Page 4666 - 4670 **DOI:** *https://doij.org/10.10000/IJLMH.119411*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 2

2025

Navigating the Dual Nature of Data

KHUSHBOO RATHORE[1] AND SAPNA T[2]

ABSTRACT

It is well said by Nandan Nilekani that "The data has become the new oil." In the digital era, data is both a tremendous tool and a huge liability, bringing complex difficulties to cyber law in balancing empowerment and protection. The data drives innovation, economic growth, and decision-making in industries such as e-commerce, artificial intelligence, healthcare, and scientific research, resulting in personalised experiences and technical improvements. However, mismanagement creates dangers such as data breaches, cyberattacks, and regulatory complexity such as India's Aadhaar-related vulnerabilities, highlight systemic flaws in data management. Robust frameworks such as the European Union's General Data Protection Regulation (GDPR) and India's Digital Personal Data Protection (DPDP) Act are crucial for managing data collection, storage, and usage, with the goal of protecting individual privacy while supporting responsible data utilization. As cybercrime evolves, tighter legislation, harsher fines, and increased cybersecurity investments become critical. This essay investigates data's dual nature as a driver of advancement and a source of vulnerability in the twenty-first century digital ecosystem. It emphasizes the importance of a balanced approach to leveraging data's potential while reducing its risks through case studies and regulatory framework research. The essay advocates for comprehensive methods, including strong legal safeguards and ethical norms, to protect personal data and promote responsible use within legal limitations, ensuring a secure and inventive data-driven future for India and beyond.

***Keywords**: Artificial intelligence, data breach, e-commerce, and cybercrime.*

The 21st century, which is often known as the digital world, where in the courtroom of cyberspace, data serves as both witness and culprit, challenging cyber law to strike a delicate balance between empowerment and protection. The data is an important asset in almost every field from social media to digital transactions, businesses to government offices, and individuals to the vast public. The economist once said that "the world's most valuable resource is no longer oil but data"[3] However, data is not only an asset but also a potential liability. Data becomes an easy target for threats through data breaches, hacking, stalking, and through many more ways.

[1] Author is a student at Amity University, Rajasthan, India.
[2] Author is a student at Amity University, Rajasthan, India.
[3] The Economist on May 6th, 2017/ https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

 [ISSN 2581-5369]

The dual-edged nature of data has led the authorities to enact data protection frameworks such as the General Data Protection Act of the European Union and the Digital Personal Data Protection Act of India. These regulations help to balance out the power of data and safeguard the privacy and security of sensitive information. This essay while explaining the dual nature of data will potentially highlight the importance of data-driven decision-making and acknowledge the risks posed by cyber threats through various case studies.

Data has emerged as an indispensable asset in the digital era, fuelling innovation, driving economic growth, and unlocking previously unheard industry opportunities. Data has become the lifeblood of modern businesses, with e-commerce giants using it to personalize recommendations and improve user experiences and healthcare providers using it to make more accurate diagnoses and personalised treatment plans. Data's value stems from its ability to provide insights, inform decision-making, and optimise processes. Organisations can discover patterns, trends, and correlations that would otherwise go unnoticed by collecting and analysing massive amounts of data. This data-driven approach allows businesses to make more informed strategic decisions, streamline operations, and gain a competitive advantage in their markets.

Furthermore, data has fuelled the development of ground-breaking technologies like artificial intelligence (AI) and machine learning (ML). These cutting-edge technologies use massive datasets to train their algorithms, allowing them to recognise patterns, predict outcomes, and automate complex tasks with remarkable accuracy. Data is the driving force behind technological advancements ranging from virtual assistants and recommendation engines to autonomous vehicles and predictive maintenance systems.

For example, Netflix attained a retention rate of more than 90% by personalizing suggestions, adjusting advertisements, and creating their own content to fit their users' individual viewing tendencies.[4] According to Netflix's Q4 2022 earnings report, the company had a retention rate of 92.8% in the United States and Canada market. This means that out of every 100 customers, 92.8 customers renewed their subscription or stayed with Netflix during that period.[5]

Aside from its commercial applications, data has proven invaluable in advancing scientific research, addressing global challenges, and improving public services. For example, genomic data has transformed our understanding of diseases and laid the groundwork for personalised medicine. Environmental data has allowed scientists to track climate change and devise

[4] "Netflix Revenue and Usage Statistics (2024)"-business of apps; Mansoor Iqbal, February 7, 2024, https://www.businessofapps.com/data/netflix-statistics/

[5] "Top Streaming Statistics In 2024"-forbeshome; Ana Durani; Feb 2, 2024., https://www.forbes.com/home-improvement/internet/streaming-stats/

 [ISSN 2581-5369]

mitigation strategies. Government agencies use data to optimise resource allocation, improve public safety, and deliver essential services. Furthermore, the importance of data goes beyond its immediate applications. Data has become a tradable commodity, and businesses are monetizing their data assets through a variety of business models, including data brokering, data licencing, and data-driven product offerings. This has resulted in a thriving data economy, where businesses can generate revenue streams by leveraging their data.

In today's data-driven world, data is a remarkable asset but as it is well known that everything comes with consequences, data also comes with liability. Challenges such as privacy breaches, misuse, and mishandling of data are quite common nowadays. Any misuse, exploitation, and unauthorized use of an individual's data could lead to a breach of privacy and cause legal proceedings as the right to privacy is a fundamental right in India under Article 21.[6] Cyber-attacks such as phishing and malware attacks risk the security of data which leads to security damages, reputational damages, and legal liabilities. By clicking on hyperlinks, individuals may expose their bank account details and personal data to data unauthorized access which may lead to identity theft, financial loss, and many more consequences such as messages (SMS) circulated in India through scammers claiming to be SBI's official SMS and asking users to update their PAN card or otherwise their YONO (SBI's mobile app) account will be blocked.[7]

Mostly, individuals these days are unaware about the frauds done by various websites and apps. New and advanced technology for better function of digital devices is improved by certain advancement in programming, as a result a new concept of cookies emerged. Cookies are small pieces of text sent to the user's browser by a website they visit which help that website remember information about the visit and can both make it easier to visit the site again and make the site more useful. After reaching any site and any app, a notification of "accept all cookies" appears, and by clicking on "accept" an individual's personal data could be accessed by a data fiduciary. Application such as Facebook have led to public outcry, regulatory scrutiny, and legal proceedings for data breaching.[8]

In India, the Aadhaar card was introduced by the central government for the sake of identity proof and further required to avail all the existing government schemes. However, the voluntary program gradually became a de facto mandatory requirement due to Aadhaar's being linked to

[6] Justice K.S. Puttaswamy (Retd) vs UOI, AIR 2018 SC (SUPP) 1841

[7] "SBI bank holder, state bank of India never sends these messages; warns the government"- Times New India, December 14, 2023, https://timesofindia.indiatimes.com/gadgets-news/sms-asking-users-to-update-their-pan-card-to-avoid-their-account-getting-blocked-is-a-scam-pib-fact-check/articleshow/106000916.cms

[8] "Facebook data breach"- Franklin D. Azar & Associates, https://www.fdazar.com/class-action/facebook-data-breach/

 [ISSN 2581-5369]

almost every document of an individual which creates a centralized database of personal data. The question of the security of the personal data of millions of individuals was raised when the website of Jharkhand state accidentally released data of 1.6 million pension beneficiaries.[9] This breach shows the failure of robust data protection measures and the vulnerabilities of the system.

Furthermore, the carelessness of the Indian government was reflected when RS Sharma, chairman of India's telecom regulator tweeted his Aadhaar number to the public to show his confidence in the system, but it ended up in the creation of a fake Aadhaar card on his name which was accepted by amazon and Facebook as genuine.[10]

For achieving the balance between leveraging data as asset, the Data Protection acts provide crucial instruments in striking the right balance between data usage and liability. These regulations aim to provide the governance of the data's collection, storage, processing, and use. There are various regulations in different countries such as European Union has its General Data Protection Regulation Act (GDPR), 2018, and India has the Digital Personal Data Protection Act (DPDPA), 2023.

India's DPDP Act is a big step by the Indian government to protect the individual's data and privacy, it is the first data protection act of India. The act applies on the processing of digital data within the territory of India as well as outside the territory of India if such processing is in connection with any activity related to the offering of goods or services to Data Principals within the territory of India.[11]

While these regulatory measures are crucial steps in the right direction, they also highlight the complex challenges associated with data management. Businesses must strike a delicate balance between leveraging data for innovation and growth while ensuring robust data security and privacy measures are in place. This requires significant investments in cybersecurity infrastructure, employee training, and the implementation of best practices for data governance.

Evolving through time, as the development in digital era is pacing up, it can be said that data is boon and bane in different aspects. As stated earlier, the exposure of personal data on the internet is controversial as the digital world is undeniably vast in nature. Therefore, to protect the privacy of the users, several laws and rules are made in order to ensure ethical use of their

[9] "Aadhaar details of about 1.6 million residents leak in Jharkhand" – First Post; April 23, 2017, https://www.firstpost.com/tech/news-analysis/aadhaar-details-of-about-1-6-million-residents-leak-in-jharkand-3701559.html

[10] "The Aadhaar Card: Cybersecurity Issues with India's Biometric Experiment"-Madhav Jain, May 9, 2019, https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/

[11] Digital Personal Data Protection Act, 2023., https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

 [ISSN 2581-5369]

personal data within legal boundaries of any nation. However, it can be seen that cyber-crimes are volatile in nature and therefore there is no limitation on the types of these crimes as new sort of crimes are emerging almost every hour in the digital realm. Considering the growth in cyber-crimes it is analysed that in India even though required measures are being taken by the authorities, the amount of cyber crimes are impossible to curb. Therefore, we would like to suggest that more stringent rules and regulations must be made not only to prevent crimes but also to severely punish the culprit.

*****

 [ISSN 2581-5369]