is created when, on the one hand, customers cannot enforce their fundamental right to privacy under Art. 32 of the constitution against private entities and on the other hand, the regulations made by the state as legislations are vague, incomplete and mere compliance of the same will not ensure complete transparency with respect to how data is used, is bridged when data privacy is part of the CSR Policy of the company.

I. INTRODUCTION

"Personal data is the new oil of the internet and new currency of the digital world" stated the European Consumer Commissioner Meglena Kuneva in the year 2009.[3] True to the statement, the usage and profitability of personal data has increased manifold, from the usage of social media websites, to smart appliances like virtual assistant devices (Siri, Alexa), smart watches, smart homes, smart refrigerators, etc. and AI chatbots. While these devices, apps and websites are increasingly becoming a part of our day to day lives, it is also true that these tools function entirely on personal data which can pose a threat to user's personal security and privacy if not dealt with responsibly. As device users add more products to their ecosystems, the threat of

[1] Author is a student at SASTRA Deemed to be University, India.
[2] Author is a student at SASTRA Deemed to be University, India.
[3] Meglena Kuneva - European Consumer Commissioner - Keynote Speech - Roundtable on Online Data Collection, Targeting and Profiling, EUROPEAN COMMISSION - EUROPEAN COMMISSION, https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156 (last visited Dec 14, 2023).

 [ISSN 2581-5369]

being victimized by acts of privacy invasion and/or hacking also goes up.[4] Thus, the companies have to deal with the collected data in an ethical manner in order to protect the consumers. While compliance with the law does not effectively address the issue of data privacy, is there a way corporate can do it and address the issue of privacy through their obligation towards corporate social responsibility?

II. WHAT IS DATA PRIVACY?

'Data' is defined in the Digital Personal Data Protection Act, 2023,[5] as "data" means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means; and 'Personal Data' is defined as any data about an individual who is identifiable by or in relation to such data. One's name, address, phone number, and online or offline conduct are examples of personal information. Companies in various industries use various types of personal data to provide services to enhance consumer experience and most importantly to train machine learning and AI systems.

Data privacy is the ability of an individual to control their personal information and to determine, when, what and how their personal information should be disseminated. The Internet on the other hand, is not only a means of communication, but also used for various other activities, even to the extent of serving as a virtual assistant to the individuals. The IoT devices collect vast quantities of granular data that include health related data, location data and consumption rate data among other things. Individuals' habits and activities are constantly monitored by these devices in order to enhance the services that they provide. An increasing number of IoT-connected devices, including smartphones, home appliances, fitness trackers, car telemetry systems, 'smart' energy meters, smart ticket gates at train stations and airports and even connected clothing – consume and produce vast quantities of personal data in the IoT to personalize retail experiences, optimize journeys, improve health, help manage finances and minimize energy consumption.[6] According to Transparency Market Research, in 2017 personal data accounted for 36% of direct data sales, both legal and illegal, in a global data market worth $250Bn.[7]

[4] Jennifer Kent, *The Smart Money: Privacy Concerns a Barrier to Smart Device Adoption*, SECURITY INFO WATCH (2023), https://www.securityinfowatch.com/residential-technologies/smart-home/article/53042437/the-smart-money-privacy-concerns-a-barrier-to-smart-device-adoption (last visited Dec 14, 2023).
[5] The Digital Personal Data Protection Act, 2023
[6] Perera C., Liu C. H., Jayawardena S.:'The emerging internet of things marketplace from an industrial perspective: A survey', IEEE Transactions on Emerging Topics in Computing, 2015, 3, (4), pp. 585-598
[7] 'Transparency Market Research - Data broker market, global industry analysis, size, share, growth, trends and forecast 2017 – 2026', https://www.transparencymarketresearch.com/data-brokersmarket.html, accessed 25

 [ISSN 2581-5369]

With such a huge amount of data materially contributing to the market of virtually every sector of businesses, it raises serious privacy concerns among the customers, as there is a potential possibility of data loss, unauthorized use and dissemination, and data breach, lack of transparency being the foremost reason for the same. According to a research done on amazon's AI technology based Alexa in the healthcare industry[8], it was noted that, the methodology for AI learning is highly proprietary[9]. Devices like Amazon's Alexa are constantly recording information, "listening" to and analyzing their surroundings. Amazon's proprietary algorithms are what transform average everyday observations into a profitable and efficient consumer assistant. It was found that due to Amazon's patents and trade secrets surrounding its Al technology, consumers may never know what they are doing with the data they collect.[10] Moreover, If the consumers are not willing to consent to the privacy policy of the devices, the service provider or the data fiduciary, is free to terminate the services provided and this is permitted by the IT (Reasonable Securities Practices) Rules, 2021[11]. Thus, the question arises as to what is the level of informed choice that the customers are exercising, and how to strike a balance between the use of data by companies for profit and protecting personal integrity of the information of the users of data.

III. DATA PRIVACY AS A FUNDAMENTAL RIGHT

Article 21 of the Indian Constitution[12] states that, "No person shall be deprived of his right to life and personal liberty except according to procedure established by law". The Supreme Court in the famous case of K.S. Puttaswamy v. Union of India[13] recognized the right to privacy as a fundamental right, intrinsic to Article 21 of the constitution. While holding so, the Court recognized the fact that the right to informational privacy is an important facet of right to privacy. The Court further acknowledged the fact that, the age of information has raised important concerns for the privacy of data of the individuals especially because of the nature of

February 2019

[8] ALEXA's ARTIFICIAL INTELLIGENCE PAVES THE WAY FOR BIG TECH'S ENTRANCE INTO THE HEALTH CARE INDUSTRY - THE BENEFITS TO EFFICIENCY AND SUPPORT OF THE PATIENTCENTRIC SYSTEM OUTWEIGH THE IMPACT ON PRIVACY - Nicole Angelica

[9] Richard Baguley & Colin McDonald, Appliance Science: Alexa, How Does Alexa Work? The Science of the Amazon Echo, CNET (Aug. 4, 2016), https://www.cnet.com/news/appliance-science-alexa-how-does-alexa-work-thescience-of-amazons-echo [https://pena.cc/9UDW-UABE].

[10] Lauren Bass, The Concealed Cost of Convenience: Protecting Personal Data Privacy in the Age ofAlexa, 30 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 261, 271-72 (2019)

[11] Rule 5(7), IT (Reasonable Securities Practices) Rules, 2021 (Such withdrawal of the consent shall be sent in writing to the body corporate. In the case of provider of information not providing or later on withdrawing his consent, the body corporate shall have the option not to provide goods or services for which the said information was sought.)

[12] Article 21 of the Indian Constitution

[13] (2017) 10 SCC 1

 [ISSN 2581-5369]

data itself as it is non-rivalrous, recombinant, and invisible, thereby making data breaches difficult to detect.

While it is clear that right to privacy is a fundamental right, where it is against a non-state actor, a common law right to privacy would lie at the ordinary courts of law[14]. The three-fold test of legality, legitimate state aim and proportionality, laid down by the Court in Justice K S Puttaswamy's case, will not be applicable as the companies that deal with data in the IoT sector are primarily private entities and not classified as 'state' under Article 12 of the Constitution. Though a right of privacy under Article 21 of the Constitution may be violated by a private entity, it cannot be enforced as a writ under Article 32 of the Constitution. Therefore, proving a violation of right to privacy and enforcing the right guaranteed under Article 21 of the Constitution becomes all the more difficult as the case will be set on a different paradigm altogether. In the Californian case of Lopez v. Apple Inc.[15], where it was contended by the plaintiff that Apple had the software-program "Siri", installed in all its devices and the said software was routinely triggered without the key wo rd, "Hey Siri" and certain devices had "high accidental trigger rates" and secondly, a "small portion" of Siri recordings, both deliberate and accidental, are sent to third-party contractors for evaluation, the Court dismissed it by stating that, the plaintiffs had failed to show a legally cognizable interest of privacy which was violated, even though the Court accepted the fact that merely stating that the device will not be error-free does not prove the fact that consent has been acquired. The Court also stated that the plaintiffs failed to show a personal injury or a specific instance where privacy has been violated. A similar stand was taken by the Court in In re Google Assistant Privacy Litigation[16]. Though it might be obvious that there is a breach of privacy by the data fiduciary, it might not always be possible to prove a personal injury. This shows the difficulty involved in bringing an action against the data fiduciary whenever there is a breach of privacy.

IV. AMBIGUITIES IN EXISTING DATA PROTECTION LAWS

Section 4 of the Digital Personal Data Protection Act, 2023 states that, A person may process the personal data of a Data Principal only in accordance with the provisions of this Act and for a lawful purpose, (a) for which the Data Principal has given her consent; or (b) for certain legitimate uses. (2) For the purposes of this section, the expression "lawful purpose" means any purpose which is not expressly forbidden by law. Here, the law does not clearly lay down what exactly constitutes a "legitimate purpose", especially considering the fact that consent is not

[14] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1
[15] "Case No. 19-cv-04577-JSW" *Lopez v. Apple, Inc.*, 519 F. Supp. 3d 672, (N.D. Cal. 2021)
[16] 457 F. Supp. 3d 797, 829 (N.D. Cal. 2020)

 [ISSN 2581-5369]

necessary if the processing is for a legitimate purpose. Something that is legitimate is acceptable according to the law.[17] Simply obtaining data for any legitimate purposes would mean that practices tracking online behavior, for instance, for providing personalized advertisements, etc., would also be valid according to the Act but it might not be the purpose for which the consumer consented for and is, therefore, unethical, considering privacy concerns associated with it.

Furthermore, Rule 5(2) of Information Technology (Reasonable Security Practices And Procedures And Sensitive Personal Data) Rules, 11 states that, (2) Body corporate or any person on its behalf shall not collect sensitive personal data or information unless — (a) the information is collected for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf; and (b) the collection of the sensitive personal data or information is considered necessary for that purpose. Though the rule is very clear on the fact that the data collected must be necessary for fulfillment of the intended purpose, it is again left to the corporations to decide whether a particular data is necessary or not for its functioning. This fact becomes all the more crucial while looking into AI and IoT based tools and devices, by the use of which, in most cases, consumers do not know what data is actually being collected, stored, processed and disseminated. According to a study by the Global Privacy Enforcement Network in 2016, the majority of connected devices fail to adequately explain to customers how their personal data is processed. Specialist market analyst IoT Analytics reports that the number of connected devices that were in use worldwide in 2018 exceeded 17 billion, with the number of IoT devices at 7 billion (this definition excludes smartphones, tablets, laptops and fixed line phones). It estimates that by 2025 there will be 34.2 billion connected devices, of which 21.5 billion will be IoT devices.[18] There is no rule or regulation specifically governing how data is to be collected, processed and disseminated in an AI or IoT based tool or device thereby providing room for legal yet *unethical* use of data. Thus, it is amply clear that data ethics is something very crucial and every corporate dealing with the use of data must incorporate it in its business practices.

V. CORPORATE SOCIAL RESPONSIBILITY - HISTORY AND BACKGROUND

According to Michel Hopkins[19] "Corporate Social Responsibility is concerned with treating the

[17] Kent, *supra* note 4.

[18] IoT Analytics: State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating', https://iotanalytics.com/state-of-the-iot-update-q1-q2-2018-number-ofiot-devices-now-7b/, accessed 25 February 2019

[19] Michael Hopkins: A Planetary Bargain: Corporate Social Responsibility Comes of Age (Macmillan, UK, 1998; updated and re-printed by Earthscan, 2003 and again reprinted by Routledge, UK, 2010). The definition has also been slightly improved over time and may continue to do so as better versions appear. Since 1998 the definition has been changed only thrice – once to note that CSR is a process to achieve sustainable development,

stakeholders of a company or institution ethically or in a responsible manner. 'Ethically or in a responsible manner' refers to treating key stakeholders in a manner deemed acceptable according to international norms." Corporate Social Responsibility is a way in which companies run their businesses in such a way that it brings a positive impact on the society, and its stakeholders. Generally, businesses are run with the intention of a profit motive, sometimes earning profits at the cost of the society and environment. To prevent that, and to make businesses recognise its obligations towards various stakeholders, Section 135[20] of the Companies Act mandates that, "(1) Every company having net worth of rupees five hundred crore or more, or turnover of rupees one thousand crore or more or a net profit of rupees five crore or more during any financial year shall constitute a Corporate Social Responsibility Committee of the Board consisting of three or more directors, out of which at least one director shall be an independent director.", and, "(3) The Corporate Social Responsibility Committee shall,— (a) formulate and recommend to the Board, a Corporate Social Responsibility Policy which shall indicate the activities to be undertaken by the company as specified in Schedule VII; (b) recommend the amount of expenditure to be incurred on the activities referred to in clause (a); and (c) monitor the Corporate Social Responsibility Policy of the company from time to time".

Majorly, there are 4 main types of responsibilities that companies undertake. They are, 1. Environmental Responsibility, which means the organization's commitment to undertake sustainable and eco-friendly operations, 2. Ethical Responsibility, which means to operate business in an ethical manner and undertake fair business practices, 3. Philanthropic Responsibility, which refers to the company's aim for the betterment of the society as a whole and 4. Economic Responsibility which means a commitment to take financial decisions that help in the betterment of the society for example, investing in alternative energy sources.

In summary, Corporate Social Responsibility is the Company's responsibilities towards its stakeholders, which can take various forms. It is a win-win approach for the companies i.e., reaping economic benefits by being socially responsible to the community as a whole. The Companies Act prescribes the activities to be undertaken in Schedule VII while leaving it to the discretion of the companies to choose the type of activity they want to undertake. However, corporations should not merely see it as mere statutory compliance but actual and voluntary

then to include non-private institutions and the most recent to link more closely to the body of work of the Global Reporting Initiative (GRI) by noting that both CSR and Sustainability address multi-stakeholders and their choice depends upon their materiality i.e., importance to the institution

[20] Section 135 of the Companies Act

 [ISSN 2581-5369]

contribution to the society's welfare.

VI. CSR AND DATA ETHICS

Data ethics means dealing with data i.e., collecting, gathering, analyzing and disseminating data in an ethical and responsible manner, so as to ensure data security to all stakeholders. Ethical responsibility is one of the main pillars of corporate social responsibility. Having ethical responsibilities means ensuring a business engages in fair business practices across the board—from the supply chain to the boardroom. It implies that companies should treat all employees, stakeholders, and customers ethically with fairness and respect.[21] Stakeholders are people who have an interest or derive a benefit from the organization. Consumers are one of the most important stakeholders in an organization.

As established earlier, AI and IoT based devices function entirely on data provided by the customers and use it to generate profit. Moreover, there is a growing concern for privacy as the usage of smart appliances grows rapidly. With the advent of Internet and data analytics, issues surrounding the protection or sharing of personal data have emerged as crucial nexuses of economic and policy debate.[22] Over the years, national surveys have consistently found widespread evidence of significant privacy concerns among Internet users.[23] These data concerns can be addressed to a certain extent if companies practice data ethics.

Data ethics includes addressing and advocating the concepts of right and wrong conduct, with transparency in and defensibility of actions and decisions driven by automated/artificial intelligence (AI) in relation to data in general and personal data in particular.[24] Thus, the Corporate Social Responsibility of companies should be aimed at providing digitized services in an ethical and responsible way. On the other hand, Corporate Digital Responsibility (CDR), a novel concept which began to gain recognition in the academic forum only after 2019 (Herden et al. 2021; Lobschat et al. 2021), is defined as a set of practices and behaviors that help an organization use data and digital technologies in socially, economically, and environmentally responsible ways. It is an extension of a firm's responsibilities which takes into account the ethical opportunities and challenges of digitalization.[25] Data privacy and security is an

[21] Pacific Oaks College, *Corporate Social Responsibility: 4 Types Explained | Pacific Oaks*, VOICES DIGITAL (2021), https://www.pacificoaks.edu/voices/business/breaking-down-the-4-types-of-corporate-social-responsibility/ (last visited Dec 14, 2023).

[22] Consider, for instance, the 2013 White House's report on "Big Data: Seizing Opportunities, Preserving Values," available at http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf.

[23] For instance, a Pew Research Center survey of 1,002 adult users conducted in 2013 found that 86 percent had taken steps online to remove or mask their digital footprints, and 68 percent believed that current laws were not good enough in protecting online privacy (Rainie et al. 2013)

[24] https://www.cognizant.com/us/en/glossary/data-ethics

[25] Herden et al 2021: 17

important aspect of ethical and social responsibilities of the companies in the Digital world. Moreover, as an organization grows, the usage of data, data security and confidentiality of data, data ethics of the organization, will have a huge impact on the trust and reputation of the organization. In a circular released by Ministry of Corporate Affairs, dated 5th January 2014[26], it was clarified via Annexure 1, Sl. No. 4 that "consumer protection Services" are eligible under CSR. Thus, all activities undertaken towards protecting the data provided by customers and using it in a responsible manner will be a part of the CSR activities necessary to be undertaken under Section 135 of the Act.

VII. CONCLUSION

CSR activities are undertaken with an intent to create a positive impact on the society, economy and the environment as a whole. While the utilization of data for AI tools and in the IoT industry is on the rise, it also raises serious privacy concerns because of lack of transparency, overwhelming amount of data, vulnerable and weak security systems, etc. On the other hand, the data that companies in the IoT and AI sector gather is extremely important for their profitability as these apps and devices entirely function on the data that they receive from the customers. Thus, when the corporations make data ethics a part of corporate social responsibility and strictly adhere to data ethics, it will benefit the society on the whole because of more data security practices, thereby benefiting the long-term growth of the organization.

*****

[26] General Circular No. 21/2014

 [ISSN 2581-5369]